Bitdefender

GravityZone

PŘÍRUČKA ADMINISTRÁTORA

Bitdefender GravityZone
Příručka administrátora

Datum vydání 2021.04.19

Právní oznámení

Bitdefender

Obsah

Předmluva

Tento průvodce je cílen na síťové správce, kteří jsou zodpovědní za správu zabezpečení GravityZone v rámci prostoru své firmy.

Cílem tohoto dokumentu je vysvětlit způsob aplikace a prohlížení bezpečnostních nastavení na koncových bodech v síti pod vaším účtem pomocí GravityZone Control Center. Naučíte se, jak prohlížet síťový inventář v Control Center, jak vytvářet a aplikovat pravidla na spravované koncové body, jak vytvářet hlášení, jak spravovat soubory v karanténě a jak používat ovládací desku.

1. Konvence použité v tomto návodu

Typografické konvence

Tento průvodce používá několik typů textu pro lepší čitelnost. Jejich vzhled a význam je uveden v následující tabulce.

Vzhled	Popis
`ukázka`	Názvy příkazů a syntaxí v řádku, cesty a názvy souborů, výstupy konfiguračních souborů a vstupní text jsou psány `neproporcionálním` písmem.
http://www.bitdefender.com	Webové stránky jsou umístěny na http nebo ftp serverech.
gravityzone-docs@bitdefender.com	Kontaktní E-mailové adresy vloženy v textu.
„Předmluva“ (str. ix)	Toto je interní odkaz, směřující na nějaké místo v dokumentu.
možnost	Všechna nastavení jsou zvýrazněna **tučným** písmem.
klíčové slovo	Možnosti rozhraní, klíčová slova nebo zkratky jsou zvýrazněny **tučným** písmem.

Poznámky k textu

Poznámky jsou v textu graficky značené, nabízejí vám dodatečné informace k stávajícímu odstavci.

Poznámka
Poznámka je jen krátké shrnutí. Ačkoli ji můžete vynechat,poznámky mohou poskytnout cenné informace, jako např. zvláštní funkce nebo odkaz na související téma.

Důležité
Toto vyžaduje vaši pozornost a není doporučeno toto přeskočit. Obvykle poskytuje ne rozhodující, avšak významné informace.

Varování
Toto je důležitá informace, se kterou byste měli zacházet se zvýšenou opatrností. Nic nezkazíte tím, budete-li se držet pokynů. Toto varování byste si měli přečíst a porozumět mu, jelikož popisuje něco velice riskantního.

1. O GRAVITYZONE

GravityZone je řešení zabezpečení pro firmy, které je od základu vytvořeno k virtualizovanému nebo cloudovému provozu, poskytující bezpečnostní služby fyzickým koncovým zařízením, mobilním zařízením a virtuálním zařízením v soukromém i veřejném cloudu, a poštovním serverům Exchange.

GravityZone je jeden produkt se sjednocenou správní konzolí, dostupný v cloudu hostovaném společností Bitdefender, nebo jako virtuální zařízení k instalaci ve firemně a poskytuje jediný bod pro nasazení, vynucení a správu bezpečnostních politik pro jakýkoli počet a typ koncových bodů, umístěných kdekoliv.

GravityZone doručuje několik vrstev zabezpečení pro koncová zařízení a pro Microsoft Exchange mail servery: Antimalware se sledováním chování, ochrana před zero day, kontrola aplikací a sandboxing, firewall, řízení zařízení, řízení obsahu, anti-phishing a antispam.

2. OCHRANNÉ VRSTVY GRAVITYZONE

GravityZone poskytuje následující ochranné vrstvy:

- Antimalware
- Pokročilá ochrana před hrozbami (ATC)
- HyperDetect
- Pokročilý Anti-Exploit
- Firewall
- Kontrola obsahu
- Patch Management
- Kontrola zařízení
- Šifrování celého disku
- Security for Exchange
- Kontrola aplikací
- Sandbox Analyzer
- Systém detekce hrozeb a následných opatření pro ochranu koncových bodů (Endpoint Detection and Response (EDR))
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

Vrstva antimalwarové ochrany je založena na skenování signatur a heuristické analýze (B-HAVE, ATC) proti: virům, červům, trojským koním, spywaru, adwaru, keyloggerům, rootkitům a dalším druhům škodlivého softwaru.

Protimalwarová skenovací technologie Bitdefender se opírá o následující vrstvy:

- Nejprve je použita tradiční metoda skenování, kde skenovaný obsah je porovnáván s databází signatur. Databáze signatur obsahuje bajtové vzory, specifické pro známé hrozby, a Bitdefender ji pravidelně aktualizuje. Tato metoda skenování je účinná proti ověřeným hrozbám, které byly prozkoumány a zdokumentovány. Nehledě na to, jak rychle je databáze signatur aktualizována, v mezičase mezi zjištěním nové hrozby a vydání nápravy vždy vznikne trhlina se zranitelností.
- Proti zbrusu novým, nezdokumentovaným hrozbám, **B-HAVE**, heuristický stroj Bitdefender, poskytuje druhou vrstvu ochrany. Heuristické algoritmy rozpoznají

malware na základě chrakteristiky chování. B-HAVE spouští podezřelé soubory ve virtuálním prostředí, aby otestoval jejich dopad na systém a ujistil se, že nepředstavují hrozbu. Pokud je zjištěna hrozba, programu je zabráněno ve spuštění.

Skenovací nástroje

Bitdefender GravityZone je schopna automaticky nastavit skenovací nástroje při vytváření balíčků agenta zabezpečení podle konfigurace koncového bodu.

Administrátor si může vybrat mezi několika skenovacími technologiemi a tím upravovat skenovací nástroje:

1. **Místní sken**, když je skenování prováděno na místním koncovém bodě. Režim lokálního skenování je vhodný pro výkonné stroje, které mají všechny signatury a nástroje uloženy lokálně.
2. **Hybridní skenování s odlehčenými nástroji (Veřejný cloud)**, se středním vytížením zdrojů koncového bodu, které využívá skenování v cloudu a částečně místní bezpečnostní nástroje. Tento režim skenování s sebou nese výhodu lepší spotřeby zdrojů, zatímco zahrnuje mimoprostorové skenování.
3. **Centrální skenování ve veřejném nebo soukromém cloudu**, s malou stopou a vyžadující Security Server pro skenování. V tomto případě žádný set signatur není uložen lokálně a skenování je přeloženo na Security Server.

   Poznámka
   Minimální sada nástrojů, potřebná k rozbalení komprimovaných souborů, je uložena lokálně.

4. **Centrální skenování (skenování veřejného nebo osobního cloudu pomocí Security Server) * v podobě Lokálního skenování (plnohodnotný agent)**
5. **Centrální skenování (skenování veřejného nebo osobního cloudu pomocí Security Server) s alternativní variantou* v podobě Hybridního skenování (Veřejný cloud s odlehčeným agentem)**

* V případě skenování pomocí dvou strojů najednou, pokud je jeden z nich nedostupný, bude použit záložní. Spotřeba zdrojů a využití sítě záleží na použitém typu skenování.

2.2. Pokročilá ochrana před hrozbami (ATC)

Pro hrozby, které uniknou i heuristickému nástroji, je zde třetí vrstva ochrany, přítomná ve formě Pokročilé ochrany před hrozbami (ATC).

Pokročilá ochrana před hrozbami nepřetržitě monitoruje spuštěné procesy a hodnotí podezřelé chování, jako například pokusy o: maskování typu procesu, spuštění kódu v umístění jiného procesu (zmocnění se procesové paměti za účelem zvýšení privilegií), replikaci, přetahování souborů, schovávání před aplikacemi pro výpočet procesů, atd. Každé podezřelé chování zvyšuje hodnocení procesu. Po dosažení prahové hodnoty,se spustí poplach.

2.3. HyperDetect

Bitdefender HyperDetect je další vrstva zabezpečení, která je speciálně navržena tak, aby detekovala pokročilé útoky a podezřelé aktivity ještě předtím, než proběhnou. HyperDetect obsahuje modely strojového učení a detekci útoků proti stealth útoku a proti hrozbám, jako jsou například: útoky nultého dne, pokročilé přetrvávající hrozby (APT), obfuskační malware, bezsouborové útoky (zneužití PowerShell, Windows Management Instrumentation atd. .), Krádeže pověření, cílené útoky, obyčejný malware, útoky založené na skriptech, exploity, nástroje hackování, podezřelý síťový provoz, potenciálně nežádoucí aplikace (PUA), ransomware.

2.4. Pokročilý Anti-Exploit

Tato nová proaktivní technologie, poháněná strojovým učením, zastaví útoky nultého dne prováděný pomocí exploitů. Advanced Anti- Exploit zachycuje nejnovější exploity v reálném čase a zmírňuje zranitelnosti v oblasti poškození paměti, které se mohou vyhnout stávajícím řešením. Chrání nejčastěji používané aplikace, jako jsou prohlížeče, Microsoft Office nebo Adobe Reader, stejně jako ostatní, na které si vzpomenete. Sleduje systémové procesy a chrání před narušením bezpečnosti a únosem stávajících procesů.

2.5. Firewall

Firewall kontroluje přístup aplikací k síti a k internetu. Přístup je automaticky povolen souhrnné databázi známých, legitimních aplikací. Firewall dokáže chránit systém proti skenování portů, zamezit ICS a varovat, když se k Wi-Fi síti připojí nové uzly.

2.6. Kontrola obsahu

Modul Kontrola obsahu pomáhá vymáhat podniková pravidla pro povolený přenos, přístup k webu, ochranu dat a kontrolu aplikací. Administrátoři mohou určit nastavení skenování přenosu a výjimky, naplánovat přístup k webu současně s blokováním vybraných webových kategorií nebo URL, konfigurovat pravidla ochrany dat, a definovat povolení pro užívání určitých aplikací.

2.7. Network Attack Defense

Modul Network Attack Defense se spoléhá na technologii Bitdefender zaměřenou na detekci síťových útoků určených k získávání přístupu ke koncovým bodům pomocí specifických technik, jako jsou: přímé útoky, zneužití sítě, odcizení hesla, Infekce vektory, roboty a trojskými koňmi.

2.8. Patch Management

Plně integrovaný v GravityZone, modul Patch Management udržuje operační systémy a softwarové aplikace aktuální, a poskytuje souhrnný přehled o stavu oprav na vašich koncových bodech s Windows.

Modul GravityZone Správa aktualizací zahrnuje několik funkcí, jako je skenování aktualizací na vyžádání / plánované, automatické / manuální opravy, nebo hlášení chybějících oprav.

Více informací o výrobcích a produktech podporovaných GravityZone Správou aktualizací se můžete dočíst v tomto KB článku.

Poznámka
Modul Patch Management e doplněk, který je dostupný společně se samostatným licenčním klíčem pro všechny dostupné licenční balíčky GravityZone.

2.9. Kontrola zařízení

Modul Device Control umožňuje prevenci úniku citlivých dat a malwarových infekcí skrze externí zařízení připojená ke koncovým bodům pomocí aplikování pravidel pro blokování a výjimky prostřednictvím politik pro širokou škálu typů zařízení (jako jsou flash disky USB, zařízení Bluetooth, přehrávače CD/DVD, paměťová zařízení, atd.).

2.10. Šifrování celého disku

Tato ochranná vrstva umožňuje poskytovat úplné šifrování na koncových bodech pomocí správy nástroje BitLocker ve Windows a FileVault a na macOS. Můžete šifrovat a dešifrovat bootovatelné a nebootovatelné svazky pouze několika kliky, zatímco GravityZone se stará o celý proces, s minimálním zásahem od uživatelů. GravityZone má uložené klíče pro obnovu, potřebné k odemčení svazku v případě, že uživatelé zapomenou své heslo.

Poznámka
Modul Full Disk Encryption je doplněk, který je dostupný pro všechny verze GravityZone ve formě separátního licenčního klíče.

2.11. Security for Exchange

Bitdefender Security for Exchange poskytuje filtrování proti malwaru, spamu, phishingu a filtrování příloh a obsahu, které je hladce zakomponované do Microsoft Exchange Serveru, a zajišťuje tak bezpečné posílání zpráv a prostředí spolupráce, čímž zvyšuje produktivitu. Díky oceňovaným antimalwarovým a antispamovým technologiím chrání uživatele Exchange proti tomu nejnovějšímu, nejpropracovanějšímu malwaru a proti pokusům o krádež důvěrných a cenných uživatelských údajů.

Důležité
Security for Exchange je určen k ochraně celé Exchange, ke které patří chráněný Exchange Server. To znamená, že chrání všechny aktivní poštovní schránky, včetně uživatele/prostoru/zařízení/sdílených poštovních schránek.
Kromě ochrany Microsoft Exchange zahrnuje licence také moduly ochrany koncových bodů instalované na serveru.

2.12. Kontrola aplikací

Modul Kontrola aplikací chrání před malwarem, útoky zero-day a posiluje zabezpečení, aniž by měla vliv na výkonnost. Kontrola aplikací zavádí pružná pravidla pro whitelisting aplikací, která identifikují a brání v instalaci a spouštění všech nežádoucích, nedůvěryhodných nebo škodlivých aplikací.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer poskytuje silnou ochrannou vrstvu proti pokročilým hrozbám díky tomu, že provádí automatickou hloubkovou analýzu podezřelých

souborů, které ještě nejsou v signaturách antimalwarové ochrany Bitdefender. Karanténa využívá rozsáhlou sadu technologií Bitdefender k provádění užitečného zatížení v uzavřeném virtuálním prostředí hostovaném společností Bitdefender nebo při lokálním nasazení, analyzuje jejich chování a hlásí jakékoli jemné systémové změny, které svědčí o zákeřném záměru.

Sandbox Analyzer používá řadu senzorů k detonaci obsahu ze spravovaných endpointů, toků síťového provozu, centralizované karantény a serverů ICAP.

Kromě toho Sandbox Analyzer umožňuje ruční odesílání prostřednictvím API.

Poznámka
Funkčnost těchto modulů může být zajištěna pomocí Sandbox Analyzer Cloud a Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises je dostupný pouze se separátním licenčním klíčem

2.14. Systém detekce hrozeb a následných opatření pro ochranu koncových bodů (Endpoint Detection and Response (EDR))

EDR je komponenta korelující události, schopná identifikovat pokročilé hrozby a nebo probíhající útoky. Jakožto součást komplexní a plně integrované platformy pro ochranu koncových bodů, EDR přináší společnou inteligenci pro všechna zařízení napříč vaší firemní sítí. Toto řešení přichází pomoci vašemu týmu bezepečnostních specialistů při řešení incidentů a pomáhá jim tak v úsilí při investigacích a také s odpovědmi na pokročilé hrozby.

Skrze Bitdefender Endpoint Security Tools klienta, si můžete na vámi spravovaných koncových bodech aktivovat ochranný modul zvaný EDR Senzor, abyste mohli schraňovat data z jejich hardware a z jejich operačních systémů. Následně díky klient-server struktuře systému, jsou metadata schraňována a zprocesovávaná na obou stranách.

Tato komponenta (vrstva ochrany) přináší datailní informaci o detekovaných hrozbách, interaktivní mapu incidentů, následných akcí oprav a integraci s komponentami (vrstvami ochrany)Sandbox Analyzer a HyperDetect.

2.15. Hypervisor Memory Introspection (HVI)

Je známé, že vysoce organizovaní, profit vyhledávající útočníci hledají neznámé zranitelnosti (zero-day zranitelnosti) nebo používají jednorázové útoky, účelně

vystavěné exploity (zero-day exploity) a jiné nástroje. Útočníci používají také pokročilé způsoby pro pozdržení a dávkování zatížení útoků tak, aby maskovali podezřelou činnost. Nové, ziskem motivované útoky jsou navrženy tak, aby byly nenápadné a dokázaly prorazit tradiční bezpečnostní nástroje.

Pro virtualizovaná prostředí je problém nyní vyřešen, HVI chrání datacentra s vysokou koncentrací virtuálních strojů proti pokročilým a sofistikovaným hrozbám, se kterými si stroje založené na signaturách neumí poradit. Prosazuje silnou izolaci a zajišťuje tak detekci útoků v reálném čase, blokuje je hned ve chvíli jejich výskytu a okamžitě odstraňuje hrozby.

Ať je chráněný stroj Windows nebo Linux, sever nebo počítač, HVI poskytuje vhled na úrovni, které je nemožné dosáhnout na hostujícím operačním systému. Stejně jako hypervizor kontroluje přístup k hardwaru za každý hostující virtuální stroj, HVI má důvěrnou znalost jak ohledně uživetelského režimu, tak kernel režimu v paměti hosta. Výsledkem je, že HVI má kompletní vhled do paměti hosta, a tím pádem do veškerého kontextu. Zároveň je HVI izolovaný od chráněných hostů, stejně jako je izolovaný samotný hypervizor. Tím, že operuje na úrovni hypervizoru a využívá hypervizorové funkce, HVI překonává technologické výzvy tradiční bezpečnosti pro odhalení škodlivé činnosti v datových centrech.

HVI rozpoznává spíše útočné techniky, než jejich vzorce. Tímto způsobem je technologie schopna rozpoznávat, hlásit a zabraňovat běžným metodám zneužívání. Jádro je chráněno proti technikám rootkit hookingu, které jsou využívány během útočného řetězce (attack kill chain) útoku pro jeho nenápadnost. Uživatelské operace jsou také chráněné před infikováním kódu, funkce detouring a provedení kódu ze stack nebo haldy

Poznámka
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

2.16. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) je řešení pro zabezpečení sítě, které analyzuje datové toky protokolu IPFIX na přítomnost škodlivého chování a škodlivého softwaru.

Bitdefender NTSA má sloužit vedle stávajících bezpečnostních opatření jako doplňková ochrana, která je schopna pokrýt slepá místa, která tradiční nástroje nemonitorují.

Tradiční nástroje pro zabezpečení sítě se obecně pokoušejí zabránit infekcím malwarem kontrolou příchozího provozu (přes sandbox, firewally, antivirové programy atd.). Bitdefender NTSA se zaměřuje výhradně na monitorování odchozího provozu sítě a zjišťuje podezřelé chování.

2.17. Security for Storage

GravityZone Security for Storage dodává ochranu v reálném čase pro vedoucí systémy pro sdílení souborů (file-sharing systems) a systémy síťových úložišť (network-storage systems). Aktualizace algoritmu pro detekci hrozeb probíhá automaticky - aniž by od vás bylo třeba vynaložit jakékoli úsilí a bez jakéhokoliv narušení činnosti koncových uživatelů.

Dva či více GravityZone Security Serverů Multi-Platform spolu tvoří roli ICAP serveru dodávajícího antimalware služby pro síťová uložiště (NAS) a také pro řešení pro sdílení souborů (file-sharing solutions) kompatibilních s Internet Content Adaptation Protokolem (ICAP, jak je definováno v RFC 3507).

Jakmile uživatel požádá o otevření, přečtení, zapsání, nebo zavření souboru z laptopu, pracovnístanice, mobilu, nebo jiného zařízení, tak pošle ICAP klient (tzn. NAS nebo systém pro sdílení souborů) požadavek na proskenování na Security Server a následně přijme verdikt (rozhodnutí o závadnosti) ohledně souboru. V závislosti na výsledku, Security Server povolí přístup, zamezí v přístupu a nebo smaže soubor.

Poznámka
Tento modul je dostupný jako doplněk se samostatným licenčním klíčem.

2.18. Security for Mobile

Na celopodnikové úrovni spojuje zabezpečení s managementem a kontrolou souladu pro zařízení iPhone, iPad a Android díky spolehlivé distribuci softwaru a aktualizací prostřednictvím trhu Apple a Android. Řešení bylo navrženo tak, aby umožnilo kontrolované přijetí iniciativ bring-your-own-device (BYOD) díky tomu, že setrvale prosazuje práva používání na všech přenosných zařízeních. Bezpečnostní funkce zahrnují zámek obrazovky, autentizační kontrolu, polohu zařízení, vymazání na dálku, detekci zařízení s rootem nebo jailbreakem a bezpečnostní profily. Pro zařízení Android je bezpečnostní úroveň zvýšena o skenování v reálném čase a šifrování vyměnitelných médií. Ve výsledku máte mobilní zařízení pod kontrolou a citlivé obchodní údaje uložené na zařízení jsou chráněny.

2.19. Dostupnost ochranných vrstev GravityZone

Dostupnost ochranných vrstev GravityZone se liší podle operačního systému koncového bodu. Další informace naleznete v článku GravityZone Protection Layers Availability.

3. ARCHITEKTURA GRAVITYZONE

Jedinečná architektura GravityZone mu umožňuje snadné přizpůsobení se a zabezpečení pro libovolný počet systémů. GravityZone lze nastavit tak, aby využívala více virtuálních zařízení a několika určitých rolí (databáze, komunikační server, aktualizační server a webová konzole) pro zajištění spolehlivosti a přizpůsobitelnosti.

Každá role může být nainstalována na jiném zařízení. Zabudované vyrovnávače rovnováhy rolí ručí za to, že zavedení GravityZone ochrání i ty nejrozsáhlejší podnikové sítě, aniž by způsobovala zpomalení nebo překážky. Místo vestavěného vyrovnávače rovnováhy lze použít i již existující software nebo hardware pro vyrovnání rovnováhy zatížení, pokud je přítomný síti.

Jelikož je GravityZone dodávána formou virtuálního kontejneru (virtuálního stroje), tak může být naimportována a spuštěna na prakticky kterékoliv virtualizační platformě, včetně VMware, Citrix, Microsoft Hyper-V a Nutanix Prism, Microsoft Azure.

Integrace s VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element a Microsoft Azure snižuje úsilí nutné pro nasazení ochrany na fyzických a virtuálních koncových strojích.

Řešení GravityZone obsahuje následující komponenty:

- Virtuální zařízení GravityZone
- Security Server
- Doplňkový balíček HVI
- Bezpečnostní agenty

3.1. GravityZone VA

GravityZone on-premise řešení je dodáváno jako Linuxová (Ubuntu) samokonfigurovatelná vytvrzená (hardened) virtuální appliance (VA), která je vnořená do obrazu virtuálního stroje a je jednoduše instalovatelná a konfigurovatelná pomocí CLI (Command Line Interface). Virtuální zařízení je dostupné v několika formátech, kompatibilních s hlavními virtualizačními platformami (OVA, XVA, VHD, OVF, RAW).

3.1.1. Databáze GravityZone

Centrální logika architektury GravityZone. Bitdefender používá nerelační databázi MongoDB, kterou lze snadno přizpůsobit a replikovat.

3.1.2. Aktualizační server GravityZone

Aktualizační server hraje důležitou roli v aktualizaci řešení GravityZone a agentů koncových bodů tak, že replikuje a vydává potřebné balíčky nebo instalační soubory.

3.1.3. Komunikační server GravityZone

Komunikační server je spojení mezi bezpečnostními agenty a databází, který přenáší pravidla a příkazy na chráněné koncové body ,a také události hlášené bezpečnostními agenty.

3.1.4. GravityZone Incident Server

Incident Server je spojením mezi agenty zabezpečení a databází, shromažďováním dat koncových bodů a generováním incidentů na základě hrozeb detekovaných preventivními technologiemi a algoritmy strojového učení.

3.1.5. Webovou konzoli (GravityZone Control Center)

Bezpečnostní řešení Bitdefender jsou spravovány z jediného správního bodu, webové konzole Control Center. Tímto je umožněna snadnější správa a přístup k celkovému bezpečnostnímu postoji, globálním bezpečnostním hrozbám a kontrole nad všemi bezpečnostními moduly, které chrání virtuální nebo fyzické počítače, servery a přenosná zařízení. Poháněna architekturou Gravity, Control Center je schopna naplnit potřeby i těch největších organizací.

Control Center se integruje s existujícími systémy správy a monitorovacími systémy, tak aby to bylo co nejjednodužší automaticky aplikuje ochranu na nespravované pracovní stanice , servery nebo mobilní zařízení, které se objevují v Microsoft Active Directory, VMware vCenter, Nutanix Prism Element nebo Citrix XenServer systémech nebo které jsou jednoduše detekovány v síti.

3.2. Security Server

Security Server je specializovaný virtuální stroj, který reduplikuje a centralizuje většinu antimalwarových funkcí antimalwarových agentů a funguje jako skenovací server.

Existují tři verze Security Server, pro každý typ virtualizačního prostředí:

- **Security Server pro VMware NSX.** Tato verze se automaticky instaluje na každého hostitele ve svazku, kde byl zaveden Bitdefender.
- **Security Server pro VMware vShield Endpoint.** Tuto verzi je nutné nainstalovat na každého hostitele, aby byl chráněn.
- **Security Server Multi-Platform.** Tato verze je pro další různá virtualizovaná prostředí a musí být nainstalována na jednom nebo více hostech, aby se přizpůsobila počtu chráněných virtuálních strojů. Při používání HVI, Security Server musí být nainstalován na každém hostu, který obsahuje virtuální stroje, které mají být chráněny.

3.3. Doplňkový balíček HVI

Balíček HVI zajišťuje spojení mezi hypervizorem a Security Server na daném hostu. Tímto způsobem je Security Server schopný monitorovat paměť využívanou na hostiteli, na kterém je nainstalován, na základě bezpečnostních pravidel GravityZone.

Poznámka
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

3.4. Bezpečnostní agenty

Pro ochranu vaší sítě pomocí Bitdefender, musíte nainstalovat vhodné bezpečnostní agenty GravityZone na koncové síťové body.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.4.1. Bitdefender Endpoint Security Tools

GravityZone zajišťuje fyzickým a virtuálním strojům ochranu pomocí Bitdefender Endpoint Security Tools, inteligentního bezpečnostního agenta, který rozpozná prostředí, a adaptuje se podle typu koncového bodu. Bitdefender Endpoint Security Tools může být nasazen na jakékoli zařízení, virtuální nebo fyzické, poskytuje flexibilní skenovací systém a je ideální volbou pro smíšená prostředí (fyzická, virtuální a cloudová).

Kromě souborové ochrany systému Bitdefender Endpoint Security Tools obsahuje také mail server ochranu pro Microsoft Exchange Servers.

Bitdefender Endpoint Security Tools používá jednu šablonu zásad pro fyzické a virtuální počítače a jeden zdroj instalační sady pro jakékoli prostředí (fyzické nebo virtuální) se systémem Windows.

Úroveně ochrany

S klientem Bitdefender Endpoint Security Tools jsou dostupné následující ochranné vrstvy:

- Antimalware
- Pokročilá ochrana před hrozbami (ATC)
- HyperDetect
- Firewall
- Kontrola obsahu
- Network Attack Defense
- Patch Management
- Kontrola zařízení
- Šifrování celého disku
- Security for Exchange
- Sandbox Analyzer
- Systém detekce hrozeb a následných opatření pro ochranu koncových bodů (Endpoint Detection and Response (EDR))
- Kontrola aplikací

Role koncových bodů

- Pokročilý uživatel
- Relay
- Patch Caching Server
- Exchange Ochrana

Pokročilý uživatel

Administrátoři centrální správy mohou udělit práva pokročilého uživatele uživatelům koncových bodů skrze nastavení politik. Modul Pokročilý uživatel aktivuje administrátorská práva na uživatelské úrovni, čímž umožní uživateli koncového bodu přístup a možnost úpravy bezpečnostních nastavení prostřednictvím lokální konzole. Control Center dostává hlášení, když je koncový uživatel v módu

Pokročilého uživatele a správce Control Center může přepsat místní bezpečnostní nastavení.

Důležité
Tento modul je dostupný pouze pro počítače a servery s podporovaným systémem Windows. Více informací naleznete v instalačním průvodci GravityZone.

Relay

Agenti koncových bodů s rolí Bitdefender Endpoint Security Tools Relay slouží jako komunikační proxy a aktualizační servery pro ostatní koncové body v síti. Agenti koncových bodů s rolí relay jsou nezbytní zvláště v organizacích s izolovanými sítěmi, kde veškerý přenos probíhá skrze jediný přístupový bod.

Ve společnostech s velkými distribuovanými sítěmi, relay agenti napomáhají snížení využití šířky pásma tím, že brání chráněným koncovým bodům a bezpečnostním serverům v komunikaci napřímo s zařízením GravityZone.

Jakmile je agent Bitdefender Endpoint Security Tools Relay nainstalovaný v síti, ostatní koncové body mohou být nastaveny pomocí pravidel pro komunikaci s Control Center prostřednictvím relay agenta.

Agenti Bitdefender Endpoint Security Tools Relay slouží k následujícím účelům:

- Odhalení všech nechráněných koncových bodů v síti.
- Nasazení agenta na koncový bod v rámci místní sítě.
- Aktualizace chráněných koncových bodů v síti.
- Zajištění komunikace mezi Control Center a připojenými koncovými body.
- Role proxy serveru pro chráněné koncové body.
- Optimalizace síťového přenosu během aktualizací, nasazení, skenování a dalších zátěžových úkolů.

Patch Caching Server

Koncové body s funkcí relay mohou také sloužit jako server pro aktualizaci programového vybavení. Je-li tato funkce povolena, Relay ukládá softwarové aktualizace stažené ze stránek prodejců, a distribuuje je do cílových koncových bodů ve vaší síti. Jakmile je na připojeném koncovém bodě se objeví software s chybějícími aktualizacemi, stáhne si je ze serveru a ne ze stránek prodejce, čímž optimalizuje vzniklý přenos a zatížení šířky pásma.

Důležité
Tato přídatná funkce je dostupná s registrovaným doplňkem Správa oprav.

Exchange Ochrana

Bitdefender Endpoint Security Tools s Exchange rolí může být nainstalován na Microsoft Exchange servery pro ochranu uživatelů Exchange před hrozbami skrytými v emailech.

Bitdefender Endpoint Security Tools s rolí Exchange chrání jak samotný server, tak řešení Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac je bezpečnostní agent vytvořený k ochraně pracovním stanic a laptopů s Macintosh OS postavených na platformě Intel. Dostupná technologie skenování je dostupná **Místní skenování** s lokálně uloženým obsahem zabezpečení.

Úroveně ochrany

Následující ochranné vrstvy jsou dostupné na Endpoint Security for Mac:

- Antimalware
- Pokročilá ochrana před hrozbami (ATC)
- Kontrola obsahu
- Kontrola zařízení
- Šifrování celého disku

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client snadno rozšiřuje bezpečnostní pravidla na jakýkoli počet zařízení s Android nebo iOS, a tak je chrání proti neoprávněnému využívání, riskwaru nebo ztrátě důvěrných dat. Bezpečnostní funkce zahrnují zámek obrazovky, autentizační kontrolu, polohu zařízení, vymazání na dálku, detekci zařízení s rootem nebo jailbreakem a bezpečnostní profily. Pro zařízení Android je bezpečnostní úroveň zvýšena o skenování v reálném čase a šifrování vyměnitelných médií.

GravityZone Mobile Client je distribuován exkluzivně prostřednictvím Apple App Store a Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools je lehký agent pro virtualizovaná prostředí VMware integrovaných s vShield Endpoint. Bezpečnostní agent se nainstaluje na virtuální stroje chráněné

Security Serverem a vy díky tomu můžete využívat výhod přídatných funkcí, které poskytuje:

- Umožňuje vám spouštět úlohy Skenování paměti a Skenování procesů na zařízení.
- Informuje ostatní uživatele o nalezených infekcích a akcích, které na nich byly provedeny.
- Přidá více možností pro výjimky z antimalwarového skenování.

3.5. Sandbox Analyzer Architektura

Bitdefender Sandbox Analyzer poskytuje silnou ochrannou vrstvu proti pokročilým hrozbám díky tomu, že provádí automatickou hloubkovou analýzu podezřelých souborů, které ještě nejsou v signaturách antimalwarové ochrany Bitdefender.

Sandbox Analyzer je k dispozici ve dvou variantách:

- Sandbox Analyzer Cloud, hostovaný Bitdefender.
- Sandbox Analyzer On-Premises, je k dispozici jako virtuální appliance, které lze nasadit lokálně.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud obsahuje následující komponenty:

- **Portál Sandbox Analyzer** - hostovaný komunikační server, užívaný pro zpracování požadavků mezi koncovými body a sandbox clusterem Bitdefender.
- **Sandbox Analyzer Cluster** - hostovaná sandboxová infrastruktura, ve které probíhá behaviorální analýza. Na této úrovni jsou podané soubory detonovány na virtuálních strojích s operačním systémem Windows 7.

GravityZone Control Center funguje jako konzole pro správu a reporting, kde nastavujete politiky zabezpečení a zobrazujete analytické zprávy a oznámení.

Bitdefender Endpoint Security Tools,bezpečnostní agent nainstalovaný na koncových bodech funguje jako datový sensor pro Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises je dodáván jako virtuální Linux Ubuntu zařízení zabudované do image virtuálního stroje. Snadno se instaluje a konfiguruje pomocí rozhraní příkazového řádku (CLI). Sandbox Analyzer On-Premises je k dispozici ve formátu OVA a lze jej nasadit na VMWare ESXi.

Sandbox Analyzer On-Premises obsahuje následující komponenty:

- **Sandbox Manager**. Tato komponenta je sandbox orchestrator. Sandbox Manager se připojuje k hypervizoru ESXi přes API a používá tyto hardwarové prostředky k vytváření a provozu prostředí pro analýzu malwaru.
- **Detonační virtuální stroje** . Tato součást se skládá z virtuálních strojů využívaných programem Sandbox Analyzer ke spouštění souborů a analýze jejich chování. Detonační virtuální stroje mohou spouštět 64bitové operační systémy Windows 7 a Windows 10.

GravityZone Control Center funguje jako konzole pro správu a reporting, kde nastavujete politiky zabezpečení a zobrazujete analytické zprávy a oznámení.

Sandbox Analyzer On-Premises pracuje s následujícími senzory:

- **Sensor koncového bodu** . Bitdefender Endpoint Security Tools pro Windows funguje jako dodávající senzor nainstalovaný na koncových bodech. Agent Bitdefender používá pokročilé strojové učení a algoritmy neuronové sítě k určení podezřelého obsahu a jeho odeslání do Sandbox Analyzer, včetně objektů z centralizované karantény.
- **Síťový senzor (Network sensor)**. Network Security Virtual Appliance (NSVA) je virtuální zařízení, které lze nasadit ve stejném virtualizovaném prostředí ESXi jako instanci Sandbox Analyzer. Síťový sensor získává obsah ze síťových toků a odešle jej do Sandbox Analyzer.
- **ICAP sensor**. Nasazeno na síťových úložných zařízeních (NAS) pomocí protokolu ICAP, Bitdefender Security Server podporuje odesílání obsahu do Sandbox Analyzer.

Kromě těchto senzorů Sandbox Analyzer On-Premises podporuje ruční odesílání a prostřednictvím API. Podrobnosti viz **Použití Sandbox Analyzer** kapitola v GravityZone administrátorském průvodci.

4. ZAČÍNÁME

Řešení GravityZone lze nastavit a spravovat prostřednictvím sjednocené správní platformy zvané Control Center. Control Center má webové rozhraní, ke kterému můžete přistupovat pomocí uživatelského jména a hesla.

4.1. Připojování se k Control Center

Přístup k Control Center je umožněn prostřednictvím uživatelských účtů. Email se svými přihlašovacími údaji obdržíte po založení účtu.

Podmínky:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Doporučené rozlišení monitoru: 1280 x 800 nebo vyšší

Varování
Control Center nebude pracovat / zobrazovat se správně v Internet Exploreru 9+ se zapnutou funkcí kompatibility zobrazení (Compatibility View feature enabled), což se rovná defakto použití nepodporované verze prohlížeče.

Pro připojení se k Control Center:

1. Do pole pro adresu ve svém webovém prohlížeči zadejte IP adresu nebo DNS hostitelské jméno zařízení Control Center (s prefixem `https://`).
2. Zadejte své uživatelské jméno a heslo.
3. Zadejte šestimístný kód od Google Authenticator, Microsoft Authenticator nebo libovolného dvoufaktorového autentizátoru TOTP (Time-Based One-Time Password Algorithm) - kompatibilní se standardem RFC6238. Více informací naleznete na „Správa vašeho účtu “ (str. 24).
4. Klikněte na **Přihlásit se**.

Při prvním přihlášení musíte souhlasit se smluvními podmínkami Bitdefender. Klepnutím na **Pokračovat** začněte používat GravityZone.

Poznámka
Pokud jste zapomněli své heslo, použijte odkaz pro obnovení hesla a obdržíte nové. Musíte uvést emailovou adresu svého účtu.

4.2. Nahlédnutí do Control Center

Control Center je zorganizována tak, aby umožnila snadný přístup ke všem funkcím. Použijte panel nabídky na pravé straně pro navigaci konzolí. Dostupné funkce závisí na typu uživatele přihlášeného ke konzoli.

Kontrolní panel

4.2.1. Přehled Control Center

Uživatelé s rolí správce společnosti mají plná oprávnění nad konfigurací Control Center a bezpečnostním nastavením sítě, zatímco uživatelé s rolí správce mají přístup k funkcím síťového zabezpečení včetně správy uživatelů.

Použijte tlačítko **Zobrazit nabídku** v levém horním rohu, chcete-li se rozbalit, skrýt nebo ukázat možnosti nabídky. Kliknutím na tlačítko postupně procházíte možnostmi nebo dvojitým kliknutím je přeskočíte.

V závislosti na Vaší roli můžete mít přístup k následujícím možnostem nabídky:

Kontrolní panel
Prohlížejte snadno čitelné grafy s klíčovými informacemi o zabezpečení vaší sítě.

Incidenty
Prohlížet a spravovat bezpečnostní incidenty napříč firemmní sítí.

Síť
Instalovat zabezpečení, aplikovat pravidla, spravovat bezpečnostní nastavení, spouštět úlohy na dálku a vytvářet rychlá hlášení.

Pravidla
Vytvořte a spravujte bezpečnostní pravidla.

Reporty
Získejte přehledy o zabezpečení spravovaných klientů.

Karanténa
Spravujte soubory v karanténě na dálku.

Účty
Spravujte přístup ostatních zaměstnanců společnosti ke Control Center.

V tomto menu naleznete také stránku **Aktivita uživatelů**, která umožňuje přístup k protokolu o činnosti uživatele.

> **Poznámka**
> Tato nabídka je k dispozici pouze uživatelům s oprávněním **Spravovat uživatele**.

Konfigurace

Konfigurujte nastavení Control Center, jako je poštovní server, integrace s Active Directory nebo virtualizačními prostředí, bezpečnostní certifikáty a nastavení síťového inventáře, včetně naplánovaných pravidel pro automatické vyčištění nepoužitých virtuálních strojů.

> **Poznámka**
> Tato nabídka je k dispozici pouze uživatelům s oprávněním **Spravovat řešení**.

Kliknutím na své uživatelské jméno v pravém horním rohu konzole se vám zpřístupní následující možnosti:

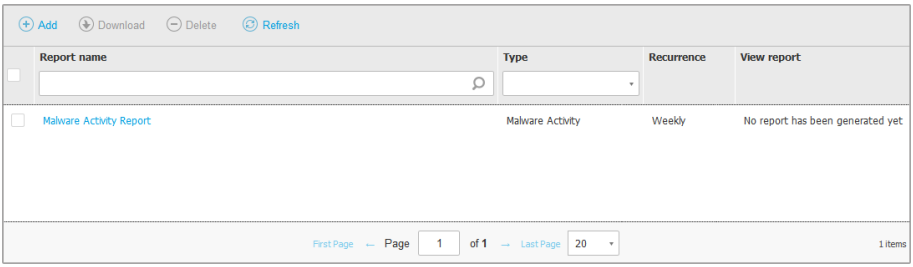
- **Můj účet**. Klikněte na tuto možnost pro správu podrobností a preferencí vašeho uživatelského účtu.
- **Správce pověření**. Klikněte na tuto možnost pro přidání a správu autentizačních pověření nezbytných pro vzdálené instalační úlohy.
- **Nápověda & podpora**. Klikněte na tuto možnost pro získání informací o pomoci a podpoře.
- **Zpětná vazba**. Klikněte na tuto možnost a zobrazí se formulář, přes který můžete upravit a odeslat své zprávy se zpětnou vazbou ohledně vašich zkušeností při práci s GravityZone.
- **Odhlásit se**. Klikněte na tuto možnost pro odhlášení se ze svého účtu.

Navíc, v pravém horním rohu konzole naleznete:

- Ikonu **Pomocný režim**, který zapne rozšiřitelná okna s tipy ohledně nástrojů na položkách Control Center. Můžete snadno získat užitečné informace ohledně funkcí Control Center.
- Ikonu **Upozornění**, která poskytuje snadný přístup k upozorněním a také ke stránce **Upozornění**.

4.2.2. Tabulkové údaje

Tabulky jsou často využívány napříč konzolí pro organizaci dat do snadno ovladatelného formátu.



Stránka s Hlášení

Procházet stránkami

Tabulky s více než 20 položkami zabírají několik stran. Ve výchozím stavu se zobrazuje pouze 20 položek na stránku. Pro pohyb mezi stránkami použijte navigační tlačítka ve spodní části tabulky. Počet položek zobrazených na stránku můžete změnit tak, že vyberete jinou možnost z menu umístěného vedle navigačních tlačítek.

Vyhledávání konkrétních položek

Pro snadné nalezení konkrétních položek použijte vyhledávací pole umístěné pod hlavičkami sloupců.

Zadejte hledaný termín do odpovídajícího pole. Zatímco píšete, odpovídající položky se zobrazují v tabulce. Pro obnovení obsahu tabulek smažte vyhledávací pole.

Třídění údajů

Pro třízení údajů podle konkrétního sloupce, klikněte na hlavičku sloupce. Pro otočení pořadí řazení klikněte znovu na hlavičku sloupce.

Aktualizace tabulkových údajů

Pro jistotu, že tabulka zobrazuje nejnovější informace, klikněte na tlačítko **Obnovit** v horní části tabulky.

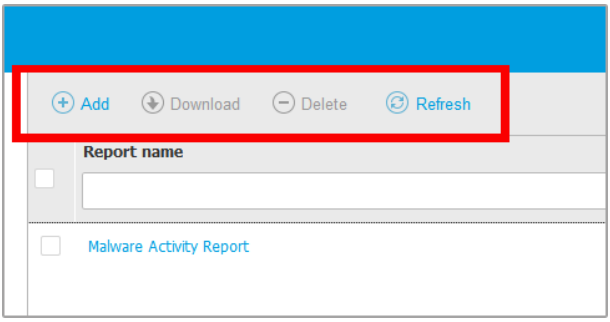
Toto může být potřeba, když na stránce strávíte více času.

4.2.3. Panely nástrojů

V Control Center, akční panely nástrojů vám umožňují provádět specifické operace vztahující se k sekci, ve které se zrovna nacházíte. Každý panel nástrojů se skládá

ze sady ikon, která je obvykle umístěna v horní části tabulky. Například, akční panel nástrojů v sekci **Hlášení** vám umožňuje provádět následující činnosti:

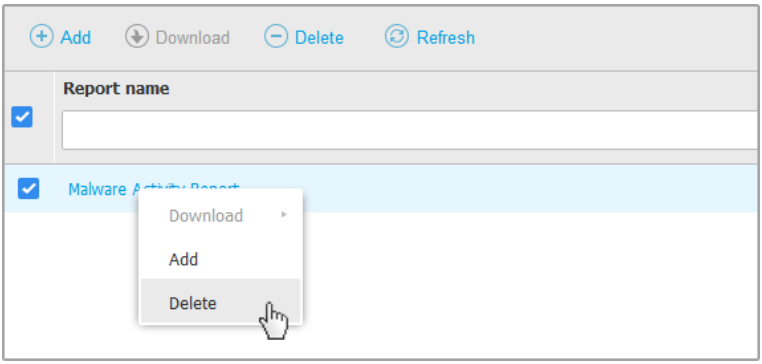
- Vytvořte nové hlášení.
- Stáhnout naplánované hlášení.
- Smazat naplánované hlášení.



Stránka Hlášení - akční panel nástrojů

4.2.4. Kontextové menu

Příkazy akčního panelu nástrojů jsou dostupné také z kontextového menu. Klikněte pravým tlačítkem na právě používanou sekci Control Center a ze seznamu zvolte potřebný příkaz.



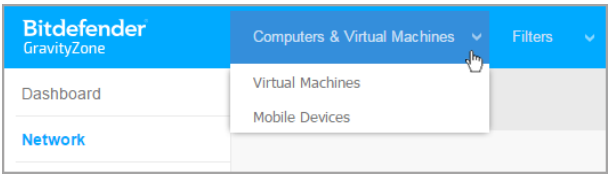
Stránka Hlášení - kontextové menu

4.2.5. Výběr zobrazení

Pokud pracujete s různými typy koncových bodů, můžete je najít seřazené podle typu na stránce **Síť** pod několika síťovými zobrazeními:

- **Počítače & a Virtuální stroje**: zobrazuje skupiny a počítače Active Directory, a také fyzické a virtuální pracovní stanice mimo Active Directory, které jsou nalezeny v síti.
- **Virtuální stroje**: zobrazuje infrastrukturu virtuálního prostředí integrovaného s Control Center a všechny obsažené virtuální stroje.
- **Mobilní zařízení**: zobrazuje uživatele a k nim přiřazená mobilní zařízení.

Pro zvolení požadovaného síťového zobrazení klikněte na nabídku zobrazení v pravém horním rohu stránky.



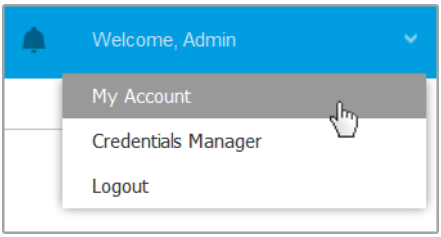
Výběr zobrazení

Poznámka
Uvidíte pouze koncové body, pro které máte oprávnění k prohlížení udělené správcem, který přidal vašeho uživatele k Control Center.

4.3. Správa vašeho účtu

Pro kontrolu a změnu údajů a nastavení vašeho účtu:

1. Klikněte na své uživatelské jméno v pravém horním rohu konzole a zvolte **Můj účet**.



Nabídka uživatelského účtu

2. Pod **Detaily účtu** opravte nebo aktualizujte informace o vašem účtu. Pokud používáte uživatelský účet Active Directory, nemůžete změnit detaily účtu.
   - **Uživatelské jméno.** Uživatelské jméno je jedinečný identifikátor uživatelského účtu a nelze ho změnit.
   - **Celé jméno.** Zadejte vaše celé jméno.
   - **E-mail.** Toto je vaše přihlašovací a kontaktní emailová adresa. Na tuto adresu jsou zasílána důležitá bezpečnostní upozornění. Emailová upozornění jsou odesílána automaticky kdykoliv jsou ve vaší síti zjištěny rizikové podmínky.
   - Odkaz **Změnit heslo** vám umožní změnit vaše přihlašovací heslo.
3. V **Nastavení** můžete konfigurovat nastavení účtu podle svých preferencí.
   - **Časová zóna.** Z nabídky zvolte časovou zónu svého účtu. Konzole bude zobrazovat časové údaje odpovídající zvolené časové zóně.
   - **Jazyk.** Z nabídky zvolte jazyk konzole.
   - **Časový limit relace.** Zvolte časový interval nečinnosti předtím, než vaše uživatelská relace vyprší.
4. V části **Zabezpečení přihlášení** nakonfigurujte dvoufaktorové ověřování a zkontrolujte stav dostupných zásad pro zabezpečení vašeho účtu GravityZone. Zásady platné pro celou společnost jsou jen pro čtení.

   Pro zapnutí dvoufaktorového ověření:

   a. **Dvoufaktorové ověřování.** Dvoufaktorové ověřování přidává do vašeho účtu GravityZone další vrstvu zabezpečení tím, že vyžaduje kromě vašeho Control Center pověření také autentikační kod.

      Při prvním přihlášení k účtu GravityZone budete vyzváni ke stažení a instalaci aplikace Google Authenticator, Microsoft Authenticator nebo libovolného dvoufaktorového TOTP (Time-Based One-Time Password Algorithm). autentizátor - kompatibilní se standardním RFC6238 na mobilním zařízení,

propojte jej se svým účtem GravityZone a poté jej použijte s každým Control Center Přihlášením. Google Authenticator generuje šestimístní kód každých 30 vteřin. Pro dokončení přihlášení se do Control Center budete muset po zadání hesla poskytnout šestimístný kód z Google Authenticatoru.

Poznámka
Tento proces můžete přeskočit třikrát, poté se nebudete moci přihlásit bez dvoufaktorové autentizace.

Pro zapnutí dvoufaktorového ověření:

i. Klikněte na tlačítko **Povolit** ve zprávě **Dvoufaktorové ověřování** .

ii. V dialogovém okně kliknutím na příslušný odkaz stáhněte a nainstalujte aplikaci Google Authenticator do svého mobilního zařízení.

iii. Otevřete Google Authenticator na vašem mobilním zařízení.

iv. Na obrazovce **Přidat účet**, oskenujte QR kód pro připojení aplikace k vašemu GravityZone účtu.

Klíč můžete zadat i ručně.

Tato činnost je vyžadována pouze jednou, pro zapnutí funkce v GravityZone.

Důležité
Ujistěte se, že jste si zkopírovali a uložili klíč na bezpečné místo. Klikněte **Vytiskněte zálohu** pro vytvoření PDF souboru s QR kódem a tajným klíčem. Pokud ztratíte nebo změníte zařízení užívané pro dvoufaktorovou autentizaci, budete muset nainstalovat Google Authenticator na nové zařízení, a zadat tajný klíč pro jeho připojení k vašemu GravityZone účtu.

v. Zadejte šestimístný kód do pole **Kód Google Authenticator**.

vi. Kkikněte na **Povolit** pro dokončení aktivace funkce.

Poznámka
Váš správce sítě může pro všechny účty GravityZone nastavit dvoufázové ověření. V tomto případě, budete tázán přihlásit se a nakonfigurovat vaší dvou fázovou autentizaci (2FA). Zároveň nebudete mít možnost deaktivovat 2FA ověření pro váš účet dokud je tato funkce vynucena vaším firemním administrátorem.

Uvědomte si, že pokud je momentálně pro váš účet 2FA vypnutá, tento tajný klíč nebude nadále platit.

b. **Zásady vypršení platnosti hesla.** Pravidelné změny hesla poskytují přidanou vrstvu ochrany před neoprávněným použitím hesel nebo omezují dobu neoprávněného použití. Je-li povoleno, GravityZone vyžaduje, abyste si své heslo změnili nejpozději do 90 dnů.

c. **Zásady blokování účtu.** Tyto zásady zabraňují přístupu k vašemu účtu po pěti po sobě jdoucích neúspěšných pokusech o přihlášení. Toto opatření má chránit před útoky brute-force.

   Chcete-li odemknout svůj účet, musíte si resetovat heslo z přihlašovací stránky nebo kontaktovat jiného správce GravityZone.

5. Kliknutím na tlačítko **Uložit** aplikujete změny.

Poznámka
Nemůžete odstranit svůj vlastní účet.

4.4. Změna přihlašovacího hesla.

Po vytvoření vašeho účtu obdržíte email s přihlašovacími údaji.

Pokud nepoužíváte pověření Active Directory pro přístup do Control Center, doporučujeme provést toto:

- Při první návštěvě Control Center změňte výchozí přihlašovací heslo.
- Pravidelně měňte své přihlašovací heslo.

Pro změnu hesla:

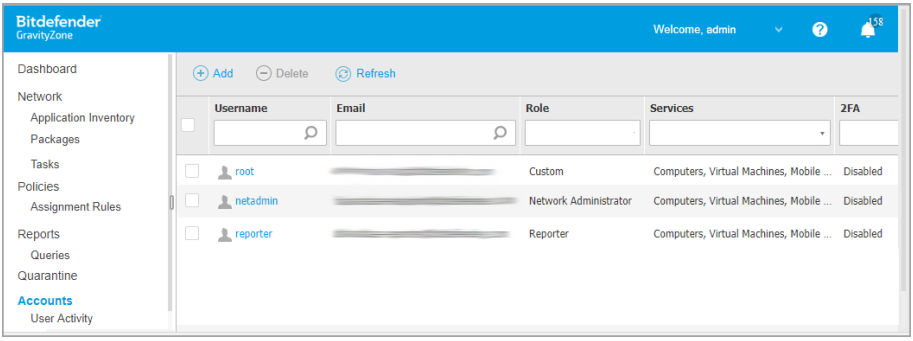
1. Klikněte na své uživatelské jméno v pravém horním rohu konzole a zvolte **Můj účet**.
2. V **Detaily účtu** klikněte na **Změnit heslo**.
3. Do příslušných polích zadejte své stávající a nové heslo.
4. Kliknutím na tlačítko **Uložit** aplikujete změny.

5. UŽIVATELSKÉ ÚČTY

Můžete vytvořit první uživatelský účet GravityZone během prvotního nastavení Control Center poté, co zavedete zařízení GravityZone. Prvotní uživatelský účet Control Center má roli správce společnosti s plnými právy nad konfigurací Control Center a správou sítě. Z tohoto účtu můžete vytvářet všechny ostatní uživatelské účty potřebné pro správu vaší firemní sítě.

To, co byste měli vědět o uživatelských účtech GravityZone:

- Chcete-li ostatním zaměstnancům společnosti umožnit přístup do Control Center, můžete si vytvořit uživatelské účty samostatně nebo povolit dynamický přístup pro více účtů prostřednictvím integrace Active Directory nebo přístupových pravidel. Můžete přiřadit uživatelské účty s různými rolemi, podle jejich přístupové úrovně ve společnosti.
- Pro každý uživatelský účet můžete nastavit přístup k funkcím GravityZone nebo k určitým částem sítě, ke které patří.
- Můžete spravovat pouze účty se stejnými nebo nižšími oprávněními, než jsou ta vaše.



Stránka Účty

V tabulce jsou zobrazeny existující účty. Pro každý uživatelský účet můžete prohlížet:

- Uživatelské jméno účtu (používané pro přihlášení se do Control Center).

- Emailová adresa účtu (používaná jako kontaktní adresa). Na tuto adresu jsou zasílána důležitá bezpečnostní upozornění. Emailová upozornění jsou odesílána automaticky kdykoliv jsou ve vaší síti zjištěny rizikové podmínky.
- Role uživatele (správce společnosti / správce sítě / bezpečnostní analytik / vlastní).
- Bezpečnostní služby GravityZone, které má uživatel právo spravovat (počítače, virtuální stroje, mobilní zařízení).
- Tento status 2FA (dvou-faktorové autentizace), umožňuje rychle zjistit jestli užiovatel má 2FA zapnutou.
- Stav pravidel přístupu indikuje uživatelský účet vytvoření pomocí pravidel oprávnění k přístupu. Ručně vytvořené uživatelské účty zobrazují **N/A**.

5.1. Uživatelské role

Uživatelská role se skládá ze specifické kombinace oprávnění uživatele. Při vytváření uživatelského účtu si můžete vybrat z předem definovaných rolí, nebo můžete vytvořit vlastní roli tak, že zvolíte pouze některá uživatelská práva.

Poznámka
Účtům můžete udělit se stejná nebo nižší oprávnění, než jsou ta vaše.

Dostupné jsou následující uživatelské role:

1. **Správce společnosti** - Obvykle je pro každou firmu vytvořen zvláštní uživatelský účet s rolí Správce společnosti, s plným přístupem ke všem funkcím pro správu řešení GravityZone. Správce společnosti nastavuje parametry Control Center, spravuje licenční klíče bezpečnostních služeb, spravuje uživatelské účty, a je oprávněn také ke správě bezpečnostních nastavení firemní sítě. Firemní administrátoři mohou své operační povinnosti sdílet nebo jimi pověřit podřízené účty administrátorů a bezpečnostních analytiků.
2. **Síťový administrátor** - Pro každou podřízenou firmu je možné vytvořit několik účtů s rolí Administrátora se správními výsadami nad celkovým zavedením bezpečnostních agentů jedné nebo více společností, nebo nad určitou skupinou koncových bodů, včetně správy uživatelů. Síťoví administrátoři jsou odpovědní za aktivní správu bezpečnostních nastavení sítě.
3. **Bezpečnostní Analytik** - Účet Bezpečnostní Analytik je účtem pouze pro čtení. Tyto povolí přístup pouze k datům spojeným se zabezpečením, reportům a

logům. Tyto účty mohou být přiděleny pouze osobám odpovědným za bezpečnostní monitoring nebo jiným zaměstnancům, kteří musí stále znát aktuální bezpečnostní status.

4. **Vlasní** - Předem definované uživatelské role obsahují určitou kombinaci uživatelských oprávnění. Pokud předem definovaná uživatelská role nevyhovuje vašim potřebám, můžete vytvořit vlastní účet tak, že vyberete pouze ta oprávnění, která vás zajímají.

Následující tabulka shrnuje vztahy mezi různými rolemi uživatelských účtů a jejich oprávnění. Podrobné informace viz „Oprávnění uživatele“ (str. 30).

Role účtu	Povolené dceřiné účty	Oprávnění uživatele
Správce společnosti	Administrátoři společnosti, Síťoví administrátoři, Bezpečnostní Analytici	Spravovat Řešení Spravovat společnost Správa uživatelů Správa sítí Zobrazit a analyzovat data
Síťový administrátor	Síťoví Administrátoři, Bezpečnostní Analytici	Správa uživatelů Správa sítí Zobrazit a analyzovat data
Bezpečnostní Analytici	-	Zobrazit a analyzovat data

5.2. Oprávnění uživatele

Uživatelským účtům GravityZone můžete přiřadit následující uživatelská práva:

- **Spravovat Řešení**. Umožňuje konfiguraci nastavení Control Center (poštovní server a nastavení proxy, integraci s Active Directory a virtualizačními platformami, bezpečnostní certifikáty a aktualizace GravityZone). Toto oprávnění je specifické pro účty firemních administrátorů.
- **Správa uživatelů**. Vytvářet, upravovat nebo mazat uživatelské účty.
- **Spravovat firmu**. Uživatelé mohou spravovat svůj vlastní licenční klíč GravityZone a upravovat profilová nastavení své firmy. Toto oprávnění je specifické pro účty firemních administrátorů.

- **Správa sítí**. Poskytuje správní oprávnění nad bezpečnostním nastavením sítě (síťový inventář, zásady, úlohy, instalační balíčky, karanténa). Toto oprávnění je specifické pro účty síťových administrátorů.
- **Zobrazit a analyzovat data**. Zobrazit události a logy související s bezpečností, spravovat reporty a nástěnku.

5.3. Správa uživatelských účtů

Chcete-li vytvářet, upravovat, odstraňovat a konfigurovat uživatelské účty, použijte následující metody:

- Individuální správa uživatelských účtů. Tuto metodu použijte k přidání místních uživatelských účtů nebo účtů služby Active Directory. Informace o integraci služby Active Directory naleznete v Instalačním průvodci GravityZone.

  Před vytvořením uživatelského účtu se ujistěte, že máte požadovanou emailovou adresu po ruce. Uživatel obdrží své přihlašovací údaje pro GravityZone na uvedenou emailovou adresu.
- Správa uživatelských účtů. Tuto metodu můžete použít k povolení dynamického přístupu prostřednictvím pravidel pro přístupová oprávnění. Tato metoda vyžaduje integraci domény služby Active Directory. Více informace o integraci služby Active Directory naleznete v Instalačním průvodci GravityZone.

5.3.1. Individuální správa uživatelských účtů

V Control Center můžete vytvářet, upravovat a mazat uživatelské účty individuálně.

Závislosti

- Lokálně vytvořené účty mohou odstranit účty vytvořené integrací služby Active Directory bez ohledu na jejich roli.
- Lokálně vytvořené účty nemohou odstranit podobný účet bez ohledu na jejich roli.

Vytváření individuálních uživatelských účtů

Pro přidání nového uživatelského účtu do konzole Control Center:

1. Přejděte na stránku **Účty**.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.

3. V sekci **Detaily** nakonfigurujte následující:
   - U uživatelských účtů služby Active Directory nakonfigurujte následující podrobnosti:

     Uživatelské jméno pro uživatelské účty Active Directory (AD). V rozevíracím seznamu vyberte uživatelský účet a přejděte ke kroku 4.

     Uživatelské účty AD můžete přidat pouze v případě, že je integrace nakonfigurována. Při přidávání uživatelského účtu služby AD jsou údaje o uživateli importovány z přidružené domény. Uživatel se přihlásí do Control Center pomocí uživatelského jména a hesla AD.

     Poznámka
     - Pro jistotu, že jsou v Control Center importovány nejnovější změny z Active Directory, klikněte na tlačítko **Synchronizovat**.
     - Uživatelé s právem **Správa řešení** mohou konfigurovat interval synchronizace služby Active Directory pomocí možností dostupných na kartě **Konfigurace > služby Active Directory** . Další informace naleznete v tématu **Instalace ochrany>Instalace GravityZone** a **Nastavení > Konfigurace nastavení Control Center** kapitoly z Instalačního průvodce GravityZone.

   - Pro místní účty nakonfigurujte následující podrobnosti:
     - **Uživatelské jméno** pro místní účet. Zakažte **Import ze služby Active Directory** a zadejte uživatelské jméno.
     - **Email**. Zadejte emailovou adresu uživatele.

       Emailová adresa musí být unikátní. Není možné vytvořit jiný uživatelský účet s tou samou emailovou adresou.

       GravityZone používá tuto e-mailovou adresu k zasílání oznámení.
     - **Celé jméno**. Zadejte celé jméno uživatele.
     - **Heslo**. Zadejte heslo, které bude uživatel používat pro přihlášení.

       Heslo musí obsahovat alespoň jedno velké písmeno, malé písmeno a alespoň jednu číslici nebo zvláštní znak.
     - **Potvrdit heslo**. Potvrďte heslo pro ověření.
4. V sekci **Nastavení a oprávnění** nastavte následující:

- **Časová zóna**. Z nabídky zvolte časovou zónu účtu. Konzole bude zobrazovat časové údaje odpovídající zvolené časové zóně.
- **Jazyk**. Z nabídky zvolte jazyk konzole.
- **Role**. Zvolte roli uživatele. Více informací ohledně uživatelských rolí naleznete na „Uživatelské role“ (str. 29).
- **Oprávnění**. Každá předem definovaná uživatelská role má určitým způsobem nakonfigurovaná oprávnění. Můžete ale zvolit pouze ta oprávnění, která potřebujete. V takovém případě se uživatelská role změní na **Vlastní**. Více informací ohledně uživatelských práv naleznete na „Oprávnění uživatele“ (str. 30).
- **Výběr cílů**. Zvolte síťové skupiny, ke kterým bude mít uživatel přístup za každou dostupnou bezpečnostní službu. Můžete omezit přístup uživatelů k určité bezpečnostní službě GravityZone nebo k určitým umístěním v síti.

  Poznámka
  Možnosti pro volbu cíle se nezobrazí uživatelům s oprávněním Spravovat Řešení, kteří, ve výchozím stavu, mají práva nad celou sítí a bezpečnostními službami.

  Důležité
  Kdykoli provádíte změny ve své síťové struktuře, nebo když nastavujete novou integraci s dalším vCenter Serverem nebo systémem XenServer, nezapomeňte také zkontrolovat a aktualizovat přístupová pravidla pro stávající uživatele.

5. Pro přidání uživatele klikněte na **Uložit**. Nový účet se zobrazí v seznamu uživatelských účtů.

   Control Center automaticky zašle uživateli email s přihlašovacími údaji za předpokladu, že byla nastavení poštovního serveru řádně nastavena. Pro více podrobností ohledně nastavení poštovního serveru se odkažte na kapitolu **Instalace ochrany > Instalace a nastavení GravityZone >Nastavení parametry centra Control Center** v Průvodci instalací GravityZone.

Úprava uživatelských účtů individuálně

Pro přidání nového uživatelského účtu do Control Center

1. Přihlaste se do Control Center.
2. Přejděte na stránku **Účty**.

3. Klikněte na uživatelské jméno.
4. Podle potřeby změňte podrobnosti a nastavení uživatelského účtu.
5. Kliknutím na tlačítko **Uložit** aplikujete změny.

Poznámka
Všechny účty s oprávněním k **Spravovat uživatele** může vytvářet, upravovat a mazat uživatelské účty. Můžete spravovat pouze účty se stejnými nebo nižšími oprávněními, než jsou ta vaše.

Smazání uživatelských účtů individuálně

Pro smazání uživatelského účtu v Control Center

1. Přihlaste se do Control Center.
2. Přejděte na stránku **Účty**.
3. Vyberte uživatelský účet ze seznamu.
4. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky.

   Potvrďte kliknutím na **Ano**.

5.3.2. Správa uživatelských účtů

Vytvořte přístupová pravidla pro udělení přístupu GravityZone Control Center uživatelům služby Active Directory na základě bezpečnostních skupin.

Podmínky

Chcete-li spravovat více uživatelských účtů, potřebujete integraci domény Active Directory s GravityZone. Informace o integraci a synchronizaci domény Active Directory naleznete v kapitole **Active Directory** v Průvodce instalací GravityZone.

Závislosti

Pravidla oprávnění přístupu jsou vázána na skupiny zabezpečení služby Active Directory (AD) a přidružené uživatelské účty. Jakékoli změny provedené v doménách služby Active Directory mohou mít dopad na související pravidla přístupu. To je to, co potřebujete vědět o vztahu mezi pravidly, uživateli a doménami služby Active Directory:

- Pravidlo povolení přístupu přidá uživatelský účet pouze v případě, že e-mail již není spojen s existujícím účtem.

- Pro duplicitní e-mailové adresy v rámci skupiny zabezpečení vytvoří pravidlo povolení přístupu uživatelského účtu GravityZone pouze pro první uživatelský účet služby Active Directory, který se přihlásí v Control Center.

  Například skupina zabezpečení obsahuje duplicitní e-mailovou adresu pro různé uživatele a všichni se pokoušejí přihlásit do Control Center pomocí svých přihlašovacích údajů služby Active Directory. Pokud je k této konkrétní doméně služby Active Directory přiřazeno pravidlo povolení přístupu, vytvoří uživatelský účet pouze pro prvního uživatele, který se přihlásil do Control Center pomocí duplicitní e-mailové adresy.
- Uživatelské účty vytvořené na základě pravidel oprávnění k přístupu se stanou neaktivní, pokud budou odebrána z přidružené skupiny zabezpečení AD. Stejní uživatelé mohou být aktivní, pokud jsou přidruženi k novému přístupovému pravidlu.
- Pravidla přístupu se stávají přístupné pouze pro čtení, jakmile již není přidružená doména služby Active Directory integrována s GravityZone. Uživatelé přidružení k těmto pravidlům se stanou neaktivní.
- Uživatelské účty vytvořené pomocí přístupových pravidel nemohou odstranit lokálně vytvořené uživatele.
- Uživatelské účty vytvořené pomocí přístupových pravidel nemohou odstranit podobné účty, které mají roli Správce společnosti.

Vytváření více uživatelských účtů

Chcete-li přidat více uživatelských účtů, vytvoříte pravidla přístupu. Pravidla přístupu jsou přiřazena ke skupinám zabezpečení služby Active Directory.

Pro přidání pravidla přístupových práv:

1. Přejděte na **Konfigurace (Configuration) > Active Directory > Přístupová práva (Access Permissions)**.
2. Pokud máte více integrací, vyberte doménu v levé horní části tabulky.
3. Klikněte na tlačítko ⊕ **Přidat** v levé části tabulky.
4. Konfigurace následujících nastavení přístupových práv (access permission settings):
   - **Priorita (Priority)**. Pravidla jsou zpracovávána v pořadí dle priorit. Čím je číslo nižší, tím vyšší je priorita.
   - **Jméno**. Název pravidla pro přístup.

- **Doména (Domain)**. Doména, ze které se přidávají skupiny zabezpečení.
- **Bezpečnostní skupiny** Bezpčnostní skupiny, které obsahují vaše budoucí uživatele GravityZone. Můžete použít automatické dokončovací pole. Skupiny zabezpečení přidané do tohoto seznamu se po uložení přístupového pravidla nemohou měnit, přidávat ani mazat.
- **Časová zóna**. Časová zóna uživatele.
- **Jazyk**. Jazyk konzole.
- **Role**. Předdefinované role uživatelů. Další podrobnosti naleznete v kapitole **Uživatelské účty** v Příručce správce GravityZone.

  Poznámka
  Oprávnění můžete udělit a odvolat jiným uživatelům se stejnými nebo menšími oprávněními, než je váš účet.

- **Oprávnění**. Každá předem definovaná uživatelská role má určitým způsobem nakonfigurovaná oprávnění. Další podrobnosti naleznete v kapitole **Uživatelská práva** v Příručce správce GravityZone.
- **Vyberte cíle** Vyberte síťové skupiny, ke kterým bude mít uživatel přístup pro každou dostupnou bezpečnostní službu. Můžete omezit přístup uživatelů k určité bezpečnostní službě GravityZone nebo k určitým umístěním v síti.

  Poznámka
  Možnosti pro volbu cíle se nezobrazí uživatelům s oprávněním Spravovat Řešení, kteří, ve výchozím stavu, mají práva nad celou sítí a bezpečnostními službami.

5. Klikněte na tlačítko **Save**.

   Pravidlo přístupu se uloží, pokud na uživatele nemá žádný dopad. Jinak budete vyzváni k zadání vyloučení uživatelů. Například když přidáte pravidlo s vyšší prioritou, uživatelé s dopadem přidružení k jiným pravidlům budou vázáni na předchozí pravidlo.
6. V případě potřeby vyberte uživatele, které chcete vyloučit. Další informace viz Vyjímky uživatelských účtů.
7. Klikněte na **Potvrdit (Confirm)**. Pravidlo je zobrazeno na stránce **Přístupová oprávnění**.

Uživatelé ve skupinách zabezpečení určených přístupovými pravidly mohou nyní přistupovat k GravityZone Control Center pomocí svých pověření domény. Control Center automaticky vytvoří nové uživatelské účty, když se poprvé přihlásí, pomocí své e-mailové adresy a hesla pro Active Directory.

Uživatelské účty vytvořené pomocí pravidla přístupu mají název pravidla přístupu zobrazeného na stránce **Účty** ve sloupci **Pravidlo přístupu** .

Úpravy více uživatelských účtů

Pro změnu pravidla oprávnění přístupu"

1. Přejděte na **Konfigurace (Configuration) > Active Directory > Přístupová práva (Access Permissions)**.
2. Chcete-li otevřít konfigurační okno, vyberte název přístupového pravidla.
3. Editujte nastavení přístupových práv. Pro více infomací si přečtěte Přidání přístupových pravidel (Adding Access Permissions).
4. Klikněte na tlačítko **Save**. Pravidlo se uloží, pokud nemá žádný vliv na uživatele. Jinak budete vyzváni k zadání vyloučení uživatelského účtu. Pokud například aktualizujete prioritu pravidla, dotčení uživatelé mohou přepnout na jiné pravidlo.
5. V případě potřeby vyberte uživatele, které chcete vyloučit. Další informace viz Vyjímky uživatelských účtů.
6. Klikněte na **Potvrdit (Confirm)**.

> **Poznámka**
> Uživatelský účet vytvořený pomocí pravidel přístupu můžete odpojim modifikací jeho práv v Control Center. Uživatelský účet nemůže být spojen zpět s pravidly přístupu.

Odstranění více uživatelských účtů

Postup odstranění pravidla přístupu:

1. Přejděte na **Konfigurace (Configuration) > Active Directory > Přístupová práva (Access Permissions)**.
2. Vyberte pravidlo, které chcete smazat a klikněte na ⊖ **Smazat (Delete)**. Okno Vás vyzve k potvrzení Vaší akce. Pokud dojde k dopadu na uživatele, budete vyzváni k zadání vyloučení uživatelského účtu. Například můžete chtít určit vyloučení pro uživatele ovlivněné odstraněním pravidla.

3. V případě potřeby vyberte uživatele, které chcete vyloučit. Další informace naleznete v části Vyjímky uživatelů .
4. Klikněte na **Potvrdit (Confirm)**.

Vymazání pravidla pro přístup zruší přístup do asociovaných uživatelských účtů. Všichni uživatelé, kteří jsou přes něj vytvořeni, budou odstraněni, pokud jim jiná pravidla neumožní přístup.

Vyjímky uživatelského účtu

Když přidáváte, upravujete nebo odstraňujete pravidla pro přístupová práva, která mají dopad na uživatele, možná budete chtít určit vyjímky uživatelského účtu. Můžete si také prohlédnout zdůvodnění a účinky dotčených uživatelů.

Specifikujte uživatelské výjimky jako následující:

1. Vyberte uživatele, které chcete vyloučit. Nebo zaškrtnutím políčka v horní části tabulky přidejte všechny uživatele do seznamu.
2. Klikněte **X** do pole uživatelského jména a odeberete jej ze seznamu.

5.4. Obnovení přihlašovacích hesel

Majitelé účtů, kteří zapomenou své heslo, ho mohou obnovit pomocí odkazu pro obnovení hesla na přihlašovací stránce. Zapomenuté heslo můžete resetovat také upravením příslušného uživatelského účtu z konzole.

Pro obnovení přihlašovacího hesla uživatele:

1. Přihlaste se do Control Center.
2. Přejděte na stránku **Účty**.
3. Klikněte na uživatelské jméno.
4. Zadejte nové heslo do příslušných polí (pod **Podrobnosti**).
5. Kliknutím na tlačítko **Uložit** aplikujete změny. Majitel účtu obdrží email s novým heslem.

5.5. Správa dvou-faktorové autentizace

Kliknutím na uživatelský účet, si budete moci prohlédnout stav 2FA jestli je zapnutá či vypnutá (enabled nebo disabled) a sice v sekci **Dvou-faktorová autentizace (Two-factor Authentication)**. Můžete provést následující akce:

- **Resetovat nebo vypnout dvou-faktorovou autentizaci pro uživatele**. Pokud uživatel, který má zapnutou 2FA vyměnil , smazal či ztratil svoje zařízení a ztratil tajný klíč:
  1. Zadejte vaše heslo pro GravityZone v dostupném poli.
  2. Klikněte na **Reset** (když je 2FA vynucena) nebo na **Vypnout (Disable)** (když 2FA není vynucena).
  3. Potvrzovací zpráva vás bude infomovat, že byla dvou-faktorová autentizace resetována / vypnuta pro danného uživatele.

     Po resetování 2FA, když je tato volba vynucena, se při přihlášení uživateli zobrazí konfigurační okno a vyzve ho znovu nakonfigurobvat dvou-faktorovou autentizaci s novým tajným klíčem.
- Pokud má uživatel 2FA vypnutou a vy ji chcete aktivovat, tak budete muset nařídit uživateli aby si zapnul tuto funkionalitu v jeho uživatelském účtu.

Poznámka
Pokud máte účet správce společnosti, můžete pro všechny účty GravityZone povolit dvoufázové ověřování. Více informací naleznete v Instalačním Manuálu, v sekci **Instalace ochrany > GravityZone instalace a nastavení > Konfigurace řídícího centra nastavení** kapitole.

Důležité
Ověřovací aplikace dle výběru (Google Authenticator, Microsoft Authenticator nebo jakýkoli dvoufaktorový autentizátor TOTP (Time-Based One-Time Password Algorithm) - kompatibilní se standardem RFC6238) kombinuje tajný klíč s aktuálním časovým razítkem mobilního zařízení a generuje šestimístný kód. Ujistěte se, že jsou časová razítka jak na mobilním zařízení tak na GravityZone appliance shodná proto aby byl šestimístný kód platný. Doporučujeme zapnout automatické nastavení času na mobilním zařízení , proto aby bylo zabráněno jakýmkoliv problémům se synchronizací časových razítek.

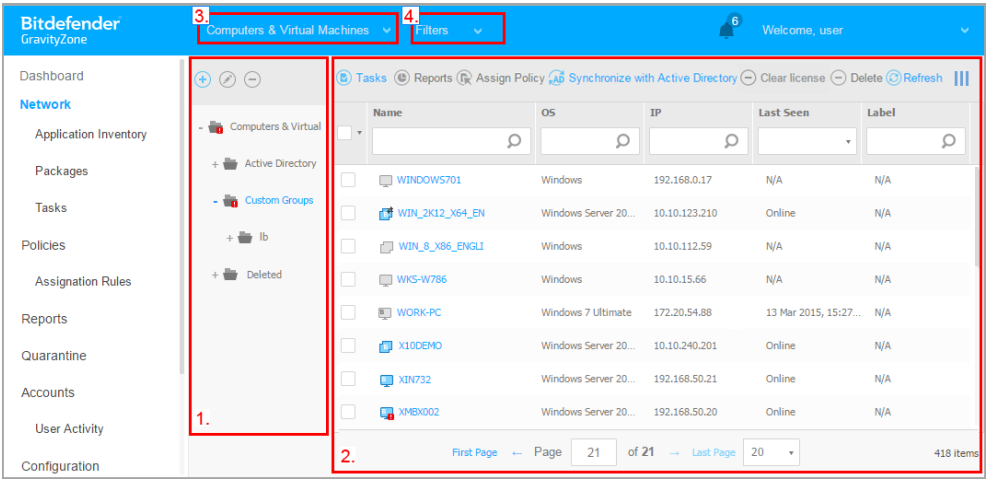
Jinou metodou pro zjištění 2FA změn u uživatelských účtů je přejít na stránku **Účty (Accounts) > Uživatelské aktivity (User Activity)** a vyfiltrovat si aktivity v záznamech logů pomocí následujících filtrů:

- Oblast (Area) > Účty / Firmy (Accounts / Company)
- Akce (Action) > Editované (Edited)

Pro více informací o zapnutí 2FA, čtěte„Správa vašeho účtu “ (str. 24)

6. SPRAVOVÁNÍ SÍŤOVÝCH OBJEKTŮ

Na stránce **Síť** naleznete několik funkcí pro prohlížení a spravování každého typu síťových objektů dostupných v Control Center (počítače, virtuální zařízení a mobilní zařízení). Sekce **Síť** se skládá z dvou-panelového rozhraní, kde je zobrazen stav všech síťových objektů v reálném čase:



Stránka Síť

1. V levém panelu je zobrazena dostupná struktura síťového stromu. Podle zvoleného zobrazení sítě je v tomto panelu zobrazena síťová infrastruktura integrovaná s Control Center, jako je Active Directory, vCenter Server nebo Xen Server.

   Zároveň, všechny počítače a virtuální stroje nalezené ve vaší síti, které nepatří do žádné z integrovaných infrastruktur, jsou zobrazeny pod **Vlastními skupinami**.

   Všechny smazané koncové body jsou uchovány ve složce **Odstraněné**. Více informací naleznete na „Odstranění koncových bodů ze Síťového inventáře“ (str. 204).

   Poznámka
   Prohlížet a spravovat můžete pouze skupiny, ke kterým máte správní oprávnění.

2. Pravý panel ukazuje obsah skupiny, kterou jste zvolili v levém panelu. Tento panel se skládá z mřížky, kde řádky obsahují síťové objekty a sloupce zobrazují konkrétní informace pro každý typ objektu.

   Pomocí tohoto panelu můžete:

   - Zobrazit detailní informace o každém objektu v síti pod vaším účtem. Můžete zobrazit status každého objektu zaškrtnutím ikony vedle názvu. Posuňte kurzor myši nad ikonu pro zobrazení nápovědy. Klepnutím na název objektu zobrazíte okno s konkrétnějšími detaily.

     Každý typ objektu, jako například počítač, virtuální stroj nebo složka je reprezentována speciální ikonou. Ve stejnou dobu, každý objekt sítě může mít určitý stav, týkající se řídícího statusu, bezpečnostní chyby, problém s připojením a podobně. Pro detaily ohledně popisu všech ikon objektů v síti a možných statusů, obraťte se na „Typy a stavy síťových souborů“ (str. 564).
   - Požijte Panel Nástrojů na vrchu tabulky, pro provedení specifické operace, pro každý objekt v síti (například spouštění úloh, vytváření přehledů, přiřazování práv a mazání) a obnovte data v tabulce.
3. Výběr zobrazení v horní části síťových panelů vám umožňuje přepínat mezi různými obsahy síťového inventáře podle toho, s jakým typem koncového bodu chcete pracovat.
4. Dostupná nabídka **Filtry** v horní části síťového panelu, pomáhá k jednoduchému zobrazení jednotlivých síťových objektů, poskytuje několik filtrovacích kritérií. Možnosti v nabídce **Filtry** se vztahují k současně zvolenému zobrazení sítě.

V sekci **Síť** můžete také spravovat instalační balíčky a úlohy pro každý typ síťového objektu.

Poznámka
Chcete-li zjistit více o instalačních balíčcích, obraťte se na GravityZone Instalační Příručku.

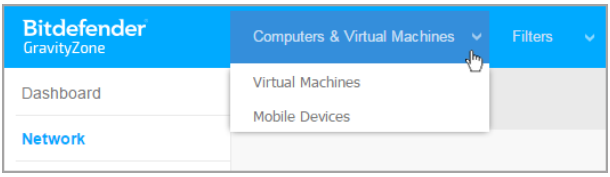
Podrobné informace o síťových objektech naleznete zde:

- „Práce s možnostmi zobrazení“ (str. 42)
- „Počítače“ (str. 45)
- „Virtuální stroje“ (str. 105)
- „Mobilní zařízení“ (str. 161)
- „Inventář Balíčků“ (str. 191)
- „Prohlížení a správa úloh“ (str. 200)
- „Odstranění koncových bodů ze Síťového inventáře“ (str. 204)

6.1. Práce s možnostmi zobrazení

Různé typy koncových zařízení dostupných v Control Center jsou uspořádány do skupin na stránce **Síť** podle různých síťových zobrazení. Každé zobrazení sítě ukazuje určitý typ síťové infrastruktury podle toho, jaký typ koncového zařízení chcete spravovat.

Pro změnu síťového zobrazení přejděte na levou horní stranu stránky **Síť** a klikněte na možnosti zobrazení:



Výběr zobrazení

K dispozici jsou následující síťová zobrazení:

- Počítače a virtuální stroje
- Virtuální stroje
- Mobilní zařízení

6.1.1. Počítače a virtuální stroje

Toto zobrazení je navrženo pro počítače a virtuální zařízení integrované v Active Directory a poskytuje specifické akce a možnosti filtrování pro spravování počítačů ve vaší síti. Pokud je dostupná integrace s Active Directory, načte se strom Active Directory společně s odpovídajícími koncovými body.

Při práci v zobrazení **Počítače a virtuální stroje** můžete kdykoli synchronizovat obsah Control Center s vaším Active Directory pomocí tlačítka **Synchronizovat s Active Directory** z Akčního panelu nástrojů.

Zároveň jsou všechny počítače a virtuální stroje, které nejsou integrované v Active Directory, uspořádány do skupin pod Vlastními skupinami. Tato složka může obsahovat následující typy koncových bodů:

- Počítače a virtuální stroje dostupné ve vaší síti mimo Active Directory.
- Virtuální stroje z virtualizované infrastruktury, které jsou dostupné ve vaší síti.
- Bezpečnostní servery, které jsou již nainstalovány na hostiteli ve vaší síti.

Poznámka
Je-li k dispozici virtualizovaná infrastruktura, můžete Bezpečnostní servery zavést a spravovat ze zobrazení **Virtuální zařízení**. V opačném případě můžete Bezpečnostní servery nainstalovat a nastavit lokálně na hostiteli.

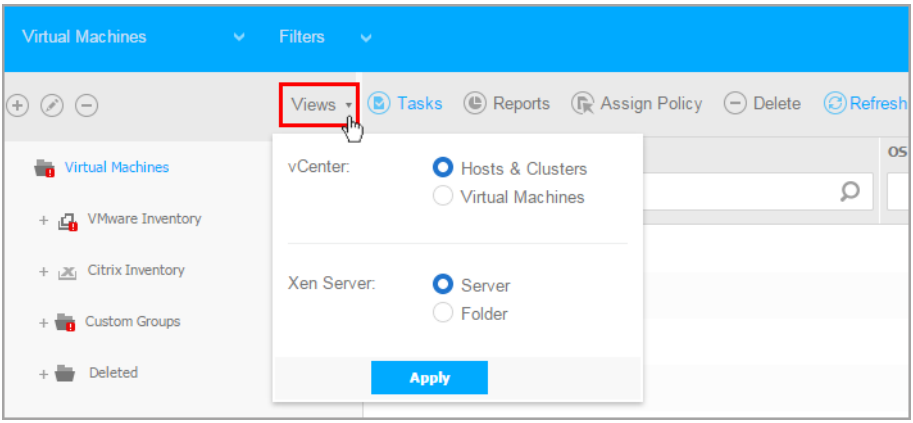
Důležité
Při přiřazování politik k virtuálním strojům v sekci **Počítače a virtuální stroje** může být omezen náhled v GravityZonesprávcem řešení v konfiguraci pro vCenter Server nebo Xen Server na stránce **Konfigurace > Dodavatelé Virtualizačních platforem**. Pro více informací se odkažte na kapitolu **Instalace ochrany > Instalace a nastavení GravityZone** v Průvodci instalací GravityZone.

6.1.2. Virtuální stroje

Toto zobrazení je navrženo speciálně pro zobrazení vašich integrací ve virtualizované infrastruktuře. Možnosti filtrování dostupné v tomto zobrazení vám umožňují zvolit zvláštní kritéria pro zobrazení jednotek virtuálního prostředí.

V levé tabulce si můžete prohlédnout inventáře od platforem: Nutanix, VMware nebo Citrix virtual.

V horní části levého panelu naleznete také nabídku **Zobrazení**, jejíž pomocí můžete zvolit režim zobrazení virtuálních inventářů.



Stránka Síť - zobrazení Virtuálních strojů

Všechny virtuální stroje ve vaší síti, které nejsou integrované ve virtuální infrastruktuře jsou zobrazeny pod **Vlastními skupinami**.

Abyste mohli přistupovat k virtualizované infrastruktuře integrované s Control Center, musíte zadat své přihlašovací údaje pro každý dostupný vCenter Server. Control Center používá vaše přihlašovací údaje pro připojení se k virtualizované infrastruktuře, a zobrazuje pouze zdroje, ke kterým máte přístup (jak je definováno v vCenter Server). Pokud jste neurčili vaše autentizační pověření, budete je muset zadat, až se pokusíte přistoupit k prohlížení inventáře jakéhokoli Center Serveru. Jakmile zadáte svá pověření, uloží se do Správce pověření a příště je už zadávat nemusíte.

6.1.3. Mobilní zařízení

Toto zobrazení je navrženo speciálně pro prohlížení a správu mobilních zařízení dostupných ve vaší síti a poskytuje zvláštní akce a možnosti filtrování.

V tomto zvláštním zobrazení můžete nechat zobrazit síťové objekty podle uživatelů nebo podle zařízení.

V okně sítě je zobrazena vaše stromová struktura Active Directory, pokud je dostupná. V tomto případě se všichni uživatelé Active Directory zobrazí ve vašem síťovém inventáři spolu se všemi mobilními zařízeními, která jsou k nim přiřazena.

Poznámka
Detaily o uživateli Active Directory se načítají automaticky a nelze je měnit.

Vlastní skupiny zahrnují všechny uživatele mobilních zařízení, které jste ručně přidali do Control Center.

6.2. Počítače

Pro prohlížení počítačů pod vaším účtem přejděte na stránku **Síť** a v možnostech zobrazení vyberte **Počítače a virtuální stroje**.

Můžete si zobrazit dostupnou strukturu sítě v levém panelu a detaily o každém koncovém zařízení v pravém panelu.

Na začátku, všechny počítače a virtuální stroje detekované ve vaší síti jsou zobrazeny jako nespravované, takže můžete na ně vzdáleně nainstalovat zabezpečení.

Pro úpravu zobrazených detailů ohledně počítače v tabulce:

1. Klikněte na tlačítko **Sloupce** napravo od Panel Nástrojů.
2. Vyberte sloupce, které chcete zobrazit.
3. Klikněte na tlačítko **Resetovat** pro návrat pro zobrazení standardních sloupců.

Ze záložky **Síť** můžete spravovat počítače následovně:

- Kontrolovat stav počítače
- Prohlížet detaily počítače
- Organizovat počítače do skupin
- Třízení, filtrování a vyhledávání
- Spravovat balíčky
- Spustit úlohy
- Vytvářejte rychlá hlášení
- Přiřaďte pravidla
- Synchronizovat s Active Directory

Pro zobrazení nejnovějších informací v tabulce, klikněte na tlačítko **Obnovit** v levém spodním rohu tabulky. Toto může být potřeba, když na stránce strávíte více času.

6.2.1. Kontrolovat stav počítačů

Každý počítač je na stránce sítí reprezentován ikonou specifickou pro jeho typ a stav.

Seznam všech dostupných ikon a stavů naleznete na „Typy a stavy síťových souborů“ (str. 564).

Podrobné informace o stavu viz:

- Správa stavů
- Stav připojení
- Stav zabezpečení

Správa stavů

Počítače mohou být v následujících stavech správy:

- **Spravované** - počítače, na kterých je nainstalovaný bezpečnostní agent.
- **Je vyžadován restart** - koncové body, které vyžadují restartování systému po instalaci nebo aktualizaci ochrany Bitdefender.
- **Nespravované** - nalezené počítače, na kterých ještě nebyl nainstalován bezpečnostní agent.
- **Smazané** - počítače, které jste odstranili z Control Center. Další informace viz „Odstranění koncových bodů ze Síťového inventáře“ (str. 204).

Stav připojení

Stav připojení se týká pouze spravovaných počítačů. Z tohoto pohledu mohou spravované počítače být:

- **Online**. Modrá ikona značí, že počítač je online.
- **Offline**. Šedá ikona značí, že počítač je offline.

Počítač je offline, pokud je bezpečnostní agent neaktivní po dobu delší než 5 minut. Možné důvody, proč se koncové body zobrazují jako offline:

- Počítač je vypnutý, v režimu spánku nebo hibernace.

  Poznámka
  Počítače jsou zobrazeny jako online, i když jsou uzamčeny, nebo je uživatel odhlášený.

- Bezpečnostní agent nemá připojení ke Komunikačnímu centru GravityZone:
  - Počítač může být odpojený od sítě.
  - Komunikace mezi bezpečnostním agentem a Komunikačním serverem GravityZone může být blokována síťovým firewallem nebo routerem.
  - Koncový bod je za proxy serverem, a nastavení proxy nebyla řádně nakonfigurována v aplikovaných zásadách.

Varování
Pro počítače za proxy serverem musí být nastavení proxy řádně nastavena v instalačním balíčku bezpečnostního agenta, nebo počítač nebude komunikovat s konzolí GravityZone a bude se vždy jevit jako offline nehledě na to, zda byly zásady s náležitým nastavením proxy aplikovány po instalaci.

- Bezpečnostní agent nebude možná pracovat správně.

Pro zjištění délky neaktivity počítačů:

1. Zobrazit pouze spravované počítače. Klikněte na **Filtry** nacházející se na vrchu tabulky a vyberte ze "Spravované" všechny možnosti, které potřebujete ze záložky **Bezpečnost**, vyberte **Všechny položky rekurzivně** ze záložky **Hloubka** a klikněte **Uložit**.
2. Klikněte na záhlaví sloupce **Posledně prohlíženo** pro seřazení počítačů podle délky neaktivity.

Kratší časové úseky neaktivity (minuty, hodiny) můžete ignorovat, protože se pravděpodobně jedná o dočasný stav z důvodu latenci v komunikaci. Například, počítač je právě vypnutý.

Delší doba neaktivity (dny, týdny) obvykle značí problém s počítačem.

Poznámka
Síťovou tabulku doporučujeme čas od času obnovit pro aktualizaci informací o koncových bodech s nejnovějšími změnami.

Stav zabezpečení

Stav zabezpečení se týká pouze spravovaných počítačů. Počítače s bezpečnostními problémy můžete identifikovat podle stavových ikon, které zobrazují varovný symbol:

- Spravovaný počítač, s problémy, online.
- Spravovaný počítač, s problémy, offline.

Počítač má problémy se zabezpečením v případě, že pro něj platí alespoň jedna z následujících situací:

- Ochrana proti malwaru je vypnutá.
- Vypršela licence.
- Bezpečnostní agent je zastaralý.
- Obsah zabezpečení je zastaralý.
- Byl nalezen malware.

- Připojení k Cloudovým službám Bitdefender nemohlo být navázáno z následujících možných důvodů:
  - Počítač má problémy s připojením k internetu.
  - Připojení k Cloudovým službám Bitdefender je blokováno síťovým firewallem.
  - Port 443, nezbytný pro komunikaci s Cloudovými službami Bitdefender, je uzavřený.

  V tomto případě se antimalwarová ochrana spoléhá pouze na místní nástroje, zatímco skenování v cloudu je vypnuté, takže bezpečnostní agent nemůže poskytovat plnou ochranu v reálném čase.

Pokud naleznete počítač s bezpečnostními problémy, klikněte na jeho jméno pro zobrazení **Informačního** okna. Bezpečnostní problémy můžete identifikovat podle ikony !. Ujistěte se, že jste zkontrolovali bezpečnostní informace ve všech záložkách informační stránky. Více podrobností se dozvíte kliknutím na nápovědu ikony. Může být nutné provést hlubší místní vyšetřování.

Poznámka
Síťovou tabulku doporučujeme čas od času obnovit pro aktualizaci informací o koncových bodech s nejnovějšími změnami.

6.2.2. Prohlížení detailů počítače

Podrobné informace o každém počítači můžete získat na stránce **Síť** následujícím způsobem:

- Prohlížení stránky **Síť**
- Prohlížení okna **Informace**

Kontrolování Záložky Síť

Chcete-li zjistit podrobnosti o počítači, zkontrolujte dostupné informace v tabulce na pravém panelu na stránce **Síť**.

Sloupce s informacemi o koncových bodech můžete přidat nebo odebrat kliknutím na tlačítko **Sloupce** v pravé horní části panelu.

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kterou chcete z levého panelu.

Všechna dostupná koncová zařízení ve vybrané skupině jsou zobrazena v pravém panelu tabulky.

4. Stav počítače můžete snadno identifikovat podle příslušné ikony. Podrobné informace viz „Kontrolovat stav počítačů“ (str. 45).
5. Zkontrolujte informace zobrazené ve sloupcích pro každý počítač.

   Používejte hlavičku podle toho co zadáte při vyhledávání určitého koncového zařízení, na základě dostupných kritérií:

   - **Název**: Název koncového zařízení.
   - **FQDN**: plně kvalifikované jméno domény, které zahrnuje název hosta a jméno domény.
   - **OS**: operační systém nainstalovaný na koncovém bodě.
   - **IP**: IP adresa koncového bodu.
   - **Naposledy prohlíženo**: datum a čas, kdy byl koncový bod naposledy viděn online.

     Poznámka
     Důležité pro sledování oblasti **Naposledy online**, jak dlouhé jsou periody nečinnosti to může znamenat problém s komunikací nebo odpojený počítač.

   - **Popisek**: vlastní řetězec s doplňujícími informacemi o koncovém bodu. Můžete přidat štítek v okně koncových zařízení **Informace** a poté použít vyhledat.
   - **Práva**: práva použitá pro koncové zařízení s odkazem na zobrazení a změnu nastavení práv.

Prohlížení okna Informace

Pro zobrazení okna **Informace** klikněte v pravém panelu na stránce **Síť** na jméno koncového bodu, který vás zajímá. V tomto okně jsou zobrazeny pouze údaje dostupné pro zvolený koncový bod, seskupené pod několika kartami.

Níže naleznete vyčerpávající seznam informací, které můžete nalézt v okně **Informace** podle typu a specifických bezpečnostních informací koncového bodu.

Karta Obecné

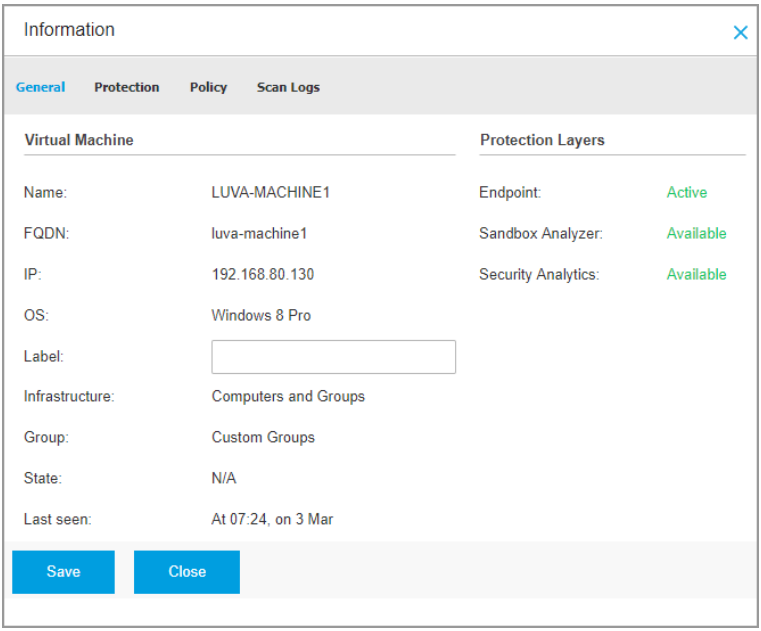
- Obecné informace o počítači, jako je název, identifikace FQDN, IP adresa, operační systém, infrastruktura, rodičovská skupina a aktuální stav připojení.

  V této sekci můžete ke koncovému bodu přiřadit popisek. Budete moci rychle najít koncové body se stejným popiskem a pracovat s nimi nehledě na to, kde v síti jsou umístěny. Více informací o filtrování koncových bodů naleznete v „Třídění, Filtrování a Hledání počítačů“ (str. 64).

- Informace o ochranných vrstvách, včetně seznamu bezpečnostních technologií získaných s vaším řešením GravityZone a stav jejich licence, který může být:
  - **Dostupné / Aktivní** - licenční klíč pro tuto ochrannou vrstvu je na koncovém bodě aktivní.
  - **Expirovaný** - licenční klíč pro tuto ochrannou vrstvu vypršel.
  - **Čekající** - licenční klíč ještě nebyl potvrzen.

    Poznámka
    Doplňující informace o ochranných vrstvách naleznete na kartě **Zabezpečení**.

- **Relay připojení**: jméno, IP a popis relaye, ke kterému je koncový bod případně připojen.



Informační okno - Karta Obecné

Karta Zabezpečení

Tato karta obsahuje podrobnosti o ochraně použité v koncovém bodě a odkazuje na:

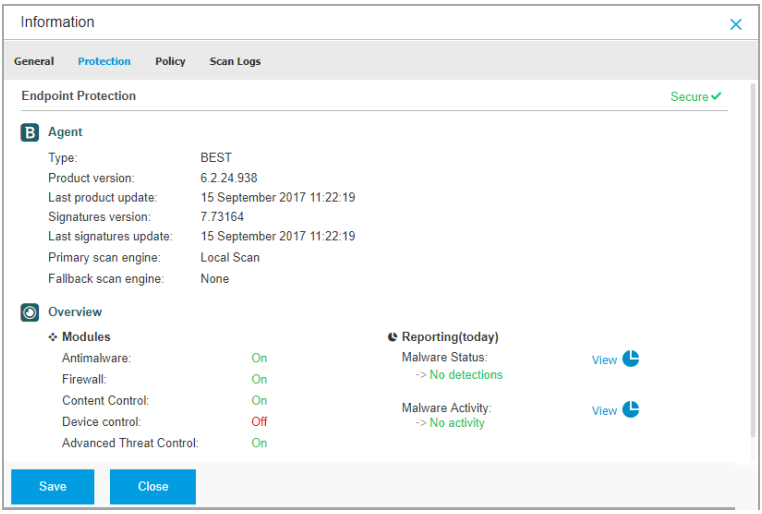
- Informace o agentovi zabezpečení, jako je název produktu, verze, stav aktualizace a umístění aktualizace, jakož i konfigurace skenovacích mechanizmů a verze obsahu zabezpečení. Pro Exchange Protection je k dispozici také verze antispamového modulu.
- Stav zabezpečení pro každou vrstvu ochrany. Tento stav je zobrazen vedle názvu ochranné vrstvy na pravé stráně:
  - **Zabezpečený**, když na koncových bodech s aplikovanou bezpečnostní vrstvou nejsou hlášeny žádné bezpečnostní problémy.
  - **Zranitelný**, když jsou na koncových bodech s aplikovanou bezpečnostní vrstvou hlášeny bezpečnostní problémy. Více informací naleznete na „Stav zabezpečení“ (str. 47).

- Přiřazený Security Server. Každý přiřazený Security Server se zobrazí v případě zavádění bez agenta, nebo když jsou skenovací nástroje bezpečnostních agentů nastaveny na skenování na dálku. Security Server informace jsou nápomocné při identifikaci virtuálního zařízení a při získání jeho aktualizačního stavu.
- Stav ochranných modulů. Můžete snadno prohlížet, jaké ochranné moduly byly nainstalovány na koncový bod, a také stav dostupných modulů (**Zapnuto / Vypnuto**) nastavených skrze aplikovaná pravidla.
- Rychlý přehled ohledně aktivity modulů a malwarových hlášení za současný den.

  Klikněte na odkaz **Zobrazení** pro přístup k nastavením hlášení a poté vytvořte hlášení. Další informace viz „Vytváření hlášení“ (str. 497)
- Informace ohledně ochranné vrstvy Sandbox Analyzer:
  - Stav využití Sandbox Analyzer na koncovém bodě je zobrazený na pravé straně okna:
    - **Active**: Sandbox Analyzer je licencovaný (dostupný) a povolený na základě politik na koncovém bodě.
    - **Neaktivní**: Sandbox Analyzer je licencovaný (dostupný), ale není povolený v politice koncového bodu.
  - Název agenta, který se chová jako detekční senzor.
  - Stav modulu na koncovém bodě:
    - **Zapnutý** - Sandbox Analyzer je povolený na koncovém bodě prostřednictvím politiky.
    - **Vypnutý** - Sandbox Analyzer není povolený na koncovém bodě prostřednictvím politiky.
  - Nalezené hrozby za poslední týden kliknutím na odkaz **Zobrazit** pro přístup k hlášení.
- Doplňující informace týkající se modulu Šifrování, jako jsou:
  - Zjištěné svazky (se zmínkou o spouštěcí jednotce).
  - Status šifrování pro každý svazek (který může být **Šifrováno**, **Probíhá Šifrování**, **Probíhá Dešifrování**, **Nešifrované**, **Uzamčené** nebo **Pozastavené**).

Klíč pro obnovu přiřazeného šifrovaného svazku získáte kliknutím na odkaz **Obnovení**. Pro detaily ohledně získání klíčů pro obnovu se obraťte na „“ (str. 103).

- Stav telemetrie zabezpečení, který vás informuje, pokud je spojení mezi koncovým bodem a serverem SIEM navázáno a funkční, je zakázáno nebo má problémy.



Informační okno - Karta Zabezpečení

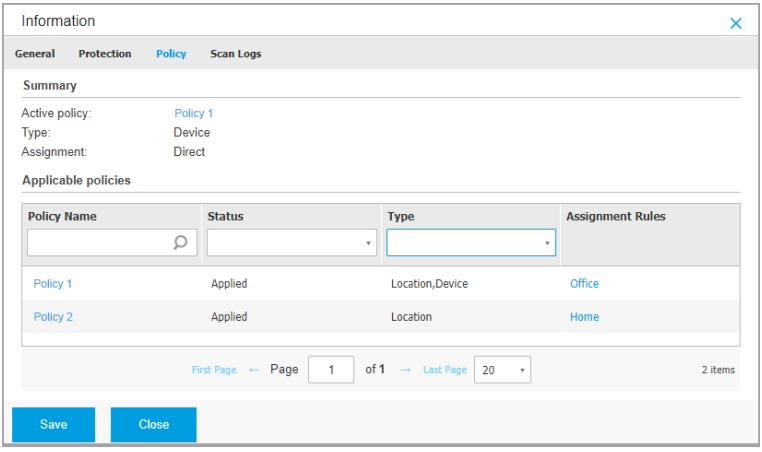
Záložka Práv

Na koncový bod lze aplikovat jedno nebo více pravidel, ale aktivní může být vždy pouze jedno. Na kartě **Politiky** jsou zobrazeny informace o všech pravidlech platných pro koncový bod.

- Název aktivní politiky. Klikněte na název pravidla pro otevření její šablony a prohlížení jejích nastavení.
- Typ aktivního pravidla, což může být:
  - **Zařízení**: když je pravidlo ke koncovému bodu přiřazeno ručně administrátorem sítě.

  - **Umístění**: zásada založená na pravidlech, automaticky přiřazená ke koncovému bodu, pokud se jeho síťová nastavení shodují s podmínkami danými v existujícím pravidle přiřazování.

    Například, notebook má přiřazená dvě pravidla rozpoznávající polohu: jedno se jmenuje `Kancelář` a je aktivní během připojení se k firemní LAN, a `Roaming`, které se aktivuje, když uživatel pracuje na dálku a připojuje se k jiným sítím.
  - **Uživatel**: zásada založená na pravidlech, automaticky přiřazená ke koncovému bodu, pokud se shoduje s cílem Active Directory určeným podle existujícího přiřazovacího pravidla.
  - **Externí (NSX)**: když je pravidlo definováno v prostředí VMware NSX.
- Typ přiřazování aktivních pravidel, který může být:
  - **Přímý**: když je pravidlo aplikováno přímo na koncový bod.
  - **Zděděný**: když koncový bod zdědí pravidlo z rodičovské skupiny.
- **Aplikovatelné politiky**: zobrazí seznam pravidel propojených s existujícími pravidly přiřazování. Tyto zásady mohou být aplikovány na koncový bod, když se shodují s podmínkami zadanými v připojených přiřazovacích pravidlech.

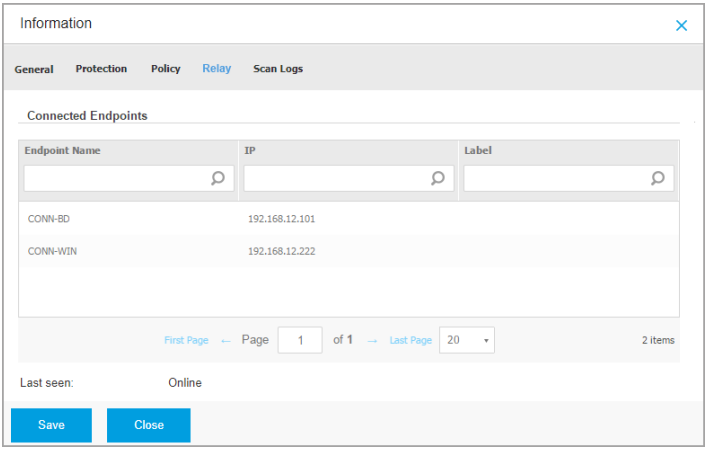


Informační okno - Záložka Práv

Více informací ohledně pravidel naleznete na „Změna nastavení pravidel“ (str. 225)

Karta Připojené koncové body

Karta **Připojené koncové body** je k dispozici pouze pro koncové body s rolí relay. Tato karta zobrazuje informace o koncových bodech připojených ke stávajícímu relayi, jako je název, IP a popis.

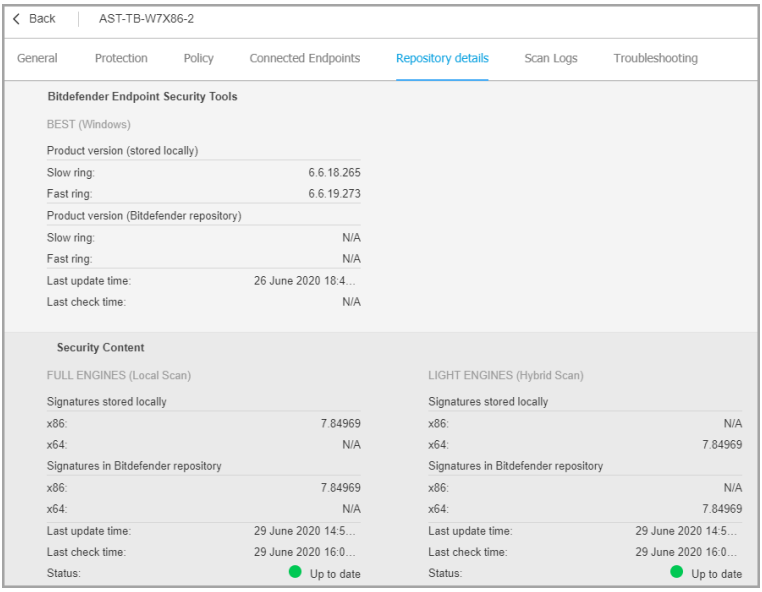


Informační okno - karta Připojené koncové body

Karta Podrobnosti úložiště

Karta **Podrobnosti úložiště** je k dispozici pouze pro koncové body s rolí relay a zobrazuje informace o aktualizacích agenta zabezpečení a obsahu zabezpečení.

Karta obsahuje podrobnosti o verzi produktu a podpisech uložených v relay a verze dostupné v oficiálním úložišti, aktualizační okruhy, datum a čas aktualizace a poslední kontrolu nových verzí.



Informační okno - záložka Podrobnosti úložiště

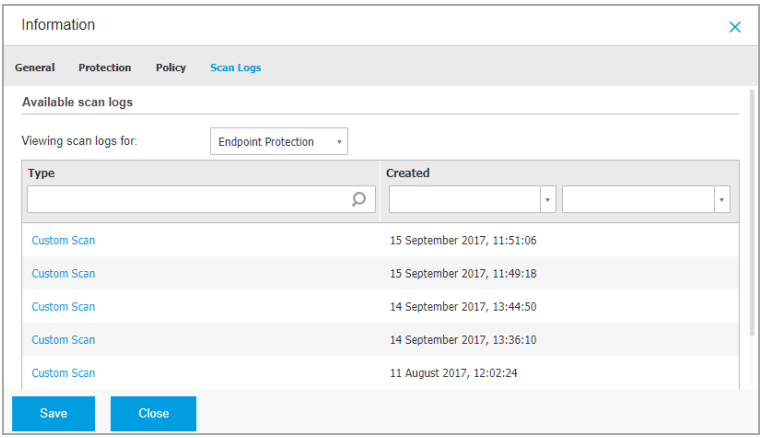
Karta Protokoly skenování

Záložka **Zpráva o skenování** ukazuje detailní informace o všech skenovacích úlohách, které proběhly na koncovém zařízení.

Zprávy jsou spojeny ochranou vrstvou a můžete si vybrat z rozbalovacího menu, pro kterou vrstvu se má zpráva zobrazit.

Klikněte na skenovací úlohu, která vás zajímá a zpráva se otevře v novém okně webového prohlížeče.

Je-li k dispozici mnoho zpráv o skenování, mohou se rozložit na několik stránek. Pro pohyb mezi stránkami, použijte navigační panel dole v tabulce. Pokud je k dispozici příliš mnoho záznamů, můžete využít možnosti filtrů, které jsou k dispozici v horní části tabulky.

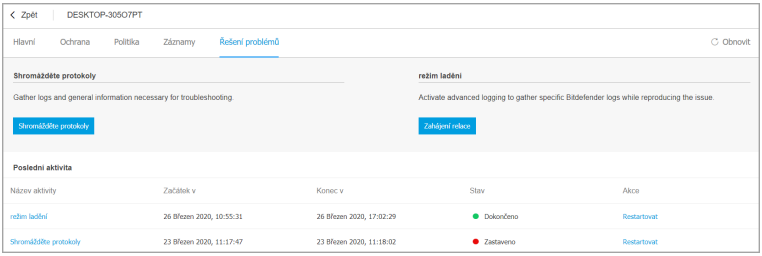


Informační okno - Záložka Zpráv o Skenu

Karta řešení problémů

Tato část je věnována činnosti agentů odstraňujících problémy . Z kontroly koncových bodů můžete shromažďovat obecné nebo konkrétní protokoly nebo provádět akce týkající se aktuálních událostí při odstraňování problémů i zobrazit předchozí aktivitu.

Důležité
Řešení problémů je k dispozici pro Windows, Linux, MacOS a všechny typy bezpečnostních serverů.



Informační okno - karta Odstraňování problémů

- **Shromážděte protokoly**

Tato možnost vám pomůže shromáždit sadu protokolů a obecných informací nezbytných pro odstraňování problémů, jako jsou nastavení, aktivní moduly nebo aplikovaná politika specifická pro cílový počítač. Všechna vygenerovaná data jsou uložena v archivu.

Doporučujeme použít tuto možnost, pokud není jasná příčina problému .

Spuštění procesu na odstraňění problémů:

1. Klikněte na tlačítko **Shromažďovat protokoly**. Zobrazí se konfigurační okno.
2. V části **Logs Storage** zvolte umístění úložiště:
   - **Cílový počítač** : archiv protokolů je uložen na zadanou místní cestu. Cesta není konfigurovatelná pro bezpečnostní servery.
   - **Sdílená síť** : archiv protokolů je uložen na zadanou cestu ze sdíleného umístění.

   Pomocí možnosti **Uložit protokoly také na cílovém počítači** můžete kopii archivu protokolů uložit na postiženém počítači jako zálohu.
3. Vyplňte potřebné informace (cestu k umístění, přihlašovací údaje pro síťové sdílení, cesta ke sdílenému umístění) v závislosti na vybraném umístění.
4. Klikněte na tlačítko **Shromažďovat protokoly**.

- **režim ladění**

  V relaci Debug můžete aktivovat pokročilé protokolování na cílovém počítači a shromažďovat konkrétní protokoly při reprodukci problému.

  Tuto možnost byste měli použít, když jste zjistili, který modul způsobuje problémy, nebo na doporučení Enterprise Bitdefender Support. Všechna vygenerovaná data jsou uložena v archivu.

  Spuštění procesu na odstraňění problémů:

  1. Klikněte na tlačítko **Zahájit relaci**. Zobrazí se konfigurační okno.
  2. V části **Typ problému** vyberte problém, který podle vás ovlivňuje počítač.

     Typy problémů pro počítače se systémem Windows a MacOS:

Typ problému	Příklad použití
Antimalware (ruční přístup a skenování)	– Zpomalení koncového bodu

Typ problému	Příklad použití
	– Odpověď na program nebo systémový prostředek trvá příliš dlouho – Proces skenování trvá déle než obvykle – Žádné připojení k hostiteli chyba zabezpečení
Chyba aktualizace...	– Chybové zprávy přijaté během aktualizace obsahu produktu nebo zabezpečení
Řízení obsahu (kontrola provozu a kontrola uživatelů)	– Webová stránka se nenačte – Prvky webové stránky nejsou zobrazeny správně
Připojení cloudových služeb	– Koncový bod nemá připojení ke službě Bitdefender Cloud Services
Obecné problémy s produktem (rozsáhlé protokolování)	– Reprodukujte obecný hlášený problém s podrobným protokolováním

Typy problémů pro počítače se systémem Linux:

Typ problému	Příklad použití
Antimalware a aktualizace	– Proces skenování trvá déle než obvykle a vyžaduje více zdrojů – Chybové zprávy přijaté během aktualizace obsahu produktu nebo zabezpečení – Koncový bod se nepodařilo připojit ke konzoly GravityZone.
Obecné problémy s produktem (rozsáhlé protokolování)	– Reprodukujte obecný hlášený problém s podrobným protokolováním

Typy problémů pro bezpečnostní servery:

Typ problému	Příklad použití
Antimalware (ruční přístup a skenování)	Jakékoli neočekávané chování bezpečnostního serveru, včetně: – Virtuální stroje nejsou řádně chráněny – Úlohy skenování antimalwaru se nepodaří spustit nebo trvat déle, než se očekávalo – Aktualizace produktu nejsou správně nainstalovány – Porucha generického bezpečnostního serveru (démoni bd neběží)
Komunikace s GravityZone Control Center	Jakékoli neočekávané chování pozorované z konzole GravityZone: – Virtuální stroje nejsou v konzoli GravityZone správně hlášeny – Problémy s politikou (zásada se neuplatňuje) – Bezpečnostní server nemůže navázat spojení s konzolí GravityZone **Poznámka** Tuto metodu použijte na doporučení Bitdefender Enterprise Support.

3. Pro **Debug session duration** vyberte časový interval, po kterém se automaticky ukončí ladicí relace.

   Poznámka
   Doporučujeme ručně zastavit relaci pomocí možnosti **Dokončit relaci**, hned poté, co problém zopakujete.

4. V části **Logs Storage** zvolte umístění úložiště:
   – **Cílový počítač** : archiv protokolů je uložen na zadanou místní cestu. Cesta není konfigurovatelná pro bezpečnostní servery.

– **Sdílená síť** : archiv protokolů je uložen na zadanou cestu ze sdíleného umístění.

Pomocí možnosti **Uložit protokoly také na cílovém počítači** můžete kopii archivu protokolů uložit na postiženém počítači jako zálohu.

5. V závislosti na vybraném umístění vyplňte potřebné informace (cesta, přihlašovací údaje pro síťové sdílení, cesta ke sdílenému umístění).
6. Klikněte na tlačítko **Zahájit relaci**.

Důležité
Na postiženém počítači můžete současně spustit pouze jeden postup odstraňování problémů (**Shromažďovat protokoly** / **Debugovací relace**).

- **Historie odstraňování problémů**

Sekce **Poslední aktivita** představuje aktivitu pro odstraňování problémů na postiženém počítači. Mřížka zobrazuje pouze posledních 10 událostí odstraňování problémů v chronologickém obráceném pořadí a automaticky odstraní aktivitu starší než 30 dnů.

Mřížka zobrazuje podrobnosti o každém procesu odstraňování problémů.

Proces má hlavní a střední status.. V závislosti na zvolených nastaveních může nastat následující status, ve kterém musíte podniknout kroky:

– **Probíhá (připraven k reprodukci problému)** - přistupujte k postiženému počítači ručně nebo vzdáleně a problém zopakujte.

Máte několik možností, jak zastavit proces odstraňování problémů:

– **Dokončit relaci** : ukončí ladicí relaci a proces shromažďování v cílovém počítači a zároveň uloží všechna shromážděná data do určeného umístění úložiště.

Doporučujeme tuto možnost použít ihned po zopakování problému.

– **Zrušit**: tato možnost zruší proces a nebudou shromažďovány žádné protokoly.

Tuto možnost použijte, pokud nechcete shromažďovat žádné protokoly z cílového počítače.

– **Vynucený Stop**: násilně zastaví proces odstraňování problémů.

Tuto možnost použijte, když zrušení relace trvá příliš dlouho nebo cílový počítač nereaguje a za několik minut budete moci zahájit novou relaci.

Postup restartování procesu odstraňování problémů:

– **Restartovat** : toto tlačítko spojené s každou událostí a umístěné pod **Akce** restartuje vybranou aktivitu při odstraňování problémů při zachování předchozího nastavení.

Důležité

– Chcete-li zajistit, aby konzola zobrazovala nejnovější informace, použijte tlačítko **Obnovit** v pravé horní části stránky **Odstraňování problémů**.

– Pro více informací o konkrétní události klikněte na název události v mřížce.

6.2.3. Organizace počítačů do skupin

Skupiny počítačů můžete spravovat v levém panelu na stránce **Síť**.

Hlavní výhodou této možnosti je, že můžete používat skupinová oprávnění pro splnění různých bezpečnostních požadavků.

Počítače importované z Active Directory jsou seskupené pod složkou **Active Directory**. Skupiny Active Directory nemůžete upravovat. Můžete pouze prohlížet a spravovat odpovídající počítače.

Všechny počítače nepatřící k Active Directory nalezené ve vaší síti budou umístěny pod **Vlastní skupiny**, kde je můžete uspořádat do skupin dle svých potřeb. Pod **Vlastními skupinami** můžete vytvořit, smazat, přejmenovat a přesunout skupiny počítačů v rámci stromové struktury na míru.

Poznámka

- Skupina může obsahovat jak počítače, tak další skupiny.
- Při výběru skupiny v levém panelu můžete prohlížet všechny počítače kromě těch, které jsou umístěny do jejích podskupin. Pro zobrazení všech počítačů zahrnutých ve skupině a jejích podskupinách, klikněte na menu **Filtry** nacházející se v horní části tabulky a vyberte **Všechny objekty opakovaně** v sekci **Hloubka**.

Vytváření Skupin

Předtím než začnete vytvářet skupiny, přemýšlejte nad důvodem proč je potřebujete a vytvořte si nějaké schéma skupin. Například, můžete seskupit všechna koncová zařízení podle jednoho, nebo smícháním následujících kritérií:

- Organizační struktura (Sales, Marketing, Záruka Kvality, Vývoj Softwaru, Správa, atd.).
- Bezpečnostní požadavky (Desktopy, Laptopy, Servery, atd.).
- Pozice (Ústředí, Místní Kanceláře, Vzdálení Pracovníci, Domácí Kanceláře, atd.).

Pro organizování vaší sítě do skupin:

1. V levém panelu vyberte **Vlastní skupiny**.
2. Klikněte na ⊕ tlačítko **Přidat skupinu** v horní části levého panelu
3. Zadejte působivé jméno pro skupinu a klikněte na **OK**. Nová skupina se zobrazí pod složkou **Vlastní skupiny**.

Přejmenování Skupin

Pro přejmenování skupiny:

1. Vyberte skupinu v levém panelu.
2. Klikněte na ✎ tlačítko **Editovat skupinu** v horní části levého panelu.
3. Zadejte nové jméno do odpovídajícího pole.
4. Potvrďte kliknutím na **OK**.

Přesouvání skupin a počítačů

Můžete přesouvat objekty do **Vlastní skupiny** kamkoliv uvnitř hierarchie skupiny. Pro přesun objektu, přetáhněte a umístěte ho z pravého panelu do skupiny v levém panelu.

Poznámka

Objekt, který je přesunut bude dědit nastavená práva nadřazené skupiny, pokud nejsou žádná jiné práva přidělena přímo k danému objektu. Pro více informací o dědění práv, obraťte se na „Zásady zabezpečení“ (str. 212).

Mazání Skupin

Mazání skupin je finální akce. Výsledkem je, že bezpečnostní agent, který byl nainstalován na cílovém koncovém zařízení bude odstraněn.

Pro smazání skupiny:

1. Klikněte na prázdnou skupinu v levém panelu **záložka Síť**.
2. Klikněte na ⊖ tlačítko **Odebrat Skupinu** v horní části levého panelu. Je nutné potvrdit kliknutím na **Ano**.

6.2.4. Třídění, Filtrování a Hledání počítačů

V závislosti na počtu koncových zařízení v pravém panelu tabulky můžete projít pár stránek (standardně je zobrazeno pouze 20 objektů na jedné stránce). Pro pohyb mezi stránkami použijte navigační tlačítka ve spodní části tabulky. Můžete změnit počet položek zobrazených na stránku tak, že vyberete nějakou z menu umístěného vedle navigačních tlačítek.

Pokud je záznamů příliš mnoho, můžete použít vyhledávací pole pod hlavičkami sloupců nebo v menu **Filtry** navrchu stránky pro zobrazení pouze těch objektů, které vás zajímají. Například můžete vyhledat konkrétní počítač, nebo zobrazit pouze spravované počítače.

Třídění Počítačů

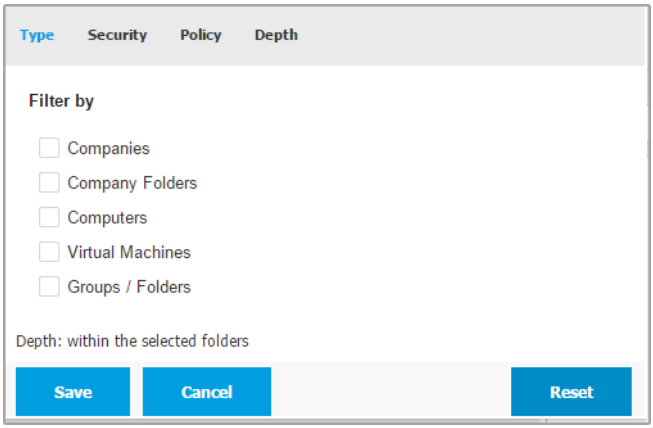
Pro třídění dat podle určitého sloupce, klikněte na hlavičku slupce. Například, pokud chcete počítače seřadit podle jména, klikněte na hlavičku **Název**. Pokud kliknete na hlavičku znovu, počítače se zobrazí v opačném pořadí.

Třídění Počítačů

Filtrování počítačů

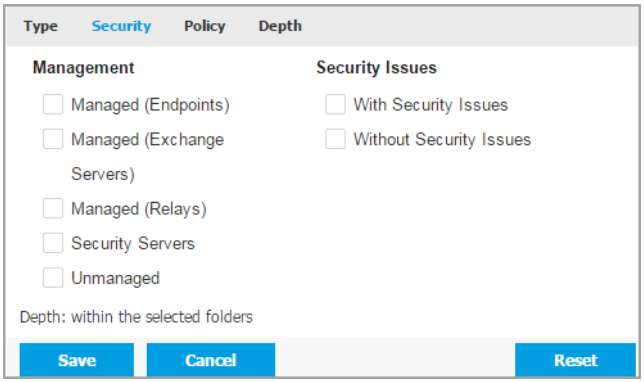
Pro filtrování vašich objektů v síti, použijte menu **Filtry** nahoře od oblasti panelů sítě.

1. Vyberte skupinu v levém panelu.
2. Klikněte na menu **Filtry** navrchu od oblasti panelů sítě.
3. Použijte následující filtrovací kriteria:
   - **Typ**. Vyberte typ objektu, které chcete zobrazit (počítače, virtuální stroje, složky).



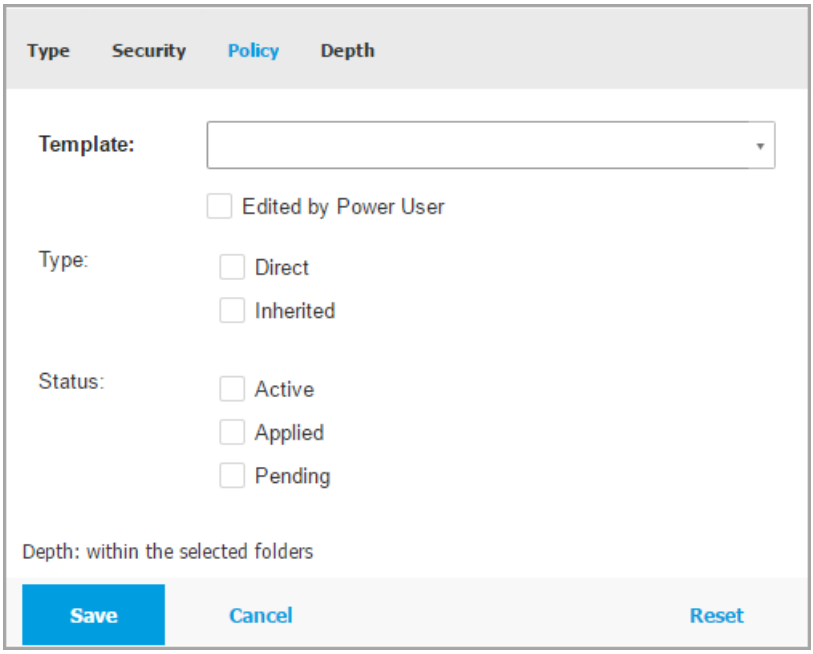
Počítače - filtrovat podle typu

- **Zabezpečení**. Zvolte zobrazení počítačů podle správy ochrany, stavu zabezpečení nebo čekající aktivity.



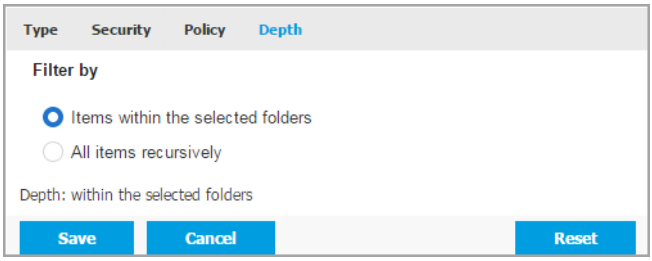
Počítače - filtrovat podle zabezpečení

- **Práva**. Vyberte šablonu pravidla, podle kterého chcete počítače filtrovat, typ přiřazení pravidla (Přímo nebo Zděděné), a také stav přiřazení pravidla (Aktivní, Aplikované nebo Čekající). Můžete také zobrazit pouze objekty s právy nastavenými v režimu Pokročilého Uživatele.



Počítače - filtrovat podle zásad

- **Struktura**. Při spravování stromové struktury sítě, se počítače umístěné do podskupin nezobrazí, když vyberete hlavní skupinu. Pro zobrazení všech počítačů v aktuální skupině a všech jejích podskupinách vyberte **Všechny objekty opakovaně**.



Počítače - filtrovat podle hloubky

Při zobrazování všech objektů opakovaně, Control Center je zobrazí v prostém seznamu. K nalezení objektu, vyberte objekt který vás zajímá a klikněte na tlačítko **Přejít do kontejneru** navrchu tabulky. Budete přesměrován do nadřazeného kontejneru vybraného objektu.

Poznámka
Můžete zobrazit všechny kriteria filtrování ve spodní části okna **Filtry**. Jestli chcete smazat všechny filtry, klikněte na tlačítko **Reset**.

4. Klikněte na **Uložit** pro filtrování počítačů podle vybraných kriterií. Filtr zůstává aktivní v záložce **Síť** dokud se neodhlásíte nebo neresetujete filtr.

Hledání počítačů

1. Vyberte požadovanou skupinu v levém panelu.
2. Do příslušného pole pod záhlavím sloupců v pravém panelu zadejte hledaný výraz. Například, zadejte IP adresu počítače, který hledáte, do pole **IP**. V tabulce se zobrazí pouze odpovídající počítač.

   Vymažte vše z vyhledávače pro zobrazení celého seznamu počítačů.

Hledejte počítače

6.2.5. Spuštěné úlohy

Ze stránky **Síť** můžete na počítačích na dálku spouštět několik administrativních úloh.

Můžete provádět následující akce:

- „Sken“ (str. 68)
- „Sken pro IOC“ (str. 77)
- „Kontrola rizik“ (str. 80)
- „Úlohy balíčků“ (str. 81)
- „Exchange Scan“ (str. 84)
- „Instalovat“ (str. 88)

- „Odinstalovat klienta“ (str. 94)
- „Aktualizace klienta“ (str. 94)
- „Přenastavení klienta“ (str. 95)
- „Opravte klienta“ (str. 97)
- „Restartovat stroj“ (str. 98)
- „Vyhledání sítě“ (str. 98)
- „Vyhledání aplikací“ (str. 99)
- „Aktualizovat Security Server“ (str. 99)
- „Přidávání Vlastních Nástrojů“ (str. 100)

Můžete si vybrat vytváření úloh individuálně pro každý počítač nebo skupinu počítačů. Například můžete na dálku nainstalovat bezpečnostního agenta na skupinu nespravovaných počítačů. Později můžete vytvořit skenovací úlohu pro určitý počítač z té samé skupiny.

Pro každý počítač můžete spouštět pouze kompatibilní úlohy. Například, pokud zvolíte nespravovaný počítač, můžete zvolit pouze instalaci bezpečnostního agenta, se všemi ostatními úlohami vypnutými.

V případě skupiny bude zvolená úloha vytvořena pouze pro kompatibilní počítače. Pokud žádný počítač ve skupině není kompatibilní se zvolenou úlohou, budete upozorněni, že úlohu nebylo možné vytvořit.

Jakmile je vytvořena, úloha se spustí automaticky na všech počítačích, které jsou online. Pokud je počítač offline, úloha se spustí jakmile bude znovu online.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

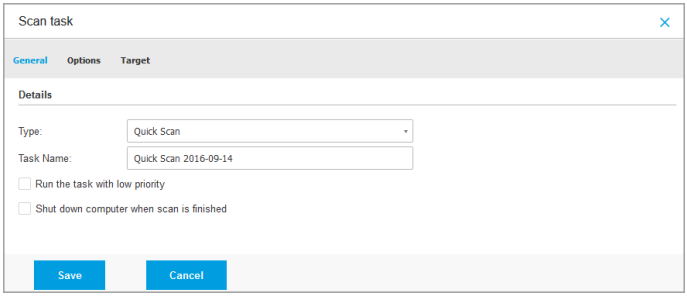
Sken

Pro vzdálené spuštění úlohy skenování na jednom nebo více počítačích:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Označte políčka počítačů nebo skupin, které chcete skenovat.
5. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Sken**.

   Zobrazí se konfigurační okno.
6. Konfigurace parametrů skenu:

- Na kartě **Obecné** si můžete zvolit typ skenování a můžete zadat název skenovací úlohy. Název skenovací úlohy je zamýšlený, aby vám pomohl jednoduše identifikovat stávající sken v záložce **Úlohy**.



Úloha skenování počítačů - konfigurace obecných nastavení

Z nabídky **Typ** zvolte typ skenování:

– **Rychlý sken** používá k nalezení malwaru ve vašem systému cloudovou detekci. Tento typ skenování je přednastaven tak, aby umožnil pouze skenování kritických umístění v operačních systémech Windows a Linux. Provedení rychlého skenu obvykle trvá méně než minutu a využije jen zlomek systémových prostředků, které potřebuje běžný sken.

  Pokud je nalezen malware nebo rootkity, Bitdefender automaticky provede dezinfekci. Pokud je soubor z jakéhokoli důvodu nemožné dezinfikovat, je přesunut do karantény. Tento typ skenování ignoruje podezřelé soubory.

– **Kompletní sken** otestuje celý počítač na přítomnost malwaru ohrožujícího jeho bezpečnost, jako viry, spyware, adware, rootkity a další.

  Bitdefender se automaticky pokusí vyčistit soubory, které byli identifikované jako malware. Pokud malware nemůže být odstraněn, je přesunut do karantény, kde nemůže napáchat žádné škody. Podezřelé soubory jsou ignorovány. Chcete-li také podniknout kroky proti podezřelým souborům nebo podniknout další běžné akce s infikovanými soubory, poté vybrat a spustit Vlastní Skenování.

– **Skenování paměti** kontroluje programy spuštěné v paměti počítače.

– **Skenování sítě** je typ vlastního skenování, umožňující skenování síťových jednotek pomocí bezpečnostního agenta Bitdefender nainstalovaného na cílovém koncovém bodě.

  Aby síťové skenování fungovalo:

  - Je nutné zadat úlohu pouze jednomu koncovému bodu ve vaší síti.
  - Musíte zadat pověření uživatelského účtu s oprávněními pro čtení/psaní na cílové síťové jednotky, aby bezpečnostní agent mohl přistupovat a provádět opatření pro tyto síťové jednotky. Požadovaná ověření mohou je možné nastavit na kartě **Cíl** v okně úloh.

– **Vlastní sken** vám umožňuje zvolit umístění, která chcete skenovat, a nastavit možnosti skenování.

Pro skenování paměti, sítě, a vlastní skenování máte také následující možnosti:

– **Spustit sken s nízkou prioritou**. Označte toto políčko pro snížení priority skenovacího procesu a umožněte ostatním programům pracovat rychleji. Toto prodlouží čas potřebný k dokončení skenovacího procesu.

  Poznámka
  Tato možnost platí pouze pro Bitdefender Endpoint Security Tools a Endpoint Security (agent pro starší verze).

– **Vypnout počítač po ukončení skenování**. Označte toto políčko, pokud plánujete počítač po nějakou dobu nepoužívat.

  Poznámka
  Tato možnost se vztahuje na Bitdefender Endpoint Security Tools, Endpoint Security (agent pro starší verze) a Endpoint Security for Mac.

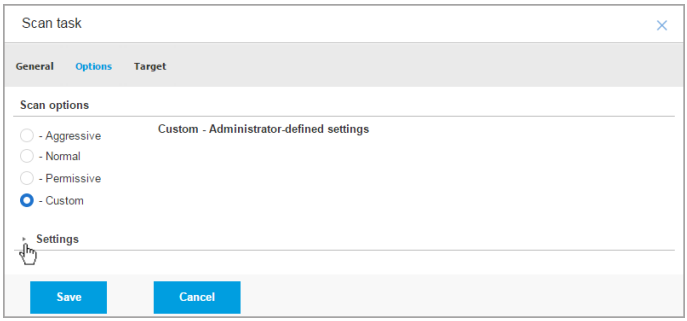
Poznámka
Tyto dvě možnosti se týkají pouze Bitdefender Endpoint Security Tools a Endpoint Security (agent pro starší verze).

Pro vlastní skenování konfigurujte následující parametry:

– Přejděte na kartu **Možnosti** a nastavte parametry skenování. Zvolte úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (agresivní,

normální nebo tolerantní). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

Na základě zvoleného profilu budou parametry skenování v sekci **Nastavení** nastaveny automaticky. Ale pokud si přejete, můžete je nastavit podrobněji. To provedete tak, že označíte políčko **Vlastní** a poté rozbalíte sekci **Nastavení**.



Úloha skenování počítače - konfigurace Vlastního skenování

K dispozici jsou následující možnosti:

- **Soubory.** Pomocí těchto možností upřesněte, které typy souborů chcete skenovat. Můžete nastavit bezpečnostního agenta, aby skenoval všechny soubory (nehledě na příponu souboru), pouze soubory aplikací, nebo určité souborové přípony, které považujete za nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

  Poznámka

  Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

  Pokud si přejete skenovat pouze určité souborové přípony, zvolte v nabídce **Vlastní přípony**, přípony zadejte do pole úprav a po každé stiskněte `Enter`.

Důležité
Bezpečnostní agenti Bitdefender nainstalované na operačních systémech Windows a Linux skenují většinu fomátů .ISO, ale neprovádí na nich žádná opatření.

Možnosti úlohy skenování počítačů - Přidání vlastních přípon

- **Archivy.** Archivy obsahující infikované soubory nepředstavují pro zabezpečení vašeho systému bezprostřední hrozbu. Malware může ovlivňovat váš systém, pouze pokud je infikovaný soubor z archivu extrahován a spuštěn bez zapnuté ochrany v reálném čase. Doporučujeme však archivy skenovat, aby byly detekovány a odstraněny všechny potenciální hrozby, i když nejsou bezprostřední.

  Důležité
  Skenování archivovaných souborů zvyšuje celkovou dobu skenu a vyžaduje více systémových prostředků.

  – **Skenovat uvnitř archivů.** Zvolte tuto možnost, pokud si přejete kontrolovat archivované soubory na malware. Pokud se rozhodnete využít této možnosti, můžete konfigurovat následující optimalizační možnosti:

    - **Omezit velikost archivu na (MB).** Můžete nastavit maximální přijatelnou velikost archivů, které mají být skenovány. Zaškrtněte příslušné políčko a zadejte maximální velikost archivů (v MB).
    - **Maximální hloubka archivu (úrovně).** Zaškrtněte příslušné políčko a z nabídky zvolte maximální hloubku archivu. Pro nejvyšší výkon zvolte nejnižší hodnotu, pro maximální ochranu zvolte nejvyšší hodnotu.

- **Skenovat emailové archivy.** Vyberte tuto možnost, pokud chcete povolit skenování souborů emailových zpráv a emailových databází včetně souborů s formáty jako .eml, .msg, .pst, .dbx, .mbx, .tbb a další.

  Důležité
  Skenování emailových archivů je zdrojově náročné a může ovlivnit výkon systému.

- **Různé.** Vyberte odpovídající políčka pro nastavení požadovaných možností skenování.
  - **Skenovat spouštěcí sektory.** Skenovat zaváděcí sektor systému. Tento sektor pevného disku obsahuje počítačový kód nezbytný k zahájení spouštěcího procesu. Když virus infikuje spouštěcí sektor, jednotka se může stát nepřístupnou a nemusí být možné spustit systém a přistupovat k datům.
  - **Skenovat registr.** Tuto možnost použijte ke skenování klíčů registru. Registr systému Windows je databáze, která uchovává nastavení konfigurací a možností pro součásti operačního systému Windows i pro nainstalované aplikace.
  - **Hledat rootkity.** Tuto možnost zvolte pro skenování rootkitů a objektů skrytých pomocí tohoto softwaru.
  - **Hledat keyloggery.** Zvolte tuto možnost pro skenování keylogger softwaru.
  - **Skenovat síťové složky.** Tato možnost skenuje mountované síťové jednotky.

    Pro rychlé skenování je tato možnost ve výchozím nastavení vypnutá. Úplný sken je aktivován už v základní konfiguraci. Vlastní skenování, pokud jste nastavily stupeň zabezpečení na možnost**Agresivní/Normální**, **Skenovat síť** je automaticky povolené Pokud jste nastavily stupeň zabezpečení na možnost **Přípustné**, **Skenovat Síť** je automaticky zakázané.
  - **Skenovat paměť.** Tuto možnost použijte ke skenování programů běžících v paměti systému.

- **Skenovat cookies.** Tuto možnost zvolte pro skenování souborů cookie, které do vašeho počítače ukládají prohlížeče.
- **Skenovat pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Skenovat pro potenciálně nežádoucí aplikace (PUA).** Potenciálně nežádoucí aplikace (PUA) je program, který může být na PC nežádoucí a někdy bývá součástí freewaru nebo softwaru. Takové programy mohou být nainstalovány bez vědomí uživatele (jsou známé také jako adware), nebo mohou být obsaženy v původní expresní instalační sadě (podporované reklamou). Možný dopad těchto programů zahrnuje zobrazování vyskakovacích oken, instalaci nechtěných nástrojových lišt ve výchozím prohlížeči nebo spuštění několika procesů na pozadí a zpomalení výkonu PC.
- **Skenovat výměnné svazky.** Vyberte tuto možnost pro skenování vyměnitelných zařízení připojených k počítači.

- **Akce.** Podle typu rozpoznaných souboru, následující možnosti jsou provedeny automaticky:
  - **Když bude nalezen infikovaný soubor.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanizmů, které zahrnují malwarové signatury, machine learnign a umělou inteligenci (AI). Bezpečnostní agent Bitdefender může za běžných okolností odstranit malwarový kód z infikovaného souboru a obnovit původní soubor. Této operaci se říká dezinfikace.

    Pokud je nalezen infikovaný soubor, bezpečnostní agent Bitdefender se ho ve výchozím nastavení automaticky pokusí dezinfikovat. Pokud se dezinfekce nezdaří, soubor je přesunut do karantény, která infekci zadrží.

    Důležité
    V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

  - **Když bude nalezen podezřelý soubor.** Soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií

Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé). Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.

Skenování je ve výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení. Soubory v karanténě jsou pravidelně posílány na analýzu do laboratoří Bitdefender. Pokud je přítomnost malwaru potvrzena, je vydána signatura umožňující odstranění malwaru.

– **Když je nalezen rootkit.** Rootkity představují specializovaný software, používaný pro ukrytí souborů před operačním systémem. Přestože ve své podstatě nejsou škodlivé, rootkity jsou často využívány pro ukrytí malwaru nebo pro zamaskování přítomnosti narušitele v systému.

  Nalezené rootkity a skryté soubory jsou ve výchozím nastavení ignorovány.

Přestože to nedoporučejeme, výchozí nastavení můžete změnit. Můžete určit druhou akci, která bude provedena v případě selhání té první, a různé akce pro každou kategorii. Z odpovídajících nabídek zvolte první a druhou akci, které budou provedeny na každém typu rozpoznaného souboru. K dispozici jsou následující akce:

vyléčit
Odstranit malwarový kód z infikovaných souborů. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech.

Přesunout soubory do karantény
Přesunout odhalené soubory z jejich současného umístění do karanténní složky. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Můžete spravovat soubory v karanténě ze záložky Karanténa v konzoli.

Odstranit
Odstranit odhalené soubory z disku, bez jakéhokoli upozornění. Této akci se doporučujeme vyhýbat.

Ignorovat
S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu.

– Přejděte na kartu **Cíl** a nastavte umístění, která si přejete skenovat na cílových počítačích.

V sekci **Cíl skenování** můžete přidat nový soubor nebo složku ke skenování:

a. Z rozbalovacího menu zvolte přednastavené umístění, nebo zadejte **Určité cesty**, které si přejete skenovat.

b. Určete cestu k objektu, který chcete skenovat, v poli úprav.

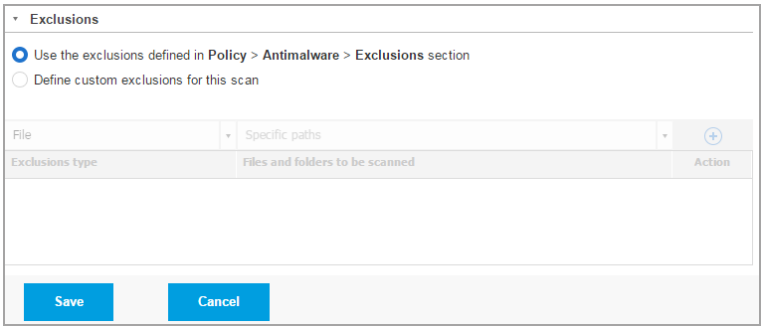
- V případě, že jste zvolili přednastavené umístění, doplňte cestu dle potřeby. Například, pro skenování celé složky `Program Files`, stačí vybrat příslušné přednastavené umístění z rozbalovací nabídky. Pro skenování konkrétní složky v `Program Files`, musíte doplnit cestu přidáním lomítka (\) a názvu složky.
- Pokud jste vybrali **Určité cesty**, zadejte celou cestu k objektu, který má být oskenován. Pro jistotu, že je cesta platná na všech cílových počítačích, doporučujeme používat systémové proměnné (tam, kde je to vhodné). Další informace o systémových proměnných naleznete na „Systémové proměnné“ (str. 567).

c. Klikněte na odpovídající tlačítko ⊕ **Přidat**.

Klikněte na něj pro úpravu existujícího umístění. Klikněte na odpovídající tlačítko ⊗ **Odstranit** pro odstranění umístění ze seznamu.

Pro úlohy skenování sítě musíte zadat pověření uživatelského účtu s oprávněními pro čtení/psaní na cílové síťové jednotky, aby bezpečnostní agent mohl přistupovat a provádět na nich opatření.

Klikněte na sekci **Výjimky**, pokud si přejete definovat výjimky.



Úloha skenování počítačů - Definování výjimek

Můžete použít buď výjimky nastavené podle pravidel, nebo definovat určité výjimky pro aktuální skenovací úlohu. Pro více detailů ohledně výjimek, se prosím odkažte na „Výjimky“ (str. 280).

7. Kliknutím na **Uložit** vytvoříte úlohu skenování. Zobrazí se potvrzovací okno.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

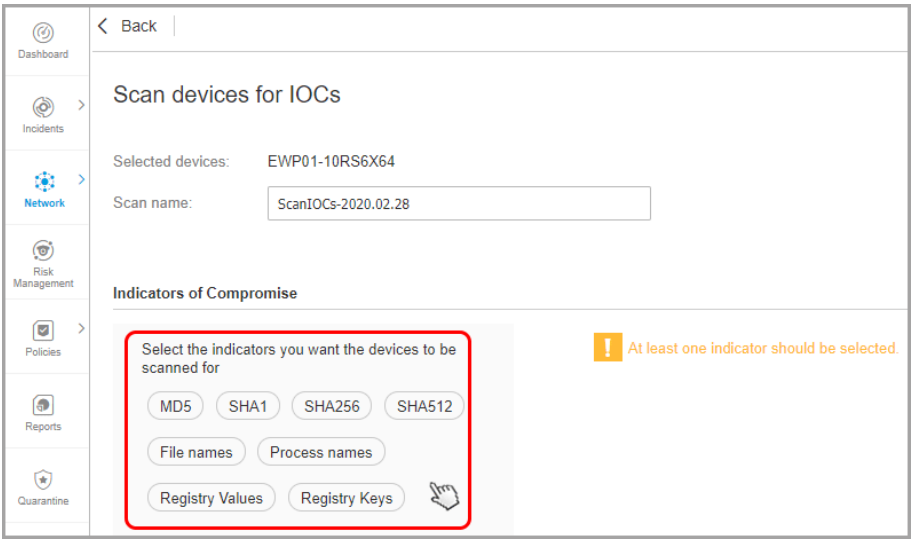
Poznámka
Pro naplánování skenovací úlohy přejděte na stránku **Pravidla**, zvolte pravidla přiřazená k počítačům, které vás zajímají, a přidejte skenovací úlohu v sekci **Antimalware > Na vyžádání**. Další informace viz „Manuální“ (str. 261).

Sken pro IOC

Kdykoli si můžete vybrat, zda chcete na vybraných koncových bodech spustit skenování známých indikátorů kompromisu (IOC) na vyžádání, a to následujícím způsobem:

1. Jděte do záložky **Síť**.
2. Procházejte kontejnery a vyberte koncové body, které chcete prohledat.
3. Klikněte na tlačítko **Úkoly** a vyberte **Hledejte IOC** .

   Zobrazí se konfigurační stránka, kde musíte vybrat typ indikátorů, které se berou v úvahu při skenování IOC.



Konfigurace úlohy Scan pro IOC

Poznámka
Chcete-li vytvořit platný úkol, musíte vybrat alespoň jeden typ indikátoru kompromisu.

4. Vyberte jeden nebo více typů IOC, které chcete při skenování vzít v úvahu, a do nově přidaného pole zapište známý název IOC.

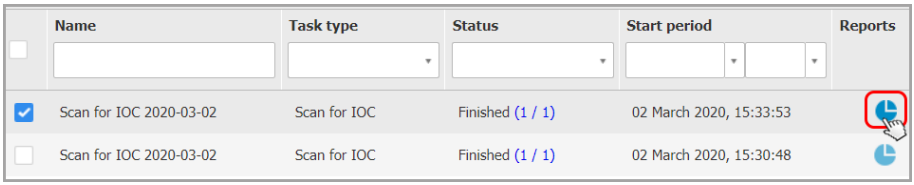
Přidejte IOC

Můžete si vybrat z následujících typů:

- MD5
- SHA1
- SHA256
- SHA512
- Názvy souborů
- Názvy Procesů
- Hodnoty registru
- Klíče registru

Poznámka
Obsah přidaný do každého pole musí být platný. Pokud není uvedeno jinak, budete vyzváni varovným signálem a zprávou.

5. Klepnutím na **Uložit** vytvořte a spusťte úlohu **Vyhledat IOC** . Zobrazí se potvrzovací okno.
   Průběh úkolu můžete zkontrolovat na stránce **Síť** / **Úkoly** .



Průběh úlohy

6. Po úspěšném dokončení úlohy můžete kliknout na tlačítko **Přehledy** pro načtení vygenerované zprávy a určení dopadu naskenovaného IOC.

Platné přípony souborů pro IOC přidané k úkolu zahrnují: `exe`, `dll`, `com`, `scr`, `jar`, `msi`, `msc`, `bat`, `ps1`, `vbs`, `vbe`, `js`, `jse`, `wsf`, `wsh`, `psc1`, `lnk`, `doc`, `docx`, `docm`, `xls`, `xlsx`, `xlsm`, `ppt`, `pptx`, `pptm`, `eml`, `rtf`, `pdf`, `html`, `ppsx`, `pps`, `ppsm`, `pot`, `potx`, `potm`, `ocx`, `sys`, `fnr`, `fne`, and `pif`.

Úloha **Sken na IOC** prohledá následující umístění:

- %Windows%\System32\Drivers
- %Windows%\System32\WindowsPowerShell\v1.0
- %Windows%\system32\config\systemprofile\AppData
- %Windows%\System32\Tasks
- %Windows%\System32\wbem
- %Windows%\SysWOW64\WindowsPowerShell\v1.0
- %Windows%\SysWOW64\config\systemprofile\AppData
- %Windows%\SysWOW64\sysprep
- %Windows%\Scripts
- %Windows%\System
- %Windows%\Web
- %Users%

Důležité
Úlohy **Sken na IOC** se nespustí / nezdaří v koncových bodech v následujících situacích:

- Koncový bod nemá operační systém Windows.
- Licence pro agenta Bitdefender koncového bodu je neplatná.
- Modul **EDR** není nainstalován v BEST klientovi nainstalovaném v cílových koncových bodech.
- V současné době je ve frontě více než 100 úloh **Sken na IOC** .
- Neplatná data zadává uživatel na stránce konfigurace úlohy **Sken na IOC** .

Kontrola rizik

Následovně můžete kdykoliv spustit úlohu kontroly rizik na vybraných koncových stanicích:

1. Jděte do záložky **Síť**.
2. Procházejte složky na levé straně okna a vyberte koncové stanice, které chcete skenovat.

3. Klikněte na tlačítko **Úkoly** a vyberte **Kontrola rizik** .

   Zobrazí se zpráva vyžadující potvrzení spuštění úlohy kontroly rizik.

   Poznámka
   Úloha kontroly rizik se spustí se všemi indikátory rizika aktivovanými ve výchozím nastavení.

4. Po úspěšném dokončení úlohy můžete přejít na kartu Miskonfigurace na stránce **Bezpečnostní rizika** , analyzovat je a vybrat, které indikátory v případě potřeby ignorovat.

   Celkové skóre podnikového rizika bude přepočítáno na základě ignorovaných ukazatelů rizika.

   Poznámka
   Úplný seznam indikátorů a jejich popis naleznete v tomto článku na KB.

Důležité
Úloha **Kontrola rizik** selže / se na koncových stanicích nespustí v následujících situacích:

- Koncový bod nemá operační systém Windows.
- Licence pro agenta Bitdefender koncového bodu je neplatná.
- Politika použitá pro koncový bod má deaktivovaný modul Řízení rizik (Risk Management module).

Úlohy balíčků

Doporučejeme pravidelnou kontrolu aktualizací softwaru a jejich co nejrychlejší aplikaci. GravityZone tento proces provádí automaticky skrze bezpečnostní pravidla, ale pokud potřebujete aktualizovat software na určitých koncových bodech neprodleně, spusťte následující úlohy v tomto pořadí:

1. Skenování balíčků
2. Instalace balíčků

Podmínky

- Bezpečnostní agent s modulem Správa balíčků je nainstalovaný na koncových bodech.

- Aby proběhly úlohy skenování a instalace úspěšně, koncové body s Windows musí splňovat následující podmínky:
  - **Důvěryhodné autority pro certifikaci rootů** ukládá certifikát **DigiCert Assured ID Root CA**.
  - **Zprostředkující certifikační autority** zahrnují **DigiCert SHA2 Assured ID Code Signing CA**.
  - Koncové body nainstalovaly opravy pro systémy Windows 7 a Windows Server 2008 R2 uvedené v tomto článku společnosti Microsoft: Microsoft Security Advisory 3033929

Skenování balíčků

Koncové body se zastaralým softwarem jsou náchylné k útokům. Doporučujeme pravidelně kontrolovat software nainstalovaný na vašich koncových zařízeních a co nejdříve je aktualizovat. Pro skenování vašich koncových bodů pro chybějící balíčky:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny koncové body z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Zvolte cílové koncové body.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Skenování balíčků**. Zobrazí se potvrzovací okno.
6. Klikněte na **Ano** pro potvrzení skenování.

   Jakmile je úloha dokončena, GravityZone přidá v Inventáři balíčků všechny balíčky, které software potřebuje. Více informací naleznete na „Inventář Balíčků“ (str. 191).

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka
Pro naplánování skenování balíčků upravte pravidla přiřazená k cílovým koncovým bodům a nastavte parametry v sekci **Správa balíčků**. Další informace viz „Patch Management“ (str. 326).

Instalace balíčků

Pro instalaci jednoho nebo více balíčků na koncové cílové body:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny koncové body z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Instalace balíčků**.

   Zobrazí se konfigurační okno. Zde můžete vidět všechny balíčky chybějící na cílových koncových bodech.
5. Pokud potřebujete najít konkrétní balíčky, použijte možnosti třízení a filtrování v horní části tabulky.
6. Klikněte na tlačítko **Sloupce** v pravé horní části panelu pro zobrazení pouze relevantních informací.
7. Zvolte balíčky, které chcete nainstalovat.

   Určité balíčky jsou závislé na jiných. V takovém případě jsou automaticky zvoleny spolu s balíčkem.

   Kliknutím na čísla **CVEs** nebo **Produktů** zobrazíte levý panel. Panel obsahuje doplňující informace, jako jsou CVE, který popisuje balíčky co řeší nebo produkty pro které je balíček určen. Po přečtení klikněte na **Zavřít** a skryjte panel.
8. Vyberte **Restartujte koncové body po instalaci záplat či aktualizací pokud je to potřeba** tak aby jste restartovali okamžitě po instalaci záplat či aktualizací, když je restart systému vyžadován. Berte v úvahu, že tato akce může přerušit uživatelské aktivity.
9. Klikněte na **Instalovat**.

   Vytvoří se instalační úloha, společně s pod-úlohami pro každý cílový koncový bod.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka

- Pro naplánování nasazení balíčků upravte pravidla přiřazená k cílovým koncovým bodům a nastavte parametry v sekci **Správa balíčků**. Další informace viz „Patch Management“ (str. 326).

- Můžete také nainstalovat záplatu ze stránky **Inventář záplat (Patch Inventory)**, počínaje od konkrétní záplaty, o kterou se zajímáte. V tomto případě vyberte záplatu či aktualizaci ze seznamu a klikněte na tlačítko **Instalace (Install)** na vrchní straně tabulky a nakonfigurujte detaily k instalaci záplat či aktualizací. Více informací naleznete na „Instalování Balíčků“ (str. 195).
- Poté co nainstalujete záplatu či aktualizaci, doporučujeme zaslat úlohu Sken hledání záplat či aktualizací (Patch Scan) na všechny cílené koncové body. Tato úloha akttualizuje informace o záplatách a aktualizacích uložené v GravityZone pro vaše spravované sítě.

Odinstalovat záplaty či aktualizace můžete takto:

- Vzdáleně na dálku, tím že pošlete úlohu odinstalace záplat (patch uninstall task) z GravityZone.
- Lokálně na koncovém bodu. V tomto případě se musíte přihlásit jako administrator přímo na koncovém bodu a spustit odinstalátor manuálně.

Exchange Scan

Databázi Exchange serveru můžete skenovat na dálku spuštěním úlohy **Skenování Exchange**.

Pro skenování databáze Exchange musíte povolit skenování na vyžádání skrze poskytnutí pověření administrátora Exchange. Další informace viz „Skenování Exchange Store“ (str. 350).

Pro skenování databáze Exchange Serveru:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Z levého panelu, vyberte skupinu obsahující cílový Exchange Server. Můžete najít server zobrazený v pravém panelu.

   Poznámka
   Volitelně si můžete aplikovat filtry pro rychlé nalezení cílového serveru:
   - Klikněte na nabídku **Filtry** a zvolte následující možnosti: **Spravované (Exchange servery)** z karty **Zabezpečení** a **Všechny položky rekurzivně** z karty **Hloubka**.
   - Zadejte název serveru nebo IP adresu do pole příslušné hlavičky sloupce.

4. Vyberte zaškrtávací pole u Exchange Serveru, kde chcete skenovat databázi.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Skenování Exchange**. Zobrazí se konfigurační okno.

6. Konfigurace parametrů skenu:
   - **Obecné.** Zvolte pro úlohu definující jméno.

     Pro rozsáhlé databáze může skenování trvat velmi dlouho a může ovlivnit výkon serveru. V mnoha případech, vyberete zaškrtávací pole **Přerušit sken pokud zabere dále jak** a vyberte vyhovující časový interval z příslušných menu.
   - **Cíl.** Zvolte kontejnery a objekty, které mají být skenovány. Můžete si zvolit skenování mailových schránek, veřejných složek, nebo obou. Kromě emailů, můžete vybrat ke skenování objekty jako jsou **Kontakty**, **Úlohy**, **Schůzky** a **Položky pošty**. Navíc můžete pro skenovaný obsah nastavit následující omezení:
     – Pouze nepřečtené zprávy
     – Pouze položky s přílohami
     – Pouze nové objekty, přijaté za určitý časový interval

     Například, můžete vybrat skenovat emaily z uživatelských mailboxů, přijatých v posledních 7 dnech.

     Označte zaškrtávací pole **Výjimky**, pokud si přejete definovat výjimky ve skenování. Pro vytvoření výjimky, použijte pole z hlavičky tabulky jako například:
     a. Z nabídky zvolte typ úložiště.
     b. Na základě typu úložiště, zadejte objekt, který má být vyloučen:

Typ úložiště	Formát objektu
Mailbox	Emailová adresa
Veřejná Složka	Cesta složky od kořenové složky
Databáze	Identita databáze

     Poznámka
     Pro získání identity databáze použijte Exchange shell příkaz:
     `Get-MailboxDatabase | fl name,identity`

     Můžete zadat pouze jednu položku v danou chvíli. Pokud máte několik objektů stejného typu, musíte definovat tolik pravidel jako je počet objektů.
     c. Kliknutím na tlačítko ⊕ **Přidat** v horní části tabulky výjimku uložíte a přidáte do seznamu.

Pro odstranění pravidla výjimky ze seznamu klikněte na odpovídající tlačítko ⊖ **Odstranit**.

- **Možnosti.** Konfigurujte možnosti skenování pro emaily odpovídající pravidlu:
  - **Skanované typy souborů.** Tuto možnost použijte pro specifikování, které typy souborů chcete aby byli skenovány. Můžete si vybrat aby skenoval všechny soubory (nehledě na jejich příponu), pouze soubory aplikací nebo specifické přípony, které si myslíte, že by mohly být nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

    Poznámka
    Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

    Pokud chcete skenovat pouze soubory s určitou příponou, máte dvě možnosti:
    - **Uživatelem definované přípony**, zde musíte jen poskytnout přípony které mají být skenované.
    - **Všechny soubory, kromě určitých přípon**, kde musíte zadat pouze přípony, které mají být ze skenování vyloučeny.
  - **Maximální velikost příloh / statí emailů (MB).** Označte toto zaškrtávací pole a zadejte hodnotu do příslušného pole, čímž nastavíte maximální přijatelnou velikost připojeného souboru nebo statě emailu, který má být skenován.
  - **Archivujte maximum struktury (úrovní).** Vyberte zaškrtávací pole a vyberte maximální strukturu v příslušném poli. Čím nižší úroveň hloubky, tím je vyšší výkon a nižší třída ochrany.
  - **Skenovat potenciálně nechtěné aplikace (PUA).** Vyberte toto zaškrtávací pole pro skenování možných škodlivých nebo nechtěných aplikací jako je adware, který se nainstaloval do systému bez vědomí uživatele, mění chování vybraných softwarových produktů a snižuje výkon systému.
- **Akce.** Můžete určit akce, které má bezpečností agent automaticky provádět na souborech podle jejich typu.

  Podle typu detekce jsou soubory rozděleny do tří kategorií:
  - **Infikované soubory.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanismů, které zahrnují malwarové signatury, a technologie na bázi machine learning a umělé inteligence (AI).

- **Podezřelé soubory.** Tyto soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé).
- **Neskenovatelné soubory.** Tyto soubory nelze skenovat. Neskenovatelné soubory zahrnují, ale ne výlučně, soubory chráněné heslem, šifrované nebo překomprimované soubory.

Každý typ detekce má jednu hlavní akci a jednu alternativní pro případ, že ta hlavní selže. Přestože to nedoporučejeme, tyto akce je možné změnit v odpovídajících nabídkách. Zvolte akci, kterou si přejete provést:

- **Dezinfikovat.** Odstraní malwarový kód z nakažených souborů a obnoví původní soubor. V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech. Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.
- **Odmítnout / Odstranit email.** Na serverech s rolí Edge Transport je rozpoznaný email odmítnut s chybovým kódem 550 SMTP. Ve všech ostatních případech je email odstraněn bez varování. Této akci se doporučujeme vyhýbat.
- **Odstranit soubor.** Odstraní problémové přílohy bez varování. Této akci se doporučujeme vyhýbat.
- **Nahradit soubor.** Odstraní problémové soubory a přiloží textový soubor, který upozorní uživatele na přijatá opatření.
- **Přesunout sobuor do karantény.** Přesune rozpoznané soubory do složky s karanténou a přiloží textový soubor informující uživatele o přijatých opatřeních. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Soubory v karanténě můžete spravovat ze stránky **Karanténa**.

  Poznámka
  Mějte prosím na paměti, že karanténa pro Exchange servery vyžaduje na oddílu, na kterém je nainstalovaný bezpečnostní agent, místo na pevném disku navíc. Velikost karantény závisí na počtu uložených položek a jejich velikosti.

- **Nedělat nic.** S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu. Skenování je ve

výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení.

– Ve výchozím nastavení, pokud se email shoduje s rámcem pravidel, je s ním speciálně nakládáno v souladu s daným pravidlem, aniž by byl porovnán s jakýmkoli z dalších zbylých pravidel. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel.**

7. Kliknutím na **Uložit** vytvoříte úlohu skenování. Zobrazí se potvrzovací okno.
8. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Instalovat

Pro ochranu vašich počítačů pomocí bezpečnostního agenta Bitdefender, musíte jej nainstalovat na každý z nich.

Důležité
V izolovaných sítích, které nemají přímé připojení k zařízení GravityZone, můžete nainstalovat bezpečnostního agenta s Funkcí Relay. V tomto případě, komunikace mezi GravityZone a dalšími bezpečnostními agenty bude probíhat skrze Relay agenta, který se chová také jako místní aktualizační server pro bezpečnostní agenty chránící izolovanou síť.
Jakmile nainstalujete Relay agenta, bude automaticky zjišťovat nechráněné počítače v té samé síti.

Poznámka

- Doporučujeme ponechat počítač, na který nainstalujete Relay agenta, stále zapnutý.
- Pokud v síti není nainstalovaný žádný Relay agent, detekce nechráněných počítačů může být provedena ručně odesláním úlohy **Nalezení sítě** na chráněný koncový bod.

Zabezpečení Bitdefender je možné nainstalovat na počítače na dálku z Control Center.

Instalace na dálku probíhá na pozadí bez vědomí uživatele.

Varování

Před instalací se ujistěte, že jste z počítačů odinstalovali existující antimalwarový nebo firewallový software. Instalace ochrany Bitdefender přes existující bezpečnostní software může ovlivnit jejich činnost a způsobit závažné systémové problémy. Se zahájením instalace budou Windows Defender a Windows Firewall automaticky vypnuty.

Pokud chcete zavést bezpečnostního agenta na počítač s Bitdefender Antivirus pro Mac 5.X, musíte tento odstranit ručně. Pro návod při postupu se podívejte na tento KB článek.

Při nasazování agenta prostřednictvím linuxového relay musí být splněny následující podmínky:

- Relay musí mít nainstalovaný balíček Samba (`smbclient`) , verzi 4.1.0 nebo novější, `net` aby mohl zavádět agenty Windows.

  #### Poznámka

  Příkaz `net` binární/příkaz je obvykle dodáván s balíčky samba-client a / nebo samba-common. Na některých distribucích systému Linux (například CentOS 7.4) je příkaz `net` instalován pouze při instalaci úplné sady Samba (Common + Client + Server). Ujistěte se, že váš koncový bod přenosu má k dispozici příkaz `net`.

- Cílové koncové body Windows musí mít zapnuté Administrative Share a Network Share.
- Cílové koncové body Linux a Mac musí mít zapnutý SSH a vypnutý firewall.

Pro spuštění instalační úlohy na dálku:

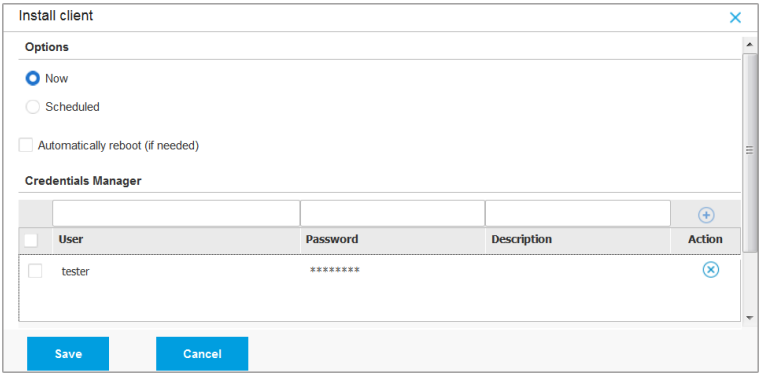
1. Připojte a přihlaste se do Control Center.
2. Jděte do záložky **Síť**.
3. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
4. Vyberte požadovanou skupinu v levém panelu. Všechny dostupné jednotky ve vybrané skupině jsou zobrazeny v pravém panelu tabulky.

   #### Poznámka

   Případně můžete také použít filtry a zobrazit pouze nespravované koncové body. Klikněte na nabídku **Filtry** a zvolte následující možnosti: **Nespravované** z karty **Zabezpečení** a **Všechny položky rekurzivně** z karty **Hloubka**.

5. Vyberte jednotky (koncové body nebo skupiny koncových bodů), na které si přejete nainstalovat zabezpečení.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Instalovat**.

   Zobrazí se průvodce **Instalačním klientem**.



Instalace Bitdefender Endpoint Security Tools z Nabídky úloh

7. V sekci **Možnosti** nastavte čas instalace:
   - **Nyní**, čímž spustíte okamžité zavádění.
   - **Plánovaný**, čímž nastavíte interval opakování zavádění. V tomto případě zvolte svůj požadovaný časový interval (každou hodinu, den nebo týden) a nastavte ho dle svých potřeb.

     Poznámka
     Například, když je na cílovém stroji nutné před instalací klienta nejprve provést určité operace (jako je odinstalace jiného softwaru a restartování OS), můžete zavedení nastavit tak, aby se spustilo každé 2 hodiny. Úloha se na každém koncovém bodě spustí každé 2 hodiny, dokud zavedení neproběhne úspěšně.

8. Pokud chcete, aby se koncové body automaticky restartovaly pro dokončení instalace, zvolte **Restartovat automaticky (je-li potřeba)**.
9. V sekci **Správce pověření** upřesněte administrativní pověření nezbytné pro vzdálenou autentizaci na cílových koncových bodech. Pověření můžete přidat zadáním uživatelského jména a hesla pro každý cílový operační systém.

Důležité
Pro stanice Windows 8.1 musíte poskytnout oprávnění zabudovaného administrátorského účtu, nebo účtu administrátora domény. Více informací naleznete v tomto KB článku.

Pro přidání požadovaných oprávnění OS:

a. Zadejte uživatelské jméno a heslo účtu administrátora do příslušných polí v záhlaví tabulky.

   Pokud jsou počítače v doméně, stačí zadat pověření administrátora domény.

   Při zadávání jména uživatelského účtu použijte konvence systému Windows:

   - Pro stroje s Active Directory použijte tyto syntaxe: `username@domain.com` a `domain\username`. Abyste si mohli být jisti, že pověření budou fungovat, zadejte je v obou tvarech (`username@domain.com` a `domain\username`).
   - Pro stroje Pracovní skupiny stačí zadat pouze uživatelské jméno bez jména pracovní skupiny.

   Můžete také přidat popis, který vám usnadní identifikaci jednotlivých účtů.

b. Klikněte na tlačítko ⊕ **Přidat**. Účet je přidán do seznamu oprávnění.

   Poznámka
   Zadaná pověření jsou automaticky uložena do vašeho Správce pověření, takže je příště už nemusíte zadávat. Do Správce pověření vstoupíte tak, že ukážete myší na vaše uživatelské jméno v pravém horním rohu konzole.

   Důležité
   Pokud jsou poskytnutá pověření neplatná, zavedení klienta na odpovídajících koncových bodech selže. Pokud jsou pověření na cílových koncových bodech změněna, ujistěte se, že jste aktualizovali zadaná pověření OS ve Správci pověření.

10. Označte zaškrtávací pole odpovídající účtům, které chcete použít.

    Poznámka
    Pokud nezvolíte žádná pověření, zobrazí se okno s varováním. Tento krok je povinný pro vzdálenou instalaci bezpečnostního agenta na koncové body.

11. V sekci **Zavaděč** nastavte relay, ke kterému se budou počítače připojovat při instalaci a aktualizacích klienta:

    - **Zařízení GravityZone**, když se koncové body připojují přímo k zařízení GravityZone.

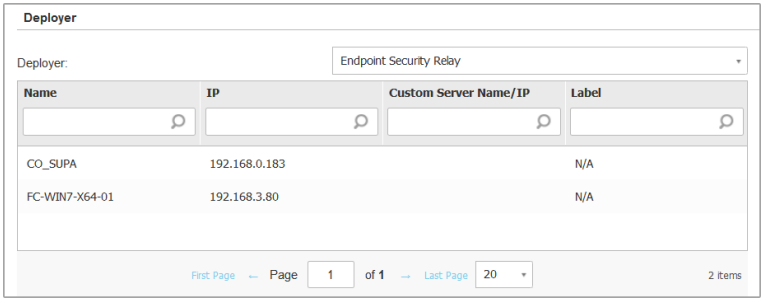
      V tomto případě můžete určit také:

      – Vlastní Komunikační server, zadáním jeho IP nebo jméno hostitele, pokud je třeba.

      – Nastavení proxy, pokud cílové koncové body komunikují se zařízením GravityZone prostřednictvím proxy. V tomto případě zvolte **Použít proxy pro komunikaci** a zadejte požadované nastavení proxy do polí níže.

    - **Endpoint Security Relay**, pokud chcete připojit koncové body k relay klientovi nainstalovanému ve vaší síti. Všechny stroje s funkcí relay, nalezené ve vaší síti, budou uvedeny v níže zobrazené tabulce. Zvolte požadovaný stroj s relay. Připojené koncové body budou komunikovat s Control Center pouze prostřednictvím zvoleného relaye.

      Důležité
      Aby zavedení prostřednictvím relay agenta fungovalo, port 7074 musí být otevřený.



12. Použijte sekci **Další cíle**, pokud chcete zavést klienta na konkrétní stroje ve vaší síti, které se nezobrazují v síťovým inventáři. Rozbalte sekci a zadejte IP adresy nebo jména hostitelů těchto strojů do určeného pole, oddělených čárkou. Můžete přidat tolik IP adres, kolik potřebujete.

13. Pro aktuální zavedení musíte zvolit jeden instalační balíček. Klikněte na seznam **Použít balíček** a zvolte požadovaný instalační balíček. Zde naleznete všechny instalační balíčky, které byly dříve vytvořeny pro váš účet a také výchozí instalační balíčky, dostupné v Control Center.
14. Pokud potřebujete, můžete upravit některá nastavení zvoleného balíčku kliknutím na tlačítko **Upravit** vedle pole **Použít balíček**.

    Nastavení instalačního balíčku se zobrazí níže a vy budete moci provést požadované změny. Více informací o úpravě instalačních balíčků naleznete v GravityZone Instalační Příručce.

    Pokud si přejete uložit změny jako nový balíček, vyberte možnost **Uložit jako balíček**, umístěnou ve spodní části seznamu nastavení balíčku, a zadejte název nového instalačního balíčku.
15. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

Důležité
Pokud požíváte VMware Horizon View Persona Management, tak doporučujeme nakonfigurovat Active Directory skupinové politiky (Group Policy) aby exkludovaly následující Bitdefender procesy (bez úplné cesty):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Tyto výjimky jsou platné dokud je na koncovém bodu nainstalovaný bezpečnostní agent. Pro dalsší detaily, se podívejte na Stránku dokumentace VMware Horizon.

Upgrade klienta

Tato úloha je dostupná pouze v případě, že je v síti nainstalován a rozpoznán agent Endpoint Security. Pro ochranu koncových bodů nové generace, Bitdefender doporučuje upgradovat z Endpoint Security na nový Bitdefender Endpoint Security Tools.

Neupgradované klienty můžete snadno nalézt vygenerováním hlášení stavu upgradů. Podrobnosti o postupu při tvorbě hlášení naleznete zde „Vytváření hlášení“ (str. 497).

Odinstalovat klienta

Pro odinstalaci zabezpečení Bitdefender na dálku:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Označte zaškrtávací pole počítačů, ze kterých chcete odinstalovat bezpečnostního agenta Bitdefender.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Odinstalovat klienta**.
6. Zobrazí se konfigurační okno, které vám umožní provést následující nastavení:
   - Můžete si zvolit ponechání souborů v karanténě na klientském stroji.
   - Pro prostředí integrovaná s vShieldem musíte vybrat požadovaná pověření pro každý stroj, nebo se nepodaří provést odinstalaci. Vyberte **Použít pověření pro integraci s vShield** a poté zkontrolujte všechna příslušná pověření v tabulce Správce pověření zobrazené níže.
7. Kliknutím na **Uložit** vytvoříte úlohu. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka
Pokud chcete znovu nainstalovat ochranu, ujistěte se, že jste nejprve restartovali počítač.

Aktualizace klienta

Pravidelně kontrolujte stav spravovaných počítačů. Pokud naleznete počítač s bezpečnostními problémy, klikněte na jeho jméno pro zobrazení stránky **Informace**. Další informace viz „Stav zabezpečení“ (str. 47).

Zastaralí klienti nebo bezpečnostní obsah představují bezpečnostní rizika. V těchto případech byste měli spustit aktualizaci na odpovídajícím počítači. Toto můžete provést lokálně z počítače, nebo na dálku z Control Center.

Vzdálená aktualizace klienta a obsahu zabezpečení na spravovaných počítačích:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Označte zaškrtávací pole počítačů, na kterých chcete spustit aktualizaci klienta.
5. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Aktualizace**. Zobrazí se konfigurační okno.
6. Můžete se rozhodnout pro aktualizaci pouze produktu, bezpečnostního agenta nebo obou.
7. Pro operační systémy Linux integrované s vShield je nutné zvolit také požadovaná pověření. Označte možnost **Použít pověření pro Linux a integraci s vShield** a poté vyberte příslušná pověření v tabulce Správce pověření zobrazené níže.
8. Klikněte na **Aktualizovat** a spusťte úlohu. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Přenastavení klienta

Ochranné moduly, role a režimy skenování bezpečnostního agenta jsou předem nakonfigurovány v rámci instalačního balíčku. Poté, co nainstalujete bezpečnostního agenta do vaší sítě, můžete kdykoli změnit počáteční nastavení tak, že na dálku odešlete úlohu**Přenastavit klienta** na požadované spravované koncové body.

Varování
Mějte prosím na paměti, že úloha **Přenastavit klienta** přepíše všechna instalační nastavení a žádné z původních nastavení pak neplatí. Při využívání této úlohy se ujistěte, že jste přenastavili všechna instalační nastavení na cílových koncových bodech.

Poznámka
Úloha **Rekonfigurace klienta (Reconfigure Client)** odtsraní veškeré nepodporované moduly z existujících instalací na legacy Windows systémech.

Nastavení instalace můžete změnit z oblasti **Síť** nebo z reportu **Stav koncových modulů** .

Pro změnu instalačních nastavení na jednom nebo více počítačích:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kterou chcete z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Označte zaškrtávací pole počítačů, u kterých chcete změnit instalační nastavení.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Přenastavit klienta**.
6. Vyberte jednu z následujících akcí:
   - **Přidat**. Přidání nových modulů kromě stávajících.
   - **Odebrat**. Odebere konkrétní moduly ze stávajících.
   - **Seznam shod**. Přizpůsobte nainstalované moduly vašemu výběru.
7. Vyberte moduly a role, které chcete nainstalovat nebo odebrat na cílových koncových bodech.

   Varování
   Nainstalují se pouze podporované moduly. Firewall se například nainstaluje pouze na podporovaných pracovních stanicích Windows.
   Další informace viz GravityZone dostupnost ochranných vrstev .

8. Vyberte **Odebrat konkurenty, pokud je to potřeba** , abyste se ujistili, že vybrané moduly nebudou v konfliktu s jinými řešeními zabezpečení nainstalovanými v cílových koncových bodech.
9. Vyberte jeden z dostupných režimů skenování:
   - **Automatické**. Bezpečnostní agent detekuje, které skenovací stroje jsou vhodné pro prostředky koncového bodu.
   - **Vlastní**. Výslovně si vyberete, které skenovací mechanizmy použít.

     Podrobnosti o dostupných možnostech naleznete v části Vytvoření instalačních balíčků v Instalační příručce.

   Poznámka
   Tato část je k dispozici pouze se **Seznamem shod** .

10. V části **Plánovač** vyberte, kdy bude úloha spuštěna:
    - **Nyní**, což spustí úlohu okamžitě.
    - **Plánovaný**, čímž nastavíte interval opakování zavádění.

      V takovém případě vyberte časový interval (hodinový, denní nebo týdenní) a nakonfigurujte jej podle svých potřeb.
11. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

    Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Opravte klienta

Úlohu Opravit klienta použijte jako počáteční úlohu řešení potíží s libovolným počtem problémů s koncovým bodem. Úloha stáhne nejnovější instalační balíček do cílového koncového bodu a poté provede přeinstalaci agenta.

Poznámka
- The modules currently configured on the agent will not be changed.
- Úloha opravy resetuje agenta zabezpečení na verzi publikovanou na stránce **Součásti, aktualizace, komponenty** .

Odeslání úlohy opravy klienta klientovi:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Zaškrtněte políčka počítačů, kde chcete spustit opravu klienta.
5. Klikněte na tlačítko **Úkoly** v horní části tabulky a zvolte **Opravit klienta** . Zobrazí se potvrzovací okno.
6. Zaškrtněte políčko **Rozumím a souhlasím** a kliknutím na tlačítko **Uložit** úlohu spusťte.

Poznámka
K dokončení úlohy opravy může být vyžadován restart klienta.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Restartovat stroj

Můžete si zvolit vzdálený restart spravovaných počítačů.

Poznámka
Předtím, než restartujete určité počítače, zkontrolujte stránku **Síť > Úlohy**. Cílové počítače mohou stále zpracovávat předtím zadané úlohy.

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Označte políčka počítačů, které chcete restartovat.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Restartovat stroj**.
6. Vyberte možnost plánovaného restartu:
   - Zvolte **Restartovat nyní** a restartujte počítače okamžitě.
   - Zvolte **Restartovat v** a pomocí polí níže naplánujte restartování v požadovaný datum a čas.
7. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Vyhledání sítě

Vyhledání sítě probíhá automaticky prostřednictvím bezpečnostních agentů s funkcí Relay. Pokud v síti nemáte nainstalovaného relay agenta, musíte poslat úlohu pro nalezení sítě z chráněného koncového bodu ručně.

Pro spuštění úlohy vyhledání sítě ve vaší síti:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.

4. Zaškrtněte políčko počítače, který má provádět vyhledání sítě.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Vyhledání sítě**.
6. Zobrazí se potvrzovací okno. Klikněte na **Ano**.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Vyhledání aplikací

Pro vyhledání aplikací ve vaší síti:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kterou chcete z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Vyberte počítače, na kterých chcete provést vyhledání aplikací.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Vyhledání aplikací**.

   Poznámka
   Na zvolených počítačích musí být nainstalovaný a aktivovaný Bitdefender Endpoint Security Tools s Kontrolou aplikací. V opačném případě bude úloha zobrazena šedě. Když zvolená skupina obsahuje jak vyhovující, tak nevyhovující cíle, úloha bude odeslána pouze na vyhovující koncová zařízení.

6. Pro pokračování klikněte na **Ano** v potvrzovacím okně.

Objevené aplikace a procesy jsou zobrazeny v záložce **Network > Application Inventory**. Další informace viz „Inventář aplikací“ (str. 186).

Poznámka
Úloha **Applications Discovery** bude chvilku trvat, na základě počtu aplikací, které jsou nainstalovány. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Aktualizovat Security Server

Instalovaný Security Server můžete prohlížet a spravovat také z **Počítače a virtuální zařízení** pod složkou **Vlastní skupiny**.

Pokud je Security Server zastaralý, můžete na něj poslat aktualizační úlohu:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kde je Security Server nainstalovaný.

   Pro snadné nalezení Security Server můžete použít nabídku **Filtrů** následujícím způsobem:

   - Přejděte na kartu **Zabezpečení** a vyberte pouze **Bezpečnostní servery**.
   - Přejděte na kartu **Hloubka** a zvolte **Všechny položky rekurzivně**.
4. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Aktualizovat Security Server**.
5. Musíte potvrdit svou činnost. Kliknutím na **Ano** vytvoříte úlohu.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Důležité
Doporučujeme vám využít tento způsob pro aktualizování Security Serveru pro NSX, nebo ztratíte karanténu uloženou na zařízení.

Přidávání Vlastních Nástrojů

Poznámka
Tato úloha je spojena s modulem HVI, který je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Pro přidání nástrojů v cílovém hostovacím operačním systému:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kterou chcete z levého panelu. Všechny koncové body z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Vyberte zaškrtávací pole cílového koncového zařízení.
5. Klikněte na tlačítko **Tasks** na pravé straně tabulky a vyberte **Inject Custom Tool**. Zobrazí se konfigurační okno.
6. Z Rozbalovacího menu, vyberte všechny nástroje které chcete použít. Pro každý vybraný nástroj se zobrazí skládací sekce s jejím nastavením.

Tyto nástroje byli předtím nahrány do GravityZone. Pokud nemůžete najít správný nástroj v seznamu, přejděte do **Tools Management Center** a odtud je přidejte. Další informace viz „Zavedení vlastních nástrojů s HVI“ (str. 532).

7. Pro každý zobrazený nástroj v okně:
   a. Klikněte na název nástroje pro zobrazení nebo skrytí jeho sekce.
   b. Zadejte příkazovou řádku nástroje, společně se všemi potřebnými parametry, stejně jako v Příkazovém Řádku nebo Terminálu. Například:

      ```
      bash script.sh <param1> <param2>
      ```

      Pro BD Remediation Tools můžete vybrat pouze nápravu akce a zálohovat nápravnou akci ze dvou rozbalujících menu.
   c. Umístění od kut Security Server by měl získávat logy:
      - **stdout**. Vyberte toto zaškrtávací pole pro získávání logů ze standardního odchozího komunikačního kanálu.
      - **Output file**. Vyberte toto zaškrtávací pole pro sbírání souborů logu na koncových zařízeních. V tomto případě, potřebujete zadat cestu, kde Security Server nalezne soubor. Můžete použít absolutní cesty nebo systémové proměnné.

        Zde je další možnost: **Delete log files from Guest after they have been transferred**. Vyberte ji pokud již nepotřebujete soubory na koncových zařízeních.
8. Pokud chcete přemístit soubory logů ze Security Server někam jinam, musíte poskytnout cestu kam se mají uložit a údaje pro authentifikaci.
9. Někdy nástroje mohou vyžadovat více času než se očekává dokončení jejich práce nebo mohou přestat odpovídat. Pro předejití pádům v mnoha situacích, v sekci **Safety configuration**, vyberte po kolika hodinách Security Server by měl automaticky ukončit proces nástroje.
10. Klikněte na tlačítko **Save**.

    Budete moci zobrazit status úlohy v záložce **Tasks**. Pro více informací se můžete obrátit také na hlášení **HVI Stav zásahu třetí strany**.

6.2.6. Tvorba Rychlých hlášení

Můžete vytvářet okamžitá hlášení na spravovaných počítačích, počínaje na stránce **Síť**.

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte požadovanou skupinu v levém panelu. Všechny počítače ze zvolené skupiny jsou zobrazeny v tabulce na pravém panelu.

   Případně můžete filtrovat obsah zvolené skupiny pouze pro spravované počítače.
4. Označte políčka počítačů, které chcete zahrnout v hlášení.
5. Klikněte na tlačítko **Hlášení** v horní části tabulky a z nabídky zvolte typ hlášení.

   Další informace viz „Hlášení pro počítače a virtuální stroje“ (str. 478).
6. Nastavte parametry hlášení. Další informace viz „Vytváření hlášení“ (str. 497).
7. Klikněte na tlačítko **Vytvořit**. Hlášení se okamžitě zobrazí.

   Čas potřebný k vytvoření hlášení se může lišit podle počtu zvolených počítačů.

6.2.7. Přiřazování pravidel

Bezpečnostní nastavení počítačů můžete spravovat prostřednictvím pravidel.

Na stránce **Síť** můžete prohlížet, měnit a přiřazovat pravidla ke každému počítači nebo skupině počítačů.

Poznámka
Bezpečnostní nastavení jsou dostupná pouze pro spravované počítače. Pro usnadnění prohlížení a správy bezpečnostních nastavení můžete filtrovat síťový inventář podle pouze spravovaných počítačů.

Pro zobrazení pravidel přiřazených k určitému počítači:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kterou chcete z levého panelu. Všechny počítače ze zvolené skupiny jsou zobrazeny v tabulce na pravém panelu.
4. Klikněte na jméno spravovaného počítače, který vás zajímá. Zobrazí se informační okno.

5. Pod kartou **Obecné** v sekci **Pravidla** klikněte na název současného pravidla a prohlížejte jeho nastavení.
6. Bezpečnostní nastavení můžete měnit dle potřeby, pod podmínkou, že majitel pravidel povolil ostatním uživatelům v nich provádět změny. Mějte prosím na vědomí, že veškeré vámi provedené změny ovlivní všechny počítače se stejným přiřazeným pravidlem.

   Pro více informací o změně nastavení pravidel počítačů se odkažte na „Pravidla pro počítače a virtuální stroje“ (str. 227).

Pro přiřazení pravidla k počítači nebo skupině:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Vyberte skupinu, kterou chcete z levého panelu. Všechny počítače ze zvolené skupiny jsou zobrazeny v tabulce na pravém panelu.
4. Označte políčko požadovaného počítače nebo skupiny. Jednu nebo více položek stejného typu můžete zvolit pouze na té samé úrovni.
5. Klikněte na tlačítko **Přiřadit pravidlo** v horní části tabulky.
6. Proveďte potřebná nastavení v okně **Přiřazení pravidel**. Další informace viz „Přiřazování pravidel“ (str. 215).

Použití Správce obnovení pro šifrované svazky

Když koncoví uživatelé zapomenou svá šifrovací hesla a nemohou na svých počítačích přistupovat k šifrovaným svazkům, můžete jim pomoci načtením obnovovacích klíčů ze stránky **Síť**.

Pro získání klíče obnovy:

1. Jděte do záložky **Síť**.
2. Klikněte na tlačítko **Správce obnovení** na panelu nástrojů akcí na levé straně okna. Objeví se nové okno.
3. V části **Identifikátor** okna zadejte následující data:
   a. ID klíče pro obnovení šifrovaného svazku. ID klíče pro obnovení je řetězec čísel a písmen dostupných v koncovém bodě na obrazovce obnovy BitLocker.

      V systému Windows je ID klíče pro obnovení řetězec čísel a písmen dostupných v koncovém bodu na obrazovce pro obnovení BitLocker.

Alternativně můžete použít možnost **Obnova** na kartě **Ochrana** podrobností o počítači automaticky vyplnit ID klíče obnovy pro koncové body Windows i MacOS.

b. Heslo vašeho účtu GravityZone.

4. Klikněte na **Odkrýt**. Okno se rozbalí.

   Informace o svazku vám představí následující údaje:

   a. Název svazku

   b. Typ svazku (boot nebo non-boot).

   c. Název koncového bodu (jak je uveden v síťovém inventáři)

   d. Obnovovací klíč. V systému Windows je klíčem pro obnovení heslo generované automaticky po zašifrování svazku. V systému Mac je klíčem pro obnovení heslo uživatele.

5. Odešlete klíč pro obnovení koncovému uživateli.

Pro více informací ohledně šifrování a dešifrování svazků s GravityZone se odkažte na „Šifrování“ (str. 370).

6.2.9. Synchronizace s Active Directory

Síťový inventář se automaticky synchronizuje s Active Directory podle časového intervalu určeném v konfigurační sekci Control Center. Pro více informací se odkažte na kapitolu Instalace a Nastavení GravityZone v Průvodci instalací GravityZone.

Pro ruční synchronizaci aktuálně zobrazeného síťového inventáře s Active Directory:

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Klikněte na tlačítko **Synchronizovat s Active Directory** v horní části tabulky.
4. Je nutné potvrdit kliknutím na **Ano**.

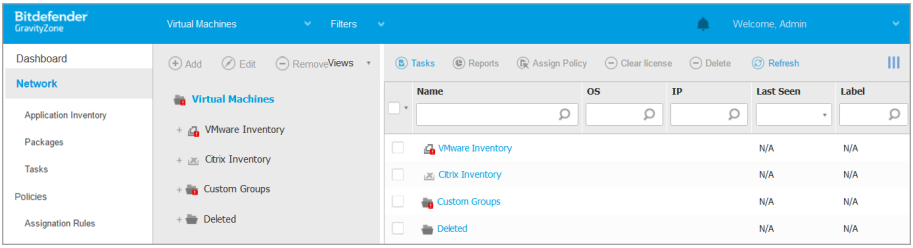
Poznámka

V rozsáhlých sítích Active Directory může dokončení synchronizace trvat déle.

6.3. Virtuální stroje

Pro zobrazení virtualizované infrastruktury pod vaším účtem přejděte na stránku **Síť** a z výběru zobrazení zvolte **Virtuální stroje**.

Poznámka
Virtuální stroje můžete spravovat také v zobrazení **Počítače a virtuální stroje**, ale prohlížet vaši virtualizovanou infrastrukturu a filtrovat její obsah pomocí určitých kritérií můžete pouze v zobrazení **Virtuální stroje**.
Pro více podrobností ohledně práce se zobrazením sítě se odkažte na „Práce s možnostmi zobrazení“ (str. 42).



Síť - zobrazení Virtuálních strojů

V panelu na levé straně můžete prohlížet dostupné sítě virtuálních strojů, a v pravém panelu podrobnosti o jednotlivých virtuálních strojích.

Pro úpravu podrobností o virtuálním stroji zobrazených v tabulce:

1. Klikněte na tlačítko **Sloupce** v pravé horní části pravého panelu.
2. Vyberte sloupce, které chcete zobrazit.
3. Klikněte na tlačítko **Resetovat** pro návrat pro zobrazení standardních sloupců.

Levý panel zobrazuje stromu podobný pohled na virtuální infrastrukturu. Kořen stromu se jmenuje **Virtuální stroje** a pod kořenem jsou seskupeny virtuální stroje, podle následujících kategorií na základě poskytovatele virtualizační technologie:

- **Inventář Nutanix.** Obsahuje seznam Nutanix Prism Element systémů, ke kterým máte přístup.
- **Inventář VMware.** Obsahuje seznam serverů vCenter, ke kterým máte přístup.
- **Inventář Citrix.** Obsahuje seznam systémů XenServer, ke kterým máte přístup.

- **Vlastní skupiny.** Obsahuje bezpečnostní servery virtuální stroje nalezené ve vaší síti mimo jakýkoli vCenter Server nebo XenServer systém.

Levý panel obsahuje také nabídku s názvem **Zobrazení**, ve které může uživatel zvolit typ zobrazení pro každého poskytovatele virtualizační technologie.

Abyste mohli přistupovat k virtualizované infrastruktuře integrované s Control Center, musíte zadat své přihlašovací údaje pro každý dostupný vCenter Server. Jakmile zadáte svá pověření, uloží se do Správce pověření a příště je už zadávat nemusíte. Další informace viz „Správce přihlašovacích údajů“ (str. 208).

V sekci **Síť** můžete spravovat virtuální stroje následujícím způsobem:

- Kontrola stavu virtuálních strojů
- Zobrazit podrobnosti virtuálních strojů
- Organizace virtuálních strojů do skupin
- Třízení, filtrování a vyhledávání
- Spustit úlohy
- Vytvářejte rychlá hlášení
- Přiřaďte pravidla
- Vyčistit licenční místa

V sekci **Konfigurace > Nastavení sítě**, můžete nakonfigurovat naplánovaná pravidla pro automatické vyčištění nepoužívaných virtuálních počítačů ze Síťového inventáře.

6.3.1. Kontrolování stavu virtuálních strojů

Každý virtuální stroj je na stránce sítí reprezentován ikonou specifickou pro jeho typ a stav.

Seznam všech dostupných ikon a stavů naleznete na „Typy a stavy síťových souborů“ (str. 564).

Podrobné informace o stavu viz:

- Správa stavů
- Stav připojení
- Stav zabezpečení

Správa stavů

Virtuální stroje mohou být v následujících stavech správy:

- **Spravované** - virtuální stroje, na kterých je nainstalované řešení Bitdefender.

- **Ve frontě na restart** - virtuální stroje, které vyžadují restartování systému po instalaci nebo aktualizaci ochrany Bitdefender.
- **Nespravované** - nalezené virtuální stroje, na kterých ještě není nainstalovaná ochrana Bitdefender.
- **Smazané** - virtuální stroje, které jste odstranili z Control Center. Další informace viz „Odstranění koncových bodů ze Síťového inventáře“ (str. 204).

Stav připojení

Stav připojení se týká spravovaných virtuálních zařízení a Security Serverů. Z tohoto pohledu mohou virtuální stroje být:

- **Online**. Modrá ikona značí, že je stroj online.
- **Offline**. Šedá ikona značí, že je stroj offline.

Virtuální stroj je offline, pokud je bezpečnostní agent neaktivní po dobu delší než 5 minut. Možné důvody, proč se virtuální stroje zobrazují jako offline:

- Virtuální stroj je vypnutý, v režimu spánku, nebo v režimu hibernace.

  Poznámka
  Virtuální stroje jsou zobrazeny jako online, i když jsou uzamčeny, nebo je uživatel odhlášený.

- Bezpečnostní agent nemá připojení ke Komunikačnímu centru GravityZone:
  - Virtuální stroj může být odpojen ze sítě.
  - Síťový firewall nebo router možná blokují komunikaci mezi bezpečnostním agentem a Bitdefender Control Center nebo s přiřazeným Endpoint Security Relay.
  - Virtuální stroj je za proxy Serverem a nastavení proxy nebyla správně nastavená pro aplikovaná práva.

    Varování
    Pro virtuální stroje za proxy serverem musí být nastavení proxy řádně nastavena v instalačním balíčku bezpečnostního agenta, nebo virtuální stroj nebude komunikovat s konzolí GravityZone a bude se vždy jevit jako offline nehledě na to, zda byly zásady s náležitým nastavením proxy aplikovány po instalaci.

- Bezpečnostní agent byl manuálně odstraněn z virtuálního zařízení, právě když virtuální zařízení nemělo spojení s Bitdefender Control Center nebo s přiřazeným Endpoint Security Relay. Za běžných okolností, když je bezpečnostní agent manuálně odinstalovaný z virtuálního stroje, Control Center je informována o této akci a virtuální stroj je označen jako nespravovaný.
- Bezpečnostní agent nebude možná pracovat správně.

Pro zjištění délky neaktivity virtuálních strojů:

1. Zobrazit pouze spravované virtuální stroje. Klikněte na **Filtry** nacházející se na vrchu tabulky a vyberte ze "Spravované" všechny možnosti, které potřebujete ze záložky **Bezpečnost**, vyberte **Všechny položky rekurzivně** ze záložky **Hloubka** a klikněte **Uložit**.
2. Klikněte na záhlaví sloupce **Posledně prohlíženo** pro seřazení virtuálních strojů podle délky neaktivity.

Kratší časové úseky neaktivity (minuty, hodiny) můžete ignorovat, protože se pravděpodobně jedná o dočasný stav z důvodu latenci v komunikaci. Například, virtuální stroj je právě vypnutý.

Delší doba neaktivity (dny, týdny) obvykle značí problém s virtuálním strojem.

Poznámka
Síťovou tabulku doporučujeme čas od času obnovit pro aktualizaci informací o koncových bodech s nejnovějšími změnami.

Stav zabezpečení

Stav zabezpečení se týká spravovaných virtuálních zařízení a Security Serverů. Virtuální stroje nebo Security Servery s bezpečnostními problémy můžete identifikovat podle stavových ikon, které zobrazují varovný symbol:

- Problémové.
- Bez problémů.

Virtuální stroj nebo Security Server má bezpečnostní problémy v případě, že se nachází v alespoň jedné z těchto situací:

- Antimalwarová ochrana je vypnuta (pouze pro virtuální zařízení).
- Vypršela licence.
- Produkt Bitdefender je zastaralý.
- Obsah zabezpečení je zastaralý.

- Je nalezen malware (pouze pro virtuální zařízení).
- Připojení k Cloudovým službám Bitdefender nemohlo být navázáno z následujících možných důvodů:
  - Virtuální stroj má potíže s připojením k internetu.
  - Připojení k Cloudovým službám Bitdefender je blokováno síťovým firewallem.
  - Port 443, nezbytný pro komunikaci s Cloudovými službami Bitdefender, je uzavřený.

  V tomto případě se antimalwarová ochrana spoléhá pouze na místní nástroje, zatímco skenování v cloudu je vypnuté, takže bezpečnostní agent nemůže poskytovat plnou ochranu v reálném čase.

Pokud naleznete virtuální stroj s bezpečnostními problémy, klikněte na jeho jméno pro zobrazení okna s **Informacemi**. Bezpečnostní problémy můžete identifikovat podle ikony ! . Ujistěte se, že jste zkontrolovali bezpečnostní informace ve všech záložkách informační stránky. Více podrobností se dozvíte kliknutím na nápovědu ikony. Může být nutné provést hlubší místní vyšetřování.

Poznámka
Síťovou tabulku doporučujeme čas od času obnovit pro aktualizaci informací o koncových bodech s nejnovějšími změnami.
Koncové body, které během posledních 24 hodin neobdrží žádné aktualizace, jsou automaticky označeny **S problémy** , bez ohledu na verzi obsahu zabezpečení přítomnou v relay nebo na GravityZone Update Server.

6.3.2. Prohlížení podrobností virtuálních strojů

Podrobné informace o každém virtuálním stroji můžete získat na stránce **Síť** následujícím způsobem:

- Prohlížení stránky **Síť**
- Prohlížení okna **Informace**

Kontrolování Záložky Síť

Chcete-li zjistit podrobnosti o virtuálním stroji, zkontrolujte dostupné informace v tabulce na pravém panelu na stránce**Síť**.

Sloupce s informacemi o virtuálních strojích můžete přidat nebo odebrat kliknutím na tlačítko **Sloupce** v pravé horní části panelu.

1. Jděte do záložky **Síť**.

2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Vyberte skupinu, kterou chcete z levého panelu.

   Všechny virtuální stroje dostupné ve vybrané skupině jsou zobrazeny v tabulce na pravém panelu.
4. Stav virtuálního stroje můžete snadno identifikovat podle příslušné ikony. Podrobné informace viz „Kontrolování stavu virtuálních strojů“ (str. 106).
5. Podívejte se na informace zobrazené ve sloupcích tabulky pro každý virtuální stroj.

   Použijte řádku se záhlavím pro vyhledávání konkrétních virtuálních strojů zatímco píšete, podle možných kritérií:

   - **Jméno**: jméno virtuálního stroje.
   - **FQDN**: plně kvalifikované jméno domény, které zahrnuje název hosta a jméno domény.
   - **OS**: operační systém nainstalovaný na virtuálním stroji.
   - **IP**: IP adresa virtuálního stroje.
   - **Naposledy prohlíženo**: datum a čas, kdy byl virtuální stroj naposledy zaznamenán online.

     Poznámka
     Pole **Naposledy prohlíženo** je důležité mít pod kontrolou, protože delší doba nečinnosti může znamenat problém s komunikací nebo odpojený virtuální stroj.

   - **Popisek**: vlastní řetězec s doplňujícími informacemi o koncovém bodu. V **Informačním okně** virtuálního stroje můžete přidat štítek a poté ho používat ve vyhledávání.
   - **Práva**: práva použitá pro virtuální stroj s odkazem pro zobrazení nebo změnu nastavení práv.

Prohlížení okna Informace

Pro zobrazení **Informačního** okna klikněte v pravém panelu na stránce **Síť** na jméno virtuálního stroje, který vás zajímá. V tomto okně jsou zobrazeny pouze údaje dostupné pro zvolené virtuální zařízení, seskupené pod několika kartami.

Níže naleznete vyčerpávající seznam informací, které můžete nalézt v **Informačním** okně podle typu stroje (virtuální zařízení, zařízení Security Server) a jeho specifických bezpečnostních informací.

Karta Obecné

- Obecné informace o zařízení, jako je název, identifikace FQDN informace, IP adresa, operační systém, infrastruktura, rodičovská skupina a aktuální stav připojení.

  V této sekci můžete k přiřadit štítek k virtuálnímu zařízení. Budete moci rychle najít virtuální stroje se stejným štítkem a pracovat s nimi nehledě na to, kde v síti jsou umístěny. Pro více informací o filtrovacím virtuálním zařízení se podívejte na „Třídění, Filtrování a Hledání virtuálních strojů“ (str. 120).

- **Podmínky HVI** obsahují informace o tom, zda můžete použít Security Server k zavedený ochrany pomocí HVI nebo ne. Tím pádem, pokud host pro Security Server pracuje na podporované verzi XenServeru s nainstalovaným doplňkovým balíčkem, můžete z tohoto hosta povolit HVI na virtuálních strojích.

- Informace o ochranných vrstvách, včetně seznamu bezpečnostních technologií získaných s vaším řešením GravityZone a stav jejich licence, který může být:

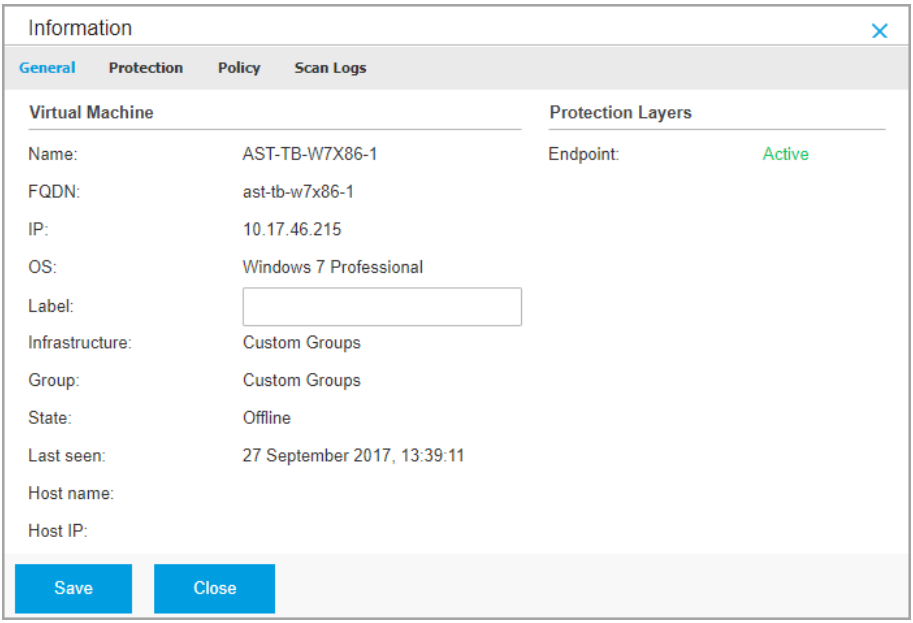
  – **Dostupné / Aktivní** - licenční klíč pro tuto ochrannou vrstvu je na virtuálním stroji aktivní.

  – **Expirovaný** - licenční klíč pro tuto ochrannou vrstvu vypršel.

  – **Čekající** - licenční klíč ještě nebyl potvrzen.

  > **Poznámka**
  > Doplňující informace o ochranných vrstvách naleznete na kartě **Zabezpečení**.

- **Relay připojení**: jméno, IP a popis relaye, ke kterému je virtuální stroj případně připojen.



Informační okno - Karta Obecné

Karta Zabezpečení

Tato karta obsahuje podrobnosti o každé vrstvě zabezpečení s licencí na koncovém bodě. Podrobnosti odkazují na:

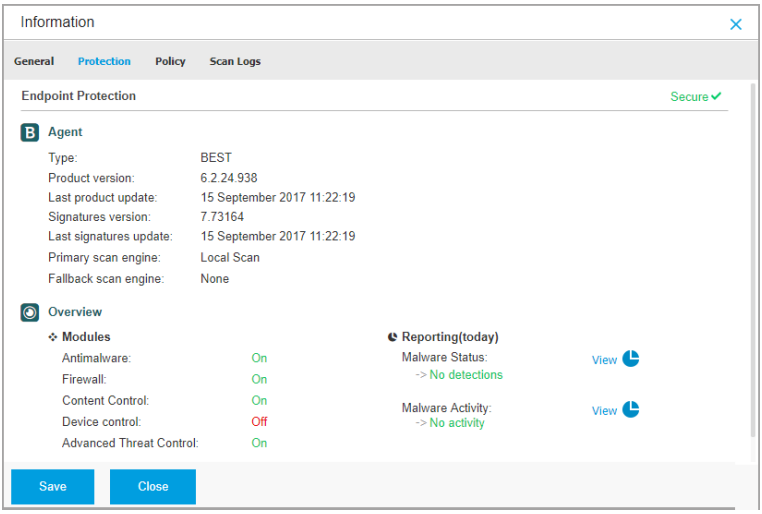
- Informace o bezpečnostním agentovi, jako je název a verze produktu, konfigurace skenovacích nástrojů a stav aktualizací. Dostupné jsou také verze pro Ochranu Exchange, antispamové nástroje a signatury.
- Stav zabezpečení pro každou vrstvu ochrany. Tento stav je zobrazen vedle názvu ochranné vrstvy na pravé stráně:
  - **Zabezpečený**, když na koncových bodech s aplikovanou bezpečnostní vrstvou nejsou hlášeny žádné bezpečnostní problémy.
  - **Zranitelný**, když jsou na koncových bodech s aplikovanou bezpečnostní vrstvou hlášeny bezpečnostní problémy. Více informací naleznete na „Stav zabezpečení“ (str. 108).

- Přiřazený Security Server. Každý přiřazený Security Server se zobrazí v případě zavádění bez agenta, nebo když jsou skenovací nástroje bezpečnostních agentů nastaveny na skenování na dálku. Security Server informace jsou nápomocné při identifikaci virtuálního zařízení a při získání jeho aktualizačního stavu.
- Informace ohledně NSX, jako je stav virových štítků a bezpečnostní skupiny, do které virtuální stroj patří. Pokud byl přiřazen bezpečnostní štítek, znamená to, že je stroj nakažený. V opačném případě je buď stroj čistý, nebo nepoužíváte bezpečnostní štítky.
- Stav ochranných modulů. Můžete snadno prohlížet, jaké ochranné moduly byly nainstalovány na koncový bod, a také stav dostupných modulů (**Zapnuto / Vypnuto**) nastavených skrze aplikovaná pravidla.
- Rychlý přehled ohledně aktivity modulů a malwarových hlášení za současný den.

  Klikněte na odkaz **Zobrazení** pro přístup k nastavením hlášení a poté vytvořte hlášení. Další informace viz „Vytváření hlášení“ (str. 497)
- Informace ohledně ochranné vrstvy Sandbox Analyzer:
  - Stav využití Sandbox Analyzer na virtuálním stroji je zobrazený na pravé straně okna:
    - **Aktivní**: Sandbox Analyzer je licencovaný (dostupný) a povolený na základě politik virtuálního stroje.
    - **Neaktivní**: Sandbox Analyzer je licencovaný (dostupný), ale není povolený na základě politik virtuálního stroje.
  - Název agenta, který se chová jako detekční senzor.
  - Status modulu na virtuálním zařízení:
    - **Zapnutý** - Sandbox Analyzer je povolený na virtuálním stroji prostřednictvím politik.
    - **Vypnutý** - Sandbox Analyzer není povolený na virtuálním stroji prostřednictvím politik.
  - Nalezené hrozby za poslední týden kliknutím na odkaz **Zobrazit** pro přístup k hlášení.
- Doplňující informace týkající se modulu Šifrování, jako jsou:
  - Zjištěné svazky (se zmínkou o spouštěcí jednotce).

– Status šifrování pro každý svazek (který může být **Šifrováno**, **Probíhá Šifrování**, **Probíhá Dešifrování**, **Nešifrované**, **Uzamčené** nebo **Pozastavené**).

  Klíč pro obnovu přiřazeného šifrovaného svazku získáte kliknutím na odkaz **Obnovení**. Pro detaily ohledně získání klíčů pro obnovu se obraťte na „Použití Správce obnovení pro šifrované svazky“ (str. 159).



Informační okno - Karta Zabezpečení

Pro Security Servery, tato část obsahuje informace o modulu ochrany úložišť (Storage Protection module). Podrobnosti odkazují na:

- Stav služby:
  - **N/A** – Ochrana úložišť (Storage Protection) je licencována, ale tato služba není prozatím nakonfigurována.
  - **Zapnutá** – služba je zapnuta v politice a funguje.
  - **Vypnutá** – služba nefunguje buď proto, že byla vypnuta v politice nebo protože vypršela platnost licenčního klíče.
- Seznam připojených ICAP-kompatibilních úložných zařízení (storage devices) s následujícími detailními informacemi:
  - Název úložného zařízení (Storage device name)
  - IP adresa úložného zařízení (Storage device IP)
  - Druh úložného zařízení (Storage device type)

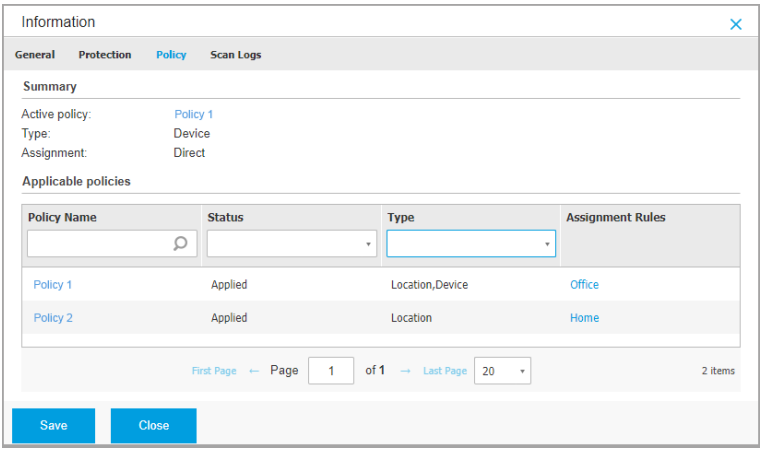
- The date and time of the last communication between the storage device and Security Server.

Záložka Práv

Na virtuální stroj lze aplikovat jedno nebo více pravidel, ale aktivní může být vždy pouze jedno. Na kartě **Pravidla** jsou zobrazeny informace o všech pravidlech platných pro virtuální stroj.

- Název aktivní politiky. Klikněte na název pravidla pro otevření její šablony a prohlížení jejích nastavení.
- Typ aktivního pravidla, což může být:
  - **Zařízení**: když je pravidlo k virtuálnímu stroji přiřazeno ručně administrátorem sítě.
  - **Umístění**: zásada založená na pravidlech, automaticky přiřazená k virtuálnímu stroji, pokud se jeho síťová nastavení shodují s podmínkami danými v existujícím pravidle přiřazování.
  - **Uživatel**: zásada založená na pravidlech, automaticky přiřazená ke koncovému bodu, pokud se shoduje s cílem Active Directory určeným podle existujícího přiřazovacího pravidla.

    Například, stroj může mít přiřazená dvě uživatele-zohledňující pravidla, jedno pro správce a druhé pro ostatní zaměstnance. Každé pravidlo se aktivuje při přihlášení uživatele s potřebnými oprávněnými.
  - **Externí (NSX)**: když je pravidlo definováno v prostředí VMware NSX.
- Typ přiřazování aktivních pravidel, který může být:
  - **Přímý**: když je pravidlo aplikováno přímo na virtuální stroj.
  - **Zděděné**: když virtuální zdroj zdědí pravidlo z rodičovské skupiny.
- **Aplikovatelné politiky**: zobrazí seznam pravidel propojených s existujícími pravidly přiřazování. Tyto zásady mohou být aplikovány na virtuální stroj, když se shodují s podmínkami zadanými v připojených přiřazovacích pravidlech.

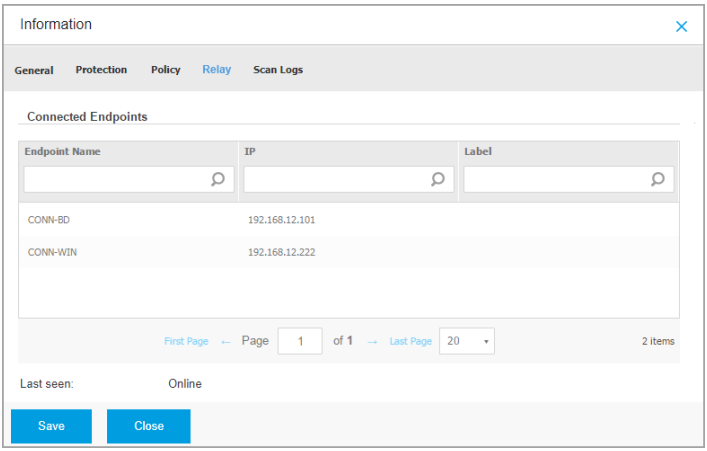


Informační okno - Záložka Práv

Více informací ohledně pravidel naleznete na „Přiřazování pravidel“ (str. 213)

Karta Relay

Karta **Relay** je dostupná pouze pro virtuální stroje s funkcí relay. Tato karta zobrazuje informace o koncových bodech připojených ke stávajícímu relayi, jako je název, IP a popis.



Informační okno - Karta Relay

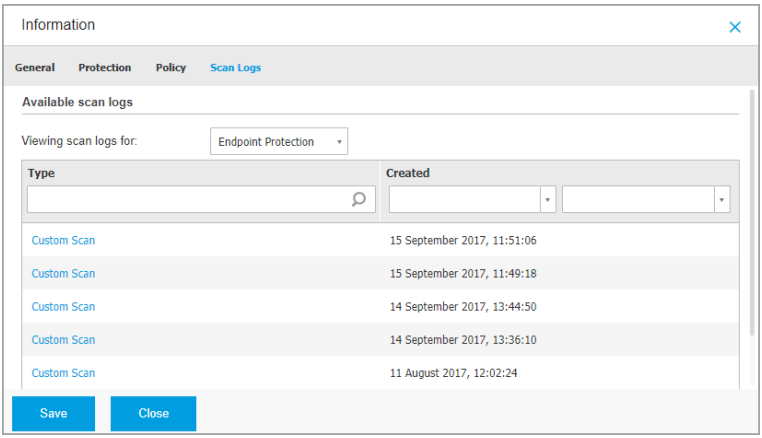
Karta Protokoly skenování

Záložka **Zpráva o skenování** ukazuje detailní informace o všech skenovacích úlohách, které proběhly na virtuálním zařízení.

Zprávy jsou spojeny ochranou vrstvou a můžete si vybrat z rozbalovacího menu, pro kterou vrstvu se má zpráva zobrazit.

Klikněte na skenovací úlohu, která vás zajímá a zpráva se otevře v novém okně webového prohlížeče.

Je-li k dispozici mnoho zpráv o skenování, mohou se rozložit na několik stránek. Pro pohyb mezi stránkami, použijte navigační panel dole v tabulce. Pokud je k dispozici příliš mnoho záznamů, můžete využít možnosti filtrů, které jsou k dispozici v horní části tabulky.



Informační okno - Záložka Zpráv o Skenu

Každá vlastnost v tomto okně, které generuje bezpečnostní problém, je označena ! ikonou. Zkontrolujte nápovědu pro ikony, kde najdete další podrobnosti. Může být nutné provést hlubší místní vyšetřování.

6.3.3. Organizace virtuálních strojů do skupin

Skupiny virtuálních strojů můžete spravovat v levém panelu na stránce **Síť** pod složkou **Vlastní skupiny**.

Virtuální stroje importované z Nutanix Prism Element se seskupují ve složce **Nutanix Inventář**. Virtuální stroje importované z VMware vCenter jsou seskupeny pod složkou **Inventář VMware**. Virtuální stroje importované z XenServer jsou seskupeny pod složkou **Inventář Citrix**. Nelze editovat Nutanix inventáře, VMware inventáře nebo Citrix inventáře. Můžete pouze prohlížet a spravovat odpovídající virtuální stroje.

Všechny vaše virtuální stroje, které nejsou spravovány Nutanix Prism, vCenter nebo XenServer systémy jsou detekovány pomocí funkce síťového rozpoznávání (Network Discovery) a jsou zařazeny do **Vlastní skupiny**, kde si je můžete organizovat do libovolných skupin, tak jak potřebujete. Hlavní výhodou této možnosti je, že můžete používat skupinová oprávnění pro splnění různých bezpečnostních požadavků.

Pod **Vlastními skupinami** můžete vytvořit, smazat, přejmenovat a přesunout skupiny virtuálních strojů v rámci stromové struktury na míru.

Poznámka

- Skupina může obsahovat jak virtuální stroje, tak další skupiny.
- Při výběru skupiny v levém panelu můžete zobrazit všechny virtuální stroje kromě těch, které jsou umístěny do jejích podskupin. Pro zobrazení všech virtuálních strojů zahrnutých ve skupině a jejích podskupinách, klikněte na menu **Filtry** nacházející se v horní části tabulky a vyberte **Všechny objekty opakovaně** v sekci **Hloubka**.

Vytváření Skupin

Předtím než začnete vytvářet skupiny, přemýšlejte nad důvodem proč je potřebujete a vytvořte si nějaké schéma skupin. Například, můžete seskupit všechny virtuální stroje podle jednoho, nebo smícháním následujících kritérií:

- Organizační struktura (Sales, Marketing, Záruka Kvality, Vývoj Softwaru, Správa, atd.).
- Bezpečnostní požadavky (Desktopy, Laptopy, Servery, atd.).
- Pozice (Ústředí, Místní Kanceláře, Vzdálení Pracovníci, Domácí Kanceláře, atd.).

Pro organizování vaší sítě do skupin:

1. V levém panelu vyberte **Vlastní skupiny**.
2. Klikněte na tlačítko **Přidat skupinu** v horní části levého panelu.
3. Zadejte působivé jméno pro skupinu a klikněte na **OK**. Nová skupina je zobrazena pod **Vlastními skupinami**.

Přejmenování Skupin

Pro přejmenování skupiny:

1. Vyberte skupinu v levém panelu.
2. Klikněte na tlačítko **Upravit skupinu** v horní části levého panelu.
3. Zadejte nové jméno do odpovídajícího pole.
4. Potvrďte kliknutím na **OK**.

Přesouvání skupin a virtuálních strojů

Položky můžete přesouvat kamkoli v hierarchii **Vlastních složek**. Pro přesun objektu, přetáhněte a umístěte ho z pravého panelu do skupiny v levém panelu.

Poznámka

Přesunutý objekt bude dědit nastavená práva nové rodičovské skupiny, pokud nejsou žádná jiné práva přidělena přímo k danému objektu. Pro více informací o dědění práv, obraťte se na „Zásady zabezpečení“ (str. 212).

Mazání Skupin

Skupina nemůže být odstraněna, pokud obsahuje alespoň jeden virtuální stroj. Přesuňte všechny virtuální stroje ze skupiny, kterou chcete odstranit, do jiných skupin. Pokud skupina zahrnuje podskupiny, můžete se rozhodnout pro přesunutí celých podskupin místo jednotlivých virtuálních strojů.

Pro smazání skupiny:

1. Zvolte prázdnou skupinu.
2. Klikněte na tlačítko ⊗ **Odstranit skupinu** v horní části levého panelu. Je nutné potvrdit kliknutím na **Ano**.

6.3.4. Třídění, Filtrování a Hledání virtuálních strojů

V závislosti na počtu virtuálních strojů může tabulka zabrat několik stran (ve výchozím stavu je zobrazeno pouze 20 objektů na stránku). Pro pohyb mezi stránkami použijte navigační tlačítka ve spodní části tabulky. Můžete změnit počet položek zobrazených na stránku tak, že vyberete nějakou z menu umístěného vedle navigačních tlačítek.

Pokud je záznamů příliš mnoho, můžete použít vyhledávací pole pod hlavičkami sloupců nebo v menu **Filtry** navrchu stránky pro zobrazení pouze těch objektů, které vás zajímají. Například můžete hledat konkrétní virtuální stroj, nebo si zvolit prohlížení pouze spravovaných virtuálních strojů.

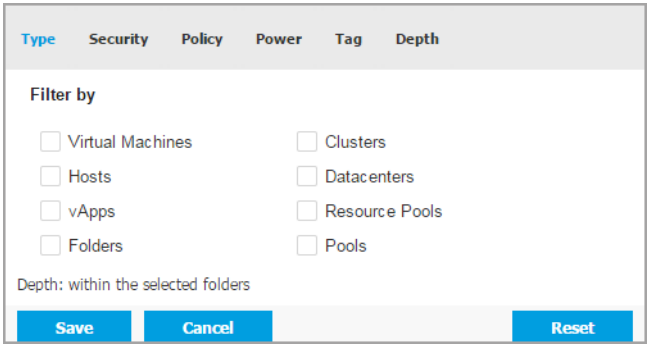
Třídění virtuálních strojů

Pro třídění dat podle určitého sloupce, klikněte na hlavičku slupce. Například, pokud chcete virtuální stroje seřadit podle jména, klikněte na hlavičku **Název**. Pokud kliknete na hlavičku znovu, virtuální body se zobrazí v opačném pořadí.

Třídění Počítačů

Filtrování virtuálních strojů

1. Vyberte skupinu v levém panelu.
2. Klikněte na menu **Filtry** navrchu od oblasti panelů sítě.
3. Použijte následující filtrovací kriteria:
   - **Typ**. Vyberte typ virtuálních objektů, které chcete zobrazit.

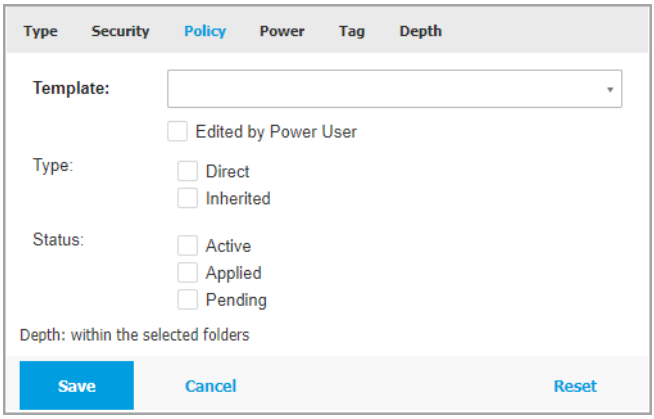


Virtuální stroje - Filtrovat podle typu

   - **Zabezpečení**. Vyberte správu zabezpečení a/nebo bezpečnostní stav, podle kterého se budou síťové objekty filtrovat. Například si můžete vybrat, jestli chcete prohlížet pouze zařízení Security Server, nebo prohlížet pouze koncové body s bezpečnostními problémy.

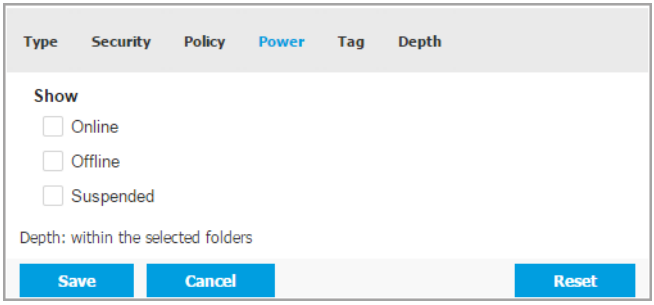
Virtuální stroje - Filtrovat podle zabezpečení

   - **Práva**. Vyberte šablonu pravidla, podle kterého chcete virtuální stroje filtrovat, typ přiřazení pravidla (Přímo nebo Zděděné), a také stav přiřazení pravidla (Aktivní, Aplikované nebo Čekající).



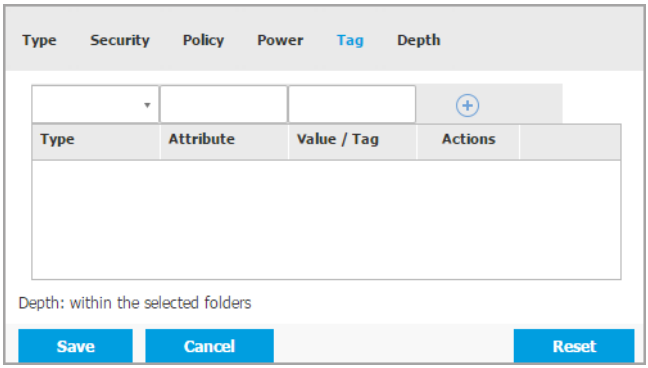
Virtuální stroje - Filtrovat podle práv

- **Pravomoc**. Můžete si zvolit mezi zobrazením virtuálních strojů jako online, offline nebo pozastavený.



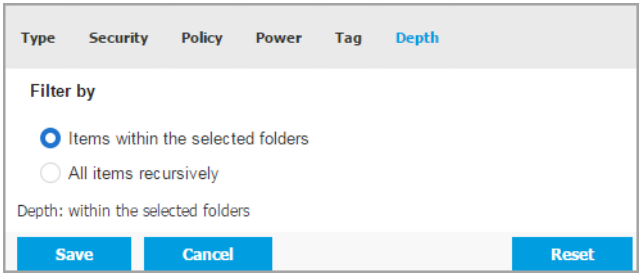
Virtuální stroje - Filtrovat podle Pravomoci

- **Štítky**. Můžete si vybrat filtrování virtuálních strojů podle štítků a vlastností, které jste definovali ve vašem virtualizačním prostředí.



Virtuální stroje - Filtrovat podle štítků

- **Struktura**. Když spravujete síť se stromovou strukturou virtuálních zařízení, virtuální zařízení umístěná v podskupinách se automaticky nezobrazují. Pro zobrazení všech virtuálních zařízení v aktuální skupině a všech jejích podskupinách vyberte **Všechny objekty opakovaně**.



Virtuální stroje - Filtrovat podle hloubky

Poznámka
Klikněte na **Obnovit** pro vyčištění filtru a zobrazení všech virtuálních strojů.

4. Klikněte na **Uložit** pro filtrování virtuálních strojů podle vybraných kriterií.

Vyhledávání virtuálních strojů

1. Zvolte požadovaný kontejner z levého panelu.

2. Do příslušného pole pod záhlavím sloupců (jméno, OS nebo IP) v pravém panelu zadejte hledaný výraz. Například, zadejte IP adresu virtuálního stroje, který hledáte, do pole **IP**. V tabulce se zobrazí pouze odpovídající virtuální zařízení.

   Vyčistěte vyhledávací pole pro zobrazení plného seznamu virtuálních strojů.

6.3.5. Spouštění úloh na virtuálních strojích

Ze stránky **Síť** můžete na virtuálních strojích na dálku spouštět několik administrativních úloh.

Můžete provádět následující akce:

- „Sken“ (str. 125)
- „Úlohy balíčků“ (str. 134)
- „Exchange Scan“ (str. 137)
- „Instalovat“ (str. 141)
- „Odinstalovat klienta“ (str. 145)
- „Aktualizace“ (str. 146)
- „Přenastavení klienta“ (str. 147)
- „Vyhledání sítě“ (str. 148)
- „Vyhledání aplikací“ (str. 149)
- „Restartovat stroj“ (str. 150)
- „Instalovat Security Server“ (str. 150)
- „Odinstalovat Security Server“ (str. 153)
- „Aktualizovat Security Server“ (str. 153)
- „Instalovat Doplňkový balíček HVI“ (str. 154)
- „Odinstalovat Doplňkový balíček HVI“ (str. 155)
- „Aktualizovat Doplňkový balíček HVI“ (str. 155)

Můžete si zvolit, zda chcete vytvářet úlohy pro každé virtuální zařízení jednotlivě, nebo pro jejich skupiny. Například můžete na dálku nainstalovat Bitdefender Endpoint Security Tools na skupinu nespravovaných virtuálních strojů. Později můžete vytvořit skenovací úlohu pro konkrétní virtuální stroj ze skupiny.

Můžete spouštět pouze úlohy kompatibilní s každým jednotlivým virtuálním zařízením. Například, pokud zvolíte nespravovaný virtuální stroj, můžete zvolit pouze instalaci bezpečnostního agenta, se všemi ostatními úlohami vypnutými.

V případě skupiny bude zvolená úloha vytvořena pouze pro kompatibilní virtuální stroje. Jestli není žádné virtuální zařízení ve skupině kompatibilní s vybranou úlohou, budete upozorněni, že tato úloha nemůže být vytvořena.

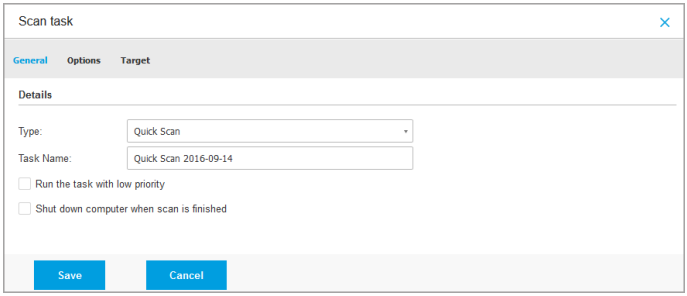
Jakmile je vytvořena, úloha se spustí automaticky na všech virtuálních strojích, které jsou online. Pokud je virtuální stroj offline, úloha se spustí jakmile bude znovu online.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Sken

Pro spuštění skenovací úlohy na jednom nebo více virtuálních zařízeních na dálku:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechna jednotky patřící k vybrané skupině jsou zobrazeny v pravém panelu tabulky.
4. Označte pole odpovídající objektům, které chcete skenovat.
5. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Sken**. Zobrazí se konfigurační okno.
6. Konfigurace parametrů skenu:
   - Na kartě **Obecné** si můžete zvolit typ skenování a můžete zadat název skenovací úlohy. Název skenovací úlohy vám má pomoci ve snadné identifikaci aktuálního skenu na stránce **Úlohy**.



Úloha skenování virtuálních strojů - konfigurace obecných nastavení

Z nabídky **Typ** zvolte typ skenování:

– **Rychlý sken** je přednastavený tak, aby umožnil skenování pouze kritických systémových umístění a nových souborů. Provedení rychlého skenu

obvykle trvá méně než minutu a využije jen zlomek systémových prostředků, které potřebuje běžný sken.

Pokud je nalezen malware nebo rootkity, Bitdefender automaticky provede dezinfekci. Pokud je soubor z jakéhokoli důvodu nemožné dezinfikovat, je přesunut do karantény. Tento typ skenování ignoruje podezřelé soubory.

– **Kompletní sken** otestuje celý počítač na přítomnost malwaru ohrožujícího jeho bezpečnost, jako viry, spyware, adware, rootkity a další.

  Bitdefender se automaticky pokusí vyčistit soubory, které byli identifikované jako malware. Pokud malware nemůže být odstraněn, je přesunut do karantény, kde nemůže napáchat žádné škody. Podezřelé soubory jsou ignorovány. Chcete-li také podniknout kroky proti podezřelým souborům nebo podniknout další běžné akce s infikovanými soubory, poté vybrat a spustit Vlastní Skenování.

– **Skenování paměti** kontroluje programy spuštěné v paměti virtuálního zařízení.

– **Skenování sítě** je typ vlastního skenování, umožňující skenování síťových jednotek pomocí bezpečnostního agenta Bitdefender nainstalovaného na cílovém virtuálním zařízení.

  Aby síťové skenování fungovalo:

  - Je nutné zadat úlohu pouze jednomu koncovému bodu ve vaší síti.
  - Musíte zadat pověření uživatelského účtu s oprávněními pro čtení/psaní na cílové síťové jednotky, aby bezpečnostní agent mohl přistupovat a provádět opatření pro tyto síťové jednotky. Požadovaná ověření mohou je možné nastavit na kartě **Cíl** v okně úloh.

– **Vlastní sken** vám umožňuje zvolit umístění, která chcete skenovat, a nastavit možnosti skenování.

Pro skenování paměti, sítě, a vlastní skenování máte také následující možnosti:

– **Spustit sken s nízkou prioritou**. Označte toto políčko pro snížení priority skenovacího procesu a umožněte ostatním programům pracovat rychleji. Toto prodlouží čas potřebný k dokončení skenovacího procesu.

> **Poznámka**
> Tato možnost platí pouze pro Bitdefender Endpoint Security Tools a Endpoint Security (agent pro starší verze).

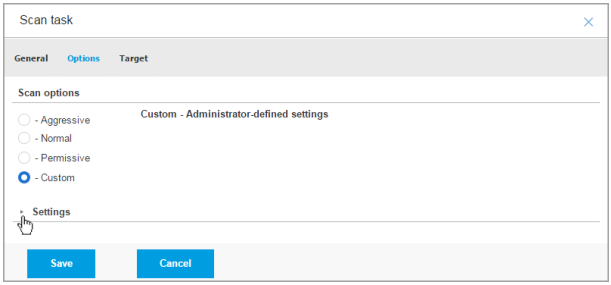
– **Vypnout počítač po ukončení skenování**. Označte toto políčko, pokud plánujete počítač po nějakou dobu nepoužívat.

> **Poznámka**
> Tato možnost se vztahuje na Bitdefender Endpoint Security Tools, Endpoint Security (agent pro starší verze) a Endpoint Security for Mac.

Pro vlastní skenování konfigurujte následující parametry:

– Přejděte na kartu **Možnosti** a nastavte parametry skenování. Zvolte úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (agresivní, normální nebo tolerantní). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

Na základě zvoleného profilu budou parametry skenování v sekci **Nastavení** nastaveny automaticky. Ale pokud si přejete, můžete je nastavit podrobněji. To provedete tak, že označíte políčko **Vlastní** a poté rozbalíte sekci **Nastavení**.



Úloha skenování virtuálních strojů - konfigurace Vlastního skenování

K dispozici jsou následující možnosti:

- **Soubory.** Pomocí těchto možností upřesněte, které typy souborů chcete skenovat. Můžete nastavit bezpečnostního agenta, aby skenoval všechny soubory (nehledě na příponu souboru), pouze soubory aplikací, nebo určité souborové přípony, které považujete za

nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

Poznámka

Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

Pokud si přejete skenovat pouze určité souborové přípony, zvolte v nabídce **Vlastní přípony**, přípony zadejte do pole úprav a po každé stiskněte `Enter`.

Důležité

Bezpečnostní agenti Bitdefender nainstalované na operačních systémech Windows a Linux skenují většinu fomátů .ISO, ale neprovádí na nich žádná opatření.

Možnosti úlohy skenování virtuálních strojů - Přidání vlastních přípon

- **Archivy.** Archivy obsahující infikované soubory nepředstavují pro zabezpečení vašeho systému bezprostřední hrozbu. Malware může ovlivňovat váš systém, pouze pokud je infikovaný soubor z archivu extrahován a spuštěn bez zapnuté ochrany v reálném čase. Doporučujeme však archivy skenovat, aby byly detekovány a odstraněny všechny potenciální hrozby, i když nejsou bezprostřední.

  Důležité

  Skenování archivovaných souborů zvyšuje celkovou dobu skenu a vyžaduje více systémových prostředků.

- **Skenovat uvnitř archivů.** Zvolte tuto možnost, pokud si přejete kontrolovat archivované soubory na malware. Pokud se rozhodnete využít této možnosti, můžete konfigurovat následující optimalizační možnosti:
  - **Omezit velikost archivu na (MB).** Můžete nastavit maximální přijatelnou velikost archivů, které mají být skenovány. Zaškrtněte příslušné políčko a zadejte maximální velikost archivů (v MB).
  - **Maximální hloubka archivu (úrovně).** Zaškrtněte příslušné políčko a z nabídky zvolte maximální hloubku archivu. Pro nejvyšší výkon zvolte nejnižší hodnotu, pro maximální ochranu zvolte nejvyšší hodnotu.
- **Skenovat emailové archivy.** Vyberte tuto možnost, pokud chcete povolit skenování souborů emailových zpráv a emailových databází včetně souborů s formáty jako .eml, .msg, .pst, .dbx, .mbx, .tbb a další.

  Důležité
  Skenování emailových archivů je zdrojově náročné a může ovlivnit výkon systému.

- **Různé.** Vyberte odpovídající políčka pro nastavení požadovaných možností skenování.
  - **Skenovat spouštěcí sektory.** Skenovat zaváděcí sektor systému. Tento sektor pevného disku obsahuje kód pro virtuální zařízení, nezbytný k zahájení spouštěcího procesu. Když virus infikuje spouštěcí sektor, jednotka se může stát nepřístupnou a nemusí být možné spustit systém a přistupovat k datům.
  - **Skenovat registr.** Tuto možnost použijte ke skenování klíčů registru. Registr systému Windows je databáze, která uchovává nastavení konfigurací a možností pro součásti operačního systému Windows i pro nainstalované aplikace.
  - **Hledat rootkity.** Tuto možnost zvolte pro skenování rootkitů a objektů skrytých pomocí tohoto softwaru.
  - **Hledat keyloggery.** Zvolte tuto možnost pro skenování keylogger softwaru. Keyloggery nejsou škodlivé aplikace samy o sobě, ale

mohou být využity se škodlivým záměrem. Hacker může ze zcizených dat získat citlivé informace, jako čísla účtů a hesla, a použít je k vlastnímu prospěchu.

- **Skenovat paměť.** Tuto možnost použijte ke skenování programů běžících v paměti systému.
- **Skenovat cookies.** Tuto možnost zvolte pro skenování souborů cookie, které jsou ukládány prohlížeči na virtuálních strojích.
- **Skenovat pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Skenovat pro potenciálně nežádoucí aplikace (PUA).** Potenciálně nežádoucí aplikace (PUA) je program, který může být na PC nežádoucí a někdy bývá součástí freewaru nebo softwaru. Takové programy mohou být nainstalovány bez vědomí uživatele (jsou známé také jako adware), nebo mohou být obsaženy v původní expresní instalační sadě (podporované reklamou). Možný dopad těchto programů zahrnuje zobrazování vyskakovacích oken, instalaci nechtěných nástrojových lišt ve výchozím prohlížeči nebo spuštění několika procesů na pozadí a zpomalení výkonu PC.
- **Skenovat výměnné svazky.** Vyberte tuto možnost pro skenování vyměnitelných zařízení připojených k virtuálnímu zařízení.

- **Akce.** Podle typu rozpoznaných souboru, následující možnosti jsou provedeny automaticky:
  - **Když bude nalezen infikovaný soubor.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanizmů, které zahrnují malwarové signatury, machine learnign a umělou inteligenci (AI). Bezpečnostní agent Bitdefender může za běžných okolností odstranit malwarový kód z infikovaného souboru a obnovit původní soubor. Této operaci se říká dezinfikace.

    Pokud je nalezen infikovaný soubor, bezpečnostní agent Bitdefender se ho automaticky pokusí dezinfikovat. Pokud se dezinfekce nezdaří, soubor je přesunut do karantény, která infekci zadrží.

Důležité
V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

- **Když bude nalezen podezřelý soubor.** Soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé). Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.

  Skenování je ve výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení. Soubory v karanténě jsou pravidelně posílány na analýzu do laboratoří Bitdefender. Pokud je přítomnost malwaru potvrzena, je vydána signatura umožňující odstranění malwaru.

- **Když je nalezen rootkit.** Rootkity představují specializovaný software, používaný pro ukrytí souborů před operačním systémem. Přestože ve své podstatě nejsou škodlivé, rootkity jsou často využívány pro ukrytí malwaru nebo pro zamaskování přítomnosti narušitele v systému.

  Nalezené rootkity a skryté soubory jsou ve výchozím nastavení ignorovány.

Když je na virtuálním zařízení NSX nalezen vir, Security Server automaticky označí virtuální zařízení Bezpečnostním štítkem za předpokladu, že tato možnost byla zvolena při integraci vCenter Server.

Pro tento účel NSX obsahuje tři bezpečnostní štítky, specifické podle závažnosti hrozby:

- `ANTI_VIRUS.VirusFound.threat=low` platí pro zařízení, když na něm Bitdefender nalezne malware s nízkým rizikem, který dokáže odstranit.

- `ANTI_VIRUS.VirusFound.threat=medium` platí pro zařízení, ze kterých Bitdefender nedokáže odstranit infikované soubory, a místo toho je dezinfikuje.
- `ANTI_VIRUS.VirusFound.threat=high` platí pro zařízení, Bitdefender nedokáže ani odstranit, ani dezinfikovat jeho infikované soubory, ale zablokuje k nim přístup.

Infikovaná zařízení můžete izolovat tak, že vytvoříte bezpečnostní skupiny s dynamickým členstvím na základě bezpečnostních štítků.

Důležité

- Pokud Bitdefender nalezne na zařízení hrozby s různými úrovněmi závažnosti, aplikuje všechny odpovídající štítky.
- Bezpečnostní štítek je ze zařízení odebrán pouze poté, co je proveden Kompletní sken a zařízení je vydezinfikováno.

Přestože to nedoporučejeme, výchozí nastavení můžete změnit. Můžete určit druhou akci, která bude provedena v případě selhání té první, a různé akce pro každou kategorii. Z odpovídajících nabídek zvolte první a druhou akci, které budou provedeny na každém typu rozpoznaného souboru. K dispozici jsou následující akce:

vyléčit
Odstranit malwarový kód z infikovaných souborů. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech.

Přesunout soubory do karantény
Přesunout odhalené soubory z jejich současného umístění do karanténní složky. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Můžete spravovat soubory v karanténě ze záložky Karanténa v konzoli.

Odstranit
Odstranit odhalené soubory z disku, bez jakéhokoli upozornění. Této akci se doporučujeme vyhýbat.

Ignorovat
S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu.

– Přejděte na kartu **Cíl** pro přidání umístění, která chcete skenovat na zvolených virtuálních zařízeních.

  V sekci **Cíl skenování** můžete přidat nový soubor nebo složku ke skenování:

  a. Z rozbalovacího menu zvolte přednastavené umístění, nebo zadejte **Určité cesty**, které si přejete skenovat.

  b. Určete cestu k objektu, který chcete skenovat, v poli úprav.

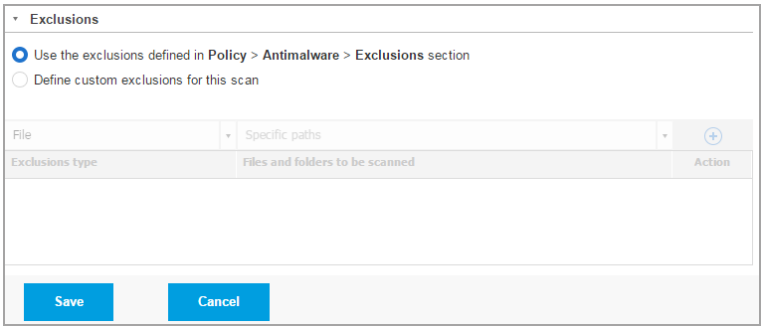
     - V případě, že jste zvolili přednastavené umístění, doplňte cestu dle potřeby. Například, pro skenování celé složky `Program Files`, stačí vybrat příslušné přednastavené umístění z rozbalovací nabídky. Pro skenování konkrétní složky v `Program Files`, musíte doplnit cestu přidáním lomítka (\) a názvu složky.
     - Pokud jste vybrali **Určité cesty**, zadejte celou cestu k objektu, který má být oskenován. Pro jistotu, že je cesta platná na všech cílových virtuálních strojích, doporučujeme používat systémové proměnné (tam, kde je to vhodné). Další informace o systémových proměnných naleznete na „Systémové proměnné“ (str. 567).

  c. Klikněte na odpovídající tlačítko ⊕ **Přidat**.

  Klikněte na něj pro úpravu existujícího umístění. Klikněte na odpovídající tlačítko ⊗ **Odstranit** pro odstranění umístění ze seznamu.

  Pro úlohy skenování sítě musíte zadat pověření uživatelského účtu s oprávněními pro čtení/psaní na cílové síťové jednotky, aby bezpečnostní agent mohl přistupovat a provádět na nich opatření.

  Klikněte na sekci **Výjimky**, pokud si přejete definovat výjimky.



Úloha skenování virtuálních strojů - definování výjimek

Můžete použít buď výjimky nastavené podle pravidel, nebo definovat určité výjimky pro aktuální skenovací úlohu. Pro více detailů ohledně výjimek, se prosím odkažte na „Výjimky“ (str. 280).

7. Kliknutím na **Uložit** vytvoříte úlohu skenování. Zobrazí se potvrzovací okno.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka
Pro naplánování skenovací úlohy přejděte na stránku **Pravidla**, zvolte pravidla přiřazená k virtuálním strojům, které vás zajímají, a přidejte skenovací úlohu v sekci **Antimalware > Na vyžádání**. Další informace viz „Manuální“ (str. 261).

Úlohy balíčků

Doporučejeme pravidelnou kontrolu aktualizací softwaru a jejich co nejrychlejší aplikaci. GravityZone tento proces provádí automaticky skrze bezpečnostní pravidla, ale pokud potřebujete aktualizovat software na určitých virtuálních strojích neprodleně, spusťte následující úlohy v tomto pořadí:

1. Skenování balíčků
2. Instalace balíčků

Podmínky

- Bezpečnostní agent s modulem Správa balíčků je nainstalovaný na cílových zařízeních.

- Aby proběhly úlohy skenování a instalace úspěšně, zařízení s Windows musí splňovat následující podmínky:
  - **Důvěryhodné autority pro certifikaci rootů** ukládá certifikát **DigiCert Assured ID Root CA**.
  - **Zprostředkující certifikační autority** zahrnují **DigiCert SHA2 Assured ID Code Signing CA**.
  - Koncové body nainstalovaly opravy pro systémy Windows 7 a Windows Server 2008 R2 uvedené v tomto článku společnosti Microsoft: Microsoft Security Advisory 3033929

Skenování balíčků

Virtuální zařízení se zastaralým softwarem jsou náchylná k útokům. Doporučujeme pravidelně kontrolovat software nainstalovaný na vašich zařízeních a co nejdříve ho aktualizovat. Pro skenování vašich zařízení na chybějící balíčky:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny koncové body z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Zvolte cílové koncové body.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Skenování balíčků**. Zobrazí se potvrzovací okno.
6. Klikněte na **Ano** pro potvrzení skenování.

   Jakmile je úloha dokončena, GravityZone přidá v Inventáři balíčků všechny balíčky, které software potřebuje. Více informací naleznete na „Inventář Balíčků“ (str. 191).

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka
Pro naplánování skenování balíčků upravte pravidla přiřazená k cílovým zařízením a nastavte parametry v sekci **Správa balíčků**. Další informace viz „Patch Management“ (str. 326).

Instalace balíčků

Pro instalaci jednoho nebo více balíčků na zvolená virtuální zařízení:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny koncové body z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Instalace balíčků**.

   Zobrazí se konfigurační okno. Zde můžete vidět všechny balíčky chybějící na cílových virtuálních zařízeních.
5. Pokud potřebujete najít konkrétní balíčky, použijte možnosti třízení a filtrování v horní části tabulky.
6. Klikněte na tlačítko **Sloupce** v pravé horní části panelu pro zobrazení pouze relevantních informací.
7. Zvolte balíčky, které chcete nainstalovat.

   Určité balíčky jsou závislé na jiných. V takovém případě jsou automaticky zvoleny spolu s balíčkem.

   Kliknutím na čísla **CVEs** nebo **Produktů** zobrazíte levý panel. Panel obsahuje doplňující informace, jako jsou CVE, který popisuje balíčky co řeší nebo produkty pro které je balíček určen. Po přečtení klikněte na **Zavřít** a skryjte panel.
8. Vyberte **Restartujte koncové body po instalaci záplat či aktualizací pokud je to potřeba** tak aby jste restartovali okamžitě po instalaci záplat či aktualizací, když je restart systému vyžadován. Berte v úvahu, že tato akce může přerušit uživatelské aktivity.
9. Klikněte na **Instalovat**.

   Vytvoří se instalační úloha, společně s pod-úlohami pro každé cílové virtuální zařízení.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka

- Pro naplánování nasazení balíčků upravte pravidla přiřazená k cílovým nařízením a nastavte parametry v sekci **Správa balíčků**. Další informace viz „Patch Management“ (str. 326).

- Můžete také nainstalovat záplatu ze stránky **Inventář záplat (Patch Inventory)**, počínaje od konkrétní záplaty, o kterou se zajímáte. V tomto případě vyberte záplatu či aktualizaci ze seznamu a klikněte na tlačítko **Instalace (Install)** na vrchní straně tabulky a nakonfigurujte detaily k instalaci záplat či aktualizací. Více informací naleznete na „Instalování Balíčků“ (str. 195).
- Poté co nainstalujete záplatu či aktualizaci, doporučujeme zaslat úlohu Sken hledání záplat či aktualizací (Patch Scan) na všechny cílené koncové body. Tato úloha akttualizuje informace o záplatách a aktualizacích uložené v GravityZone pro vaše spravované sítě.

Odinstalovat záplaty či aktualizace můžete takto:

- Vzdáleně na dálku, tím že pošlete úlohu odinstalace záplat (patch uninstall task) z GravityZone.
- Lokálně na vašem stroji. V tomto případě se musíte přihlásit jako administrator přímo na koncovém bodu a spustit odinstalátor manuálně.

Exchange Scan

Databázi Exchange serveru můžete skenovat na dálku spuštěním úlohy **Skenování Exchange**.

Pro skenování databáze Exchange musíte povolit skenování na vyžádání skrze poskytnutí pověření administrátora Exchange. Další informace viz „Skenování Exchange Store“ (str. 350).

Pro skenování databáze Exchange Serveru:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Z levého panelu, vyberte skupinu obsahující cílový Exchange Server. Můžete najít server zobrazený v pravém panelu.

   Poznámka
   Volitelně si můžete aplikovat filtry pro rychlé nalezení cílového serveru:
   - Klikněte na nabídku **Filtry** a zvolte následující možnosti: **Spravované (Exchange servery)** z karty **Zabezpečení** a **Všechny položky rekurzivně** z karty **Hloubka**.
   - Zadejte název serveru nebo IP adresu do pole příslušné hlavičky sloupce.

4. Vyberte zaškrtávací pole u Exchange Serveru, kde chcete skenovat databázi.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Skenování Exchange**. Zobrazí se konfigurační okno.

6. Konfigurace parametrů skenu:
   - **Obecné.** Zvolte pro úlohu definující jméno.

     Pro rozsáhlé databáze může skenování trvat velmi dlouho a může ovlivnit výkon serveru. V mnoha případech, vyberete zaškrtávací pole **Přerušit sken pokud zabere dále jak** a vyberte vyhovující časový interval z příslušných menu.
   - **Cíl.** Zvolte kontejnery a objekty, které mají být skenovány. Můžete si zvolit skenování mailových schránek, veřejných složek, nebo obou. Kromě emailů, můžete vybrat ke skenování objekty jako jsou **Kontakty**, **Úlohy**, **Schůzky** a **Položky pošty**. Navíc můžete pro skenovaný obsah nastavit následující omezení:
     – Pouze nepřečtené zprávy
     – Pouze položky s přílohami
     – Pouze nové objekty, přijaté za určitý časový interval

     Například, můžete vybrat skenovat emaily z uživatelských mailboxů, přijatých v posledních 7 dnech.

     Označte zaškrtávací pole **Výjimky**, pokud si přejete definovat výjimky ve skenování. Pro vytvoření výjimky, použijte pole z hlavičky tabulky jako například:
     a. Z nabídky zvolte typ úložiště.
     b. Na základě typu úložiště, zadejte objekt, který má být vyloučen:

Typ úložiště	Formát objektu
Mailbox	Emailová adresa
Veřejná Složka	Cesta složky od kořenové složky
Databáze	Identita databáze

     Poznámka
     Pro získání identity databáze použijte Exchange shell příkaz:
     `Get-MailboxDatabase | fl name,identity`

     Můžete zadat pouze jednu položku v danou chvíli. Pokud máte několik objektů stejného typu, musíte definovat tolik pravidel jako je počet objektů.
     c. Kliknutím na tlačítko ⊕ **Přidat** v horní části tabulky výjimku uložíte a přidáte do seznamu.

Pro odstranění pravidla výjimky ze seznamu klikněte na odpovídající tlačítko ⊖ **Odstranit**.

- **Možnosti.** Konfigurujte možnosti skenování pro emaily odpovídající pravidlu:
  - **Skanované typy souborů.** Tuto možnost použijte pro specifikování, které typy souborů chcete aby byli skenovány. Můžete si vybrat aby skenoval všechny soubory (nehledě na jejich příponu), pouze soubory aplikací nebo specifické přípony, které si myslíte, že by mohly být nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

    Poznámka
    Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

    Pokud chcete skenovat pouze soubory s určitou příponou, máte dvě možnosti:
    - **Uživatelem definované přípony**, zde musíte jen poskytnout přípony které mají být skenované.
    - **Všechny soubory, kromě určitých přípon**, kde musíte zadat pouze přípony, které mají být ze skenování vyloučeny.
  - **Maximální velikost příloh / statí emailů (MB).** Označte toto zaškrtávací pole a zadejte hodnotu do příslušného pole, čímž nastavíte maximální přijatelnou velikost připojeného souboru nebo statě emailu, který má být skenován.
  - **Archivujte maximum struktury (úrovní).** Vyberte zaškrtávací pole a vyberte maximální strukturu v příslušném poli. Čím nižší úroveň hloubky, tím je vyšší výkon a nižší třída ochrany.
  - **Skenovat potenciálně nechtěné aplikace (PUA).** Vyberte toto zaškrtávací pole pro skenování možných škodlivých nebo nechtěných aplikací jako je adware, který se nainstaloval do systému bez vědomí uživatele, mění chování vybraných softwarových produktů a snižuje výkon systému.
- **Akce.** Můžete určit akce, které má bezpečností agent automaticky provádět na souborech podle jejich typu.

  Podle typu detekce jsou soubory rozděleny do tří kategorií:
  - **Infikované soubory.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanismů, které zahrnují malwarové signatury, a technologie na bázi machine learning a umělé inteligence (AI).

- **Podezřelé soubory.** Tyto soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé).
- **Neskenovatelné soubory.** Tyto soubory nelze skenovat. Neskenovatelné soubory zahrnují, ale ne výlučně, soubory chráněné heslem, šifrované nebo překomprimované soubory.

Každý typ detekce má jednu hlavní akci a jednu alternativní pro případ, že ta hlavní selže. Přestože to nedoporučejeme, tyto akce je možné změnit v odpovídajících nabídkách. Zvolte akci, kterou si přejete provést:

- **Dezinfikovat.** Odstraní malwarový kód z nakažených souborů a obnoví původní soubor. V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech. Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.
- **Odmítnout / Odstranit email.** Na serverech s rolí Edge Transport je rozpoznaný email odmítnut s chybovým kódem 550 SMTP. Ve všech ostatních případech je email odstraněn bez varování. Této akci se doporučujeme vyhýbat.
- **Odstranit soubor.** Odstraní problémové přílohy bez varování. Této akci se doporučujeme vyhýbat.
- **Nahradit soubor.** Odstraní problémové soubory a přiloží textový soubor, který upozorní uživatele na přijatá opatření.
- **Přesunout sobuor do karantény.** Přesune rozpoznané soubory do složky s karanténou a přiloží textový soubor informující uživatele o přijatých opatřeních. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Soubory v karanténě můžete spravovat ze stránky **Karanténa**.

  > **Poznámka**
  > Mějte prosím na paměti, že karanténa pro Exchange servery vyžaduje na oddílu, na kterém je nainstalovaný bezpečnostní agent, místo na pevném disku navíc. Velikost karantény závisí na počtu uložených položek a jejich velikosti.

- **Nedělat nic.** S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu. Skenování je ve

výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení.

– Ve výchozím nastavení, pokud se email shoduje s rámcem pravidel, je s ním speciálně nakládáno v souladu s daným pravidlem, aniž by byl porovnán s jakýmkoli z dalších zbylých pravidel. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel.**

7. Kliknutím na **Uložit** vytvoříte úlohu skenování. Zobrazí se potvrzovací okno.
8. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Instalovat

Pro zabezpečení vašich virtuálních zařízení pomocí Security for Virtualized Environments, musíte na každý z nich nainstalovat bezpečnostního agenta Bitdefender. Bezpečnostní agent Bitdefender spravuje zabezpečení na virtuálních strojích. Také komunikuje s Control Center, aby mohl přijímat příkazy správce a odesílat výsledky provedených akcí. Jakmile nainstalujete do sítě bezpečnostního agenta Bitdefender, bude automaticky vyhledávat nechráněná virtuální zařízení v dané síti. Ochranu Security for Virtualized Environments lze nainstalovat na virtuální zařízení na dálku prostřednictvím Control Center. Instalace na dálku probíhá na pozadí bez vědomí uživatele.

V izolovaných sítích, které nemají přímé připojení k zařízení GravityZone, můžete nainstalovat bezpečnostního agenta s Funkcí Relay. V tomto případě, komunikace mezi GravityZone a dalšími bezpečnostními agenty bude probíhat skrze Relay agenta, který se chová také jako místní aktualizační server pro bezpečnostní agenty chránící izolovanou síť.

Poznámka
Doporučujeme ponechat stroj, na který nainstalujete Relay agenta, stále zapnutý.

Varování
Před instalací se ujistěte, že jste z virtuálních zařízení odinstalovali existující antimalwarový nebo firewallový software. Instalace ochrany Bitdefender přes existující bezpečnostní software může ovlivnit jejich činnost a způsobit závažné systémové problémy. Se zahájením instalace budou Windows Defender a Windows Firewall automaticky vypnuty.

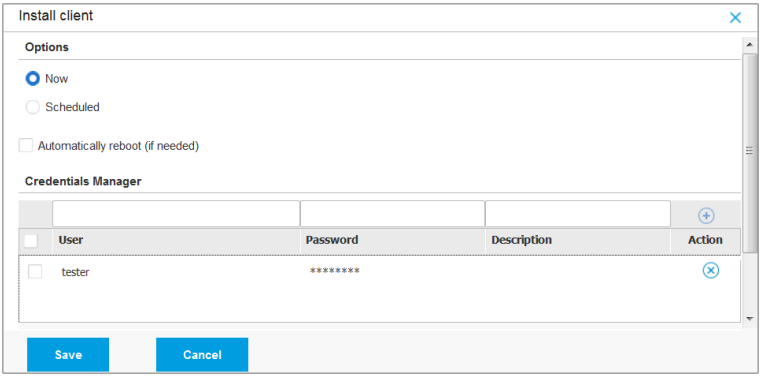
Pro vzdálenou instalaci ochrany Security for Virtualized Environments na jedno nebo více virtuálních zařízení:

1. Připojte a přihlaste se do Control Center.
2. Jděte do záložky **Síť**.
3. Z možnosti zobrazení vyberte **Virtuální Stroje**.
4. Zvolte požadovaný kontejner z levého panelu. Všechny dostupné jednotky ve vybrané skupině jsou zobrazeny v pravém panelu tabulky.

   Poznámka
   Případně můžete také použít filtry a zobrazit pouze nespravovaná zařízení. Klikněte na nabídku **Filtry** a zvolte následující možnosti: **Nespravované** z karty **Zabezpečení** a **Všechny položky rekurzivně** z karty **Hloubka**.

5. Vyberte objekty (virtuální zařízení, hostitelé, svazky nebo skupiny), na které chcete nainstalovat ochranu.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Instalovat > BEST**.

   Zobrazí se průvodce **Instalačním klientem**.



Instalace Bitdefender Endpoint Security Tools z Nabídky úloh

7. V sekci **Možnosti** nastavte čas instalace:
   - **Nyní**, čímž spustíte okamžité zavádění.

- **Plánovaný**, čímž nastavíte interval opakování zavádění. V tomto případě zvolte svůj požadovaný časový interval (každou hodinu, den nebo týden) a nastavte ho dle svých potřeb.

  Poznámka
  Například, když je na cílovém stroji nutné před instalací klienta nejprve provést určité operace (jako je odinstalace jiného softwaru a restartování OS), můžete zavedení nastavit tak, aby se spustilo každé 2 hodiny. Úloha se na každém koncovém bodě spustí každé 2 hodiny, dokud zavedení neproběhne úspěšně.

8. Pokud chcete, aby se koncové body automaticky restartovaly pro dokončení instalace, zvolte **Restartovat automaticky (je-li potřeba)**.
9. V sekci **Správce pověření** upřesněte administrativní pověření nezbytné pro vzdálenou autentizaci na cílových koncových bodech. Pověření můžete přidat zadáním uživatelského jména a hesla pro každý cílový operační systém.

   Důležité
   Pro stanice Windows 8.1 musíte poskytnout oprávnění zabudovaného administrátorského účtu, nebo účtu administrátora domény. Více informací naleznete v tomto KB článku.

   Poznámka
   Pokud nezvolíte žádná pověření, zobrazí se okno s varováním. Tento krok je povinný pro vzdálenou instalaci Bitdefender Endpoint Security Tools na koncové body.

   Pro přidání požadovaných oprávnění OS:

   a. Zadejte uživatelské jméno a heslo administrátorského účtu pro každý cílový operační systém do příslušných polí v záhlaví tabulky s pověřeními. Můžete také přidat popis, který vám usnadní identifikaci jednotlivých účtů.

      Pokud jsou zařízení v doméně, stačí zadat pověření administrátora domény.

      Při zadávání jména uživatelského účtu použijte konvence systému Windows:

      - Pro stroje s Active Directory použijte tyto syntaxe: `username@domain.com` a `domain\username`. Abyste si mohli být jisti, že pověření budou fungovat, zadejte je v obou tvarech (`username@domain.com` a `domain\username`).

- Pro stroje Pracovní skupiny stačí zadat pouze uživatelské jméno bez jména pracovní skupiny.

b. Klikněte na tlačítko ⊕ **Přidat**. Účet je přidán do seznamu oprávnění.

> **Poznámka**
> Zadaná pověření jsou automaticky uložena do vašeho Správce pověření, takže je příště už nemusíte zadávat. Do Správce pověření vstoupíte tak, že kliknete na vaše uživatelské jméno v pravém horním rohu konzole.

> **Důležité**
> Pokud jsou poskytnutá pověření neplatná, zavedení klienta na odpovídajících koncových bodech selže. Pokud jsou pověření na cílových koncových bodech změněna, ujistěte se, že jste aktualizovali zadaná pověření OS ve Správci pověření.

c. Označte zaškrtávací pole odpovídající účtům, které chcete použít.

10. V sekci **Zavaděč** nastavte objekt, ke kterému se budou cílová zařízení připojovat při instalaci a aktualizacích klienta:

- **Zařízení GravityZone**, když se zařízení připojují přímo k zařízení GravityZone.

  Pro tento případ můžete také určit vlastní Komunikační server tak, že zadáte jeho IP nebo název hostitele, pokud je třeba.

- **Endpoint Security Relay** pokud chcete připojit stroje k klientovi Relay nainstalovanému ve vaší síti. Všechny stroje s funkcí relay, nalezené ve vaší síti, budou uvedeny v níže zobrazené tabulce. Zvolte požadovaný stroj s relay. Připojené koncové body budou komunikovat s Control Center pouze prostřednictvím zvoleného relaye.

> **Důležité**
> - Aby zavedení prostřednictvím relay agenta fungovalo, port 7074 musí být otevřený.
> - Při nasazování agenta prostřednictvím linuxového relay musí být splněny následující podmínky:
>   - Relay musí mít nainstalovaný balíček Samba (`smbclient`) , verzi 4.1.0 nebo novější, `net` aby mohl zavádět agenty Windows.

Poznámka
Příkaz `net` binární/příkaz je obvykle dodáván s balíčky samba-client a / nebo samba-common. Na některých distribucích systému Linux (například CentOS 7.4) je příkaz `net` instalován pouze při instalaci úplné sady Samba (Common + Client + Server). Ujistěte se, že váš koncový bod přenosu má k dispozici příkaz `net`.

- Cílové koncové body Windows musí mít zapnuté Administrative Share a Network Share.
- Cílové koncové body Linux a Mac musí mít zapnutý SSH a vypnutý firewall.

11. Pro aktuální zavedení musíte zvolit jeden instalační balíček. Klikněte na seznam **Použít balíček** a zvolte požadovaný instalační balíček. Zde můžete najít všechny instalační balíčky, které byly již dříve vytvořeny pro vaši společnost.
12. Pokud potřebujete, můžete upravit některá nastavení zvoleného balíčku kliknutím na tlačítko **Upravit** vedle pole **Použít balíček**.

    Nastavení instalačního balíčku se zobrazí níže a vy budete moci provést požadované změny. Více informací o úpravě instalačních balíčků naleznete v GravityZone Instalační Příručce.

    Varování
    Mějte prosím na paměti, že modul Firewall je dostupný pouze pro podporované pracovní stanice Windows.

    Pokud si přejete uložit změny jako nový balíček, vyberte možnost **Uložit jako balíček**, umístěnou ve spodní části seznamu nastavení balíčku, a zadejte název nového instalačního balíčku.
13. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

Odinstalovat klienta

Pro odinstalaci zabezpečení Bitdefender na dálku:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.

3. Zvolte požadovaný kontejner z levého panelu. Všechny jednotky z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Označte zaškrtávací pole virtuálních strojů, ze kterých chcete odinstalovat bezpečnostního agenta Bitdefender.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Odinstalovat klienta**.
6. Zobrazí se konfigurační okno, které vám umožní provést následující nastavení:
   - Můžete si zvolit ponechání souborů v karanténě na klientském stroji.
   - Pro prostředí integrovaná s vShieldem musíte vybrat požadovaná pověření pro každý stroj, nebo se nepodaří provést odinstalaci. Vyberte **Použít pověření pro integraci s vShield** a poté zkontrolujte všechna příslušná pověření v tabulce Správce pověření zobrazené níže.
7. Kliknutím na **Uložit** vytvoříte úlohu. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Poznámka
Pokud chcete znovu nainstalovat ochranu, ujistěte se, že jste nejprve restartovali počítač.

Aktualizace

Pravidelně kontrolujte stav spravovaných virtuálních zařízení. Pokud naleznete virtuální stroj s bezpečnostními problémy, klikněte na jeho jméno pro zobrazení okna s **Informacemi**. Další informace viz „Stav zabezpečení“ (str. 108).

Zastaralí klienti nebo bezpečnostní obsah představují bezpečnostní rizika. V těchto případech byste měli na příslušných virtuálních zařízeních spustit aktualizaci. Tuto úlohu je možné provést lokálně z virtuálního zařízení, nebo vzdáleně z Control Center.

Chcete-li vzdáleně aktualizovat klienta a obsah zabezpečení na spravovaných virtuálních počítačích:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny jednotky z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.

4. Označte zaškrtávací pole virtuálních zařízení, na kterých chcete spustit aktualizaci klienta.
5. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Aktualizace**. Zobrazí se konfigurační okno.
6. Můžete se rozhodnout pro aktualizaci pouze produktu, bezpečnostního agenta nebo obou.
7. Pro operační systémy Linux integrované s vShield je nutné zvolit také požadovaná pověření. Označte možnost **Použít pověření pro Linux a integraci s vShield** a poté vyberte příslušná pověření v tabulce Správce pověření zobrazené níže.
8. Klikněte na **Aktualizovat** a spusťte úlohu. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Přenastavení klienta

Ochranné moduly, role a režimy skenování bezpečnostního agenta jsou předem nakonfigurovány v rámci instalačního balíčku. Poté, co nainstalujete bezpečnostního agenta do vaší sítě, můžete kdykoli změnit počáteční nastavení tak, že na dálku odešlete úlohu**Přenastavit klienta** na požadované spravované koncové body.

Varování
Mějte prosím na paměti, že úloha **Přenastavit klienta** přepíše všechna instalační nastavení a žádné z původních nastavení pak neplatí. Při využívání této úlohy se ujistěte, že jste přenastavili všechna instalační nastavení na cílových koncových bodech.

Pro změnu instalačních nastavení na jednom nebo více virtuálních zařízeních:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny jednotky z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Označte zaškrtávací pole virtuálních zařízení, u kterých chcete změnit instalační nastavení.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Přenastavit klienta**.

6. V sekci **Obecné** nastavte čas, kdy bude úloha provedena:
   - **Nyní**, což spustí úlohu okamžitě.
   - **Plánovaný**, čímž nastavíte interval opakování zavádění. V tomto případě zvolte svůj požadovaný časový interval (každou hodinu, den nebo týden) a nastavte ho dle svých potřeb.

     Poznámka
     Například, když mají na cílovém stroji probíhat také další důležité procesy, můžete úlohu nastavit tak, aby se spustila každé 2 hodiny. Úloha se na každém cílovém stroji spustí každé 2 hodiny, dokud neproběhne úspěšně.

7. Nastavte moduly, role a režimy skenování pro cílový koncový bod tak, jak si přejete. Více informací naleznete v instalačním průvodci GravityZone.

   Varování
   - Nainstalují se pouze moduly, které jsou v daném operačním systému podporované.

     Mějte prosím na paměti, že modul Firewall je dostupný pouze pro podporované pracovní stanice Windows.
   - Bitdefender Tools (starší verze agenta) podporuje pouze Centrální skenování.

8. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Vyhledání sítě

Vyhledání sítě probíhá automaticky pouze prostřednictvím bezpečnostních agentů s funkcí Relay. Pokud v síti nemáte nainstalovaného relay agenta, musíte poslat úlohu pro nalezení sítě z chráněného koncového bodu ručně.

Pro spuštění úlohy vyhledání sítě ve vaší síti:

Důležité
okud používáte relay Linux pro nalezení dalších koncových bodů s Linux nebo Mac, musíte na koncové body buď nainstalovat Samba, nebo je propojit v Active Directory a použít DHCP. Tímto na nich bude NetBIOS automaticky nastaven.

1. Jděte do záložky **Síť**.

2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny jednotky z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Zaškrtněte políčko zařízení, které má provádět vyhledání sítě.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Vyhledání sítě**.
6. Zobrazí se potvrzovací okno. Klikněte na **Ano**.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Vyhledání aplikací

Pro vyhledání aplikací ve vaší síti:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny virtuální zařízení z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Vyberte virtuální stroje, na kterých potřebujete provést hledání aplikací.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Vyhledání aplikací**.

   Poznámka
   Bitdefender Endpoint Security Tools se Řízením Aplikací musí být nainstalována a aktivní na vybraných virtuálních strojích. V opačném případě bude úloha zobrazena šedě. Když zvolená skupina obsahuje jak vyhovující, tak nevyhovující cíle, úloha bude odeslána pouze na vyhovující koncová zařízení.

6. Pro pokračování klikněte na **Ano** v potvrzovacím okně.

Objevené aplikace a procesy jsou zobrazeny v záložce **Network > Application Inventory**. Další informace viz „Inventář aplikací“ (str. 186).

Poznámka
Úloha **Applications Discovery** bude chvilku trvat, na základě počtu aplikací, které jsou nainstalovány. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Restartovat stroj

Můžete si zvolit vzdálený restart spravovaných virtuálních zařízení.

Poznámka
Předtím, než restartujete určitá virtuální zařízení, zkontrolujte stránku **Síť > Úlohy**. Cílová zařízení mohou stále zpracovávat předtím zadané úlohy.

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny jednotky z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Označte pole virtuálních zařízení, která chcete restartovat.
5. Klikněte na tlačítko **Úlohy** v horní části tabulky a zvolte **Restartovat stroj**.
6. Vyberte možnost plánovaného restartu:
   - Zvolte **Restartovat nyní** a restartujte virtuální zařízení okamžitě.
   - Zvolte **Restartovat v** a pomocí polí níže naplánujte restartování v požadovaný datum a čas.
7. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Více informací naleznete v Prohlížení a správa úloh.

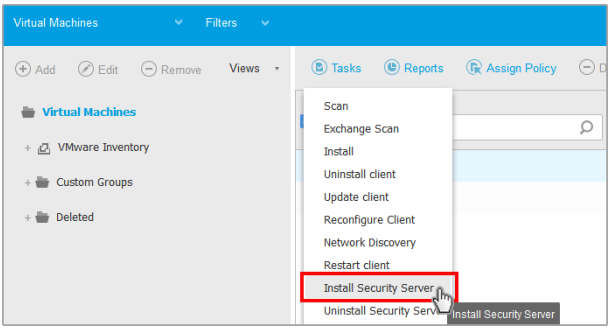
Instalovat Security Server

Pro instalaci Security Server ve vašem virtuálním prostředí:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Prohlédněte si Nutanix, VMware nebo Citrix inventář a vyberte si pomocí označovacích rámečků příslušné chtěné hosty nebo kontejnery (Nutanix Prism, vCenter Server, XenServer or datacenter). Pro rychlý výběr, si můžete přímo vybrat (root) kořenový kontejner (Nutanix inventář, VMware inventář nebo Citrix inventář). Budete moci zvolit hostitele jednotlivě z instalačního průvodce.

   Poznámka
   Nemůžete vybírat hostitele z různých složek.

4. Klikněte na tlačítko **Úlohy** v horní části tabulky a z menu vyberte **Aktualizovat Security Server**. Zobrazí se okno **Instalace Security Server**.



Instalace Security Server z Nabídky úloh

5. Všichni hostitelé nalezení ve zvoleném kontejneru se zobrazí na seznamu. Vyberte hostitele, na které chcete instalovat Security Servery.
6. Vyberte konfigurační nastavení, která chcete použít.

> **Důležité**
> Používání obecných nastavení při zavádění několika Security Serverů současně vyžaduje od hostitelů, aby sdíleli tu samou paměť, měli IP adresy přiřazené DHCP serverem, a byli součástí té samé sítě.

7. Klikněte **Další**.
8. Pro každé zařízení vCenter zadejte odpovídající pověření VMware vShield.
9. Zadejte definující jméno pro Security Server.
10. Pro VMware prostředí si vyberte kontejner, do kterého chcete zahrnout Security Server z menu **Nasadit Kontejner (Deploy Container)** menu.
11. Vyberte cílovou paměť.
12. Vyberte typ zásobování disku. Doporučujeme používat zásobování tlustého disku.

Důležité
Pokud použijete zásobování tenkého disku a místo na disku v datovém úložišti dojde, Security Server zamrzne a hostitel tím pádem zůstane nechráněný.

13. Nastavte paměť a přidělování zdrojů pevnému disku na základě poměru konsolidace na hostiteli. Zvolte **Nízké**, **Střední** nebo **Vysoké** pro načtení doporučeného nastavení přidělování zdrojů, nebo **Ručně** pro nastavení přidělování zdrojů ručně.
14. Chcete nastavit administrativní heslo pro Security Server konzoli. Nastavení hesla pro správu přepíše výchozí kořenové heslo ("sve").
15. Nastavte časovou zónu zařízení.
16. Vyberte typ síťové konfigurace pro síť Bitdefender. IP adresa Security Server se nesmí změnit, protože ji agenti Linux používají ke komunikaci.

    Pokud zvolíte DHCP, ujistěte se, že jste nastavili DHCP server tak, aby rezervoval IP adresu zařízení.

    Pokud vyberete statický, musíte zadat IP adresu, masku podsítě, bránu a informace o DNS.
17. Vyberte síť vShield a zadejte pověření pro vShield. Výchozí štítek pro síť vShield je `vmservice-vshield-pg`.
18. Kliknutím na **Uložit** vytvoříte úlohu. Zobrazí se potvrzovací okno.

Důležité

- Balíčky Security Server nejsou automaticky zahrnuty v zařízení GravityZone. Podle nastavení určených správcem systému bude balíček Security Server, nezbytný pro vaše prostředí, buď stažen při spuštění instalační úlohy Security Server, nebo bude správce upozorněn na chybějící obraz a instalace neproběhne. V případě chybějícího balíčku ho bude muset správce systému stáhnout ručně, aby umožnil instalaci.
- Instalace Security Serveru na Nutanix pomocí vzdálené úlohy může selhat pokud je Prism Element cluster registrovaný do Prism Central nebo i z jiného důvodu. V těchto situacích, je doporučeno provést manuální nasazeníSecurity Serveru. Pro více informací čtěte KB article.

19. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Odinstalovat Security Server

Pro odinstalování Security Server:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Vyberte datové centrum nebo složku, která obsahuje hostitele, na kterém je Security Server nainstalovaný.
4. Označte pole odpovídající hostiteli, na kterém je Security Server nainstalovaný.
5. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Odinstalovat Security Server**.
6. Pro vytvoření úlohy zadejte pověření pro vShield a klikněte na **Ano**.
7. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Aktualizovat Security Server

Pro aktualizování Security Server:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Vyberte hostitele, na kterém je Security Server nainstalovaný.

   Pro snadné nalezení Security Server můžete použít nabídku **Filtrů** následujícím způsobem:

   - Přejděte na kartu **Zabezpečení** a vyberte pouze **Bezpečnostní servery**.
   - Přejděte na kartu **Hloubka** a zvolte **Všechny položky rekurzivně**.

   Poznámka
   Pokud používáte nástroj pro virtualizační správu, který momentálně není integrovaný s Control Center, Security Server bude umístěn pod **Vlastní skupiny**. Pro více informací ohledně podporovaných virtualizačních platforem se podívejte do Průvodce instalací GravityZone.

4. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Aktualizovat Security Server**.
5. Je nutné potvrdit kliknutím na **Ano**.

6. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Důležité
Doporučujeme vám využít tento způsob pro aktualizování Security Serveru pro NSX, nebo ztratíte karanténu uloženou na zařízení.

Instalovat Doplňkový balíček HVI

Pro ochranu virtuálních strojů s HVI musíte na hosta nainstalovat doplňkový balíček. Role toho balíčku je zajištění komunikace mezi Hypervisorem a Security Server instalovaném u hosta. Jakmile je nainstalovaný, HVI chrání virtuální stroje, které mají HVI povolený ve svých pravidlech.

Důležité
- HVI chrání virtuální stroje výhradně na hypervizorech Citrix Xen.
- Není nutné, abyste z virtuálních zařízení odinstalovali stávajícího bezpečnostního agenta.

Pro instalaci doplňkového balíčku na hostitele:

1. Přejděte na stránku **Konfigurace > Aktualizace**.
2. Vyberte Doplňkový balíček HVI ze seznamu **Komponentů** a klikněte na tlačítko **Stáhnout** v horní části tabulky.
3. Přejděte na stránku **Síť** a v nastavení zobrazení vyberte **Virtuální zařízení**.
4. Z menu **Zobrazení** v levém panelu vyberte **Server**.
5. Vyberte jednoho nebo více hostitelů Xen ze síťového inventáře. Dostupné hostitele můžete snadno prohlížet zvolením možnosti **Typ > Hostitelé** v nabídce **Filtry**.
6. Klikněte na tlačítko **Úlohy** na pravé liště a vyberte **Instalovat Doplňkový balíček HVI**. Otevře se instalační okno.
7. Naplánujte, kdy má být instalační úloha spuštěna. Můžete si zvolit, zda chcete spustit úlohu okamžitě po jejím uložení, nebo v konkrétním čase. V případě, že instalaci nelze dokončit v určený čas, úloha bude automaticky opakována podle nastavených parametrů pro opakování. Například, pokud vyberete více hostitelů a jeden hostitel je v době, kdy má instalace balíčku proběhnout nedostupný, úloha se spustí znovu v určeném čase.

8. Hostitel musí být restartován pro aplikování změn a dokončení instalace. Pokud chcete, aby se hostitel sám restartoval, zvolte **Restartovat automaticky (je-li potřeba)**.
9. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

Odinstalovat Doplňkový balíček HVI

Poznámka
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Pro odinstalaci Doplňkového balíčku z hostitelů:

1. Přejděte na stránku **Síť** a v nastavení zobrazení vyberte **Virtuální zařízení**.
2. Z menu **Zobrazení** v levém panelu vyberte **Server**.
3. Vyberte jednoho nebo více hostitelů Xen ze síťového inventáře. Dostupné hostitele můžete snadno prohlížet zvolením možnosti **Typ > Hostitelé** v nabídce **Filtry**.
4. Klikněte na tlačítko **Úlohy** na pravé liště a vyberte **odinstalovat Doplňkový balíček HVI**. Otevře se konfigurační okno.
5. Naplánujte, kdy chcete balíček odstranit. Můžete si zvolit, zda chcete spustit úlohu okamžitě po jejím uložení, nebo v konkrétním čase. V případě, že odstranění nelze dokončit v určený čas, úloha bude automaticky opakována podle nastavených parametrů pro opakování. Například, pokud vyberete více hostitelů a jeden hostitel je v době, kdy má odstranění balíčku proběhnout nedostupný, úloha se spustí znovu v určeném čase.
6. Hostitel musí být restartován pro dokončení odstraňování. Pokud chcete, aby se hostitel sám restartoval, zvolte **Restartovat automaticky (je-li potřeba)**.
7. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

Aktualizovat Doplňkový balíček HVI

Pro aktualizaci Doplňkového balíčku na hostitelích:

1. Nainstalujte nejnovější dostupnou doplňkovou sadu HVI.

Další informace viz „Instalovat Doplňkový balíček HVI“ (str. 154).

2. Jděte do záložky **Síť**.
3. Z výběrového zobrazení vyberte **Virtuální počítače** .
4. Z menu **Zobrazení** v levém panelu vyberte **Server**.
5. Vyberte jednoho nebo více hostitelů Xen ze síťového inventáře.

   Dostupné hostitele můžete snadno prohlížet zvolením možnosti **Typ > Hostitelé** v nabídce **Filtry**.
6. Klikněte na tlačítko **Úlohy** na pravé horní liště a vyberte **Aktualizovat Doplňkový balíček HVI**. Otevře se konfigurační okno.
7. Naplánujte, kdy chcete balíček aktualizovat. Můžete si zvolit, zda chcete spustit úlohu okamžitě po jejím uložení, nebo v konkrétním čase.

   V případě, že aktualizaci nelze dokončit v určený čas, úloha bude automaticky opakována podle nastavených parametrů pro opakování. Například, pokud vyberete více hostitelů a jeden hostitel je v době, kdy má aktualizace balíčku proběhnout nedostupný, úloha se spustí znovu v určeném čase.
8. Vyberte **Automaticky restartovat (v případě potřeby)** , pokud chcete restartovat hostitele bez dozoru. V opačném případě musíte restartovat hostitele ručně, aby se aktualizace použila.
9. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

Stav úlohy můžete zkontrolovat na stránce **síť > úkoly** .

Přidávání Vlastních Nástrojů

Poznámka
Tato úloha je spojena s modulem HVI, který je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Pro přidání nástrojů v cílovém hostovacím operačním systému:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Vyberte skupinu, kterou chcete z levého panelu. Všechny koncové body z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Vyberte zaškrtávací pole cílového koncového zařízení.

5. Klikněte na tlačítko **Tasks** na pravé straně tabulky a vyberte **Inject Custom Tool**. Zobrazí se konfigurační okno.
6. Z Rozbalovacího menu, vyberte všechny nástroje které chcete použít. Pro každý vybraný nástroj se zobrazí skládací sekce s jejím nastavením.

   Tyto nástroje byli předtím nahrány do GravityZone. Pokud nemůžete najít správný nástroj v seznamu, přejděte do **Tools Management Center** a odtud je přidejte. Další informace viz „Zavedení vlastních nástrojů s HVI“ (str. 532).
7. Pro každý zobrazený nástroj v okně:
   a. Klikněte na název nástroje pro zobrazení nebo skrytí jeho sekce.
   b. Zadejte příkazovou řádku nástroje, společně se všemi potřebnými parametry, stejně jako v Příkazovém Řádku nebo Terminálu. Například:

      ```
      bash script.sh <param1> <param2>
      ```

      Pro BD Remediation Tools můžete vybrat pouze nápravu akce a zálohovat nápravnou akci ze dvou rozbalujících menu.
   c. Umístění od kut Security Server by měl získávat logy:
      - **stdout**. Vyberte toto zaškrtávací pole pro získávání logů ze standardního odchozího komunikačního kanálu.
      - **Output file**. Vyberte toto zaškrtávací pole pro sbírání souborů logu na koncových zařízeních. V tomto případě, potřebujete zadat cestu, kde Security Server nalezne soubor. Můžete použít absolutní cesty nebo systémové proměnné.

        Zde je další možnost: **Delete log files from Guest after they have been transferred**. Vyberte ji pokud již nepotřebujete soubory na koncových zařízeních.
8. Pokud chcete přemístit soubory logů ze Security Server někam jinam, musíte poskytnout cestu kam se mají uložit a údaje pro authentifikaci.
9. Někdy nástroje mohou vyžadovat více času než se očekává dokončení jejich práce nebo mohou přestat odpovídat. Pro předejití pádům v mnoha situacích, v sekci **Safety configuration**, vyberte po kolika hodinách Security Server by měl automaticky ukončit proces nástroje.
10. Klikněte na tlačítko **Save**.

Budete moci zobrazit status úlohy v záložce **Tasks**. Pro více informací se můžete obrátit také na hlášení **HVI Stav zásahu třetí strany**.

6.3.6. Tvorba Rychlých hlášení

Můžete vytvářet okamžitá hlášení na spravovaných virtuálních zařízeních, počínaje na stránce **Síť**.

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny virtuální zařízení z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Filtrujte obsah zvolené skupiny pouze podle spravovaných virtuálních zařízení.
5. Označte pole odpovídající virtuálním zařízením, která chcete zahrnout v hlášení.
6. Klikněte na tlačítko **Hlášení** v horní části tabulky a z nabídky zvolte typ hlášení. Další informace viz „Hlášení pro počítače a virtuální stroje“ (str. 478).
7. Nastavte parametry hlášení. Další informace viz „Vytváření hlášení“ (str. 497)
8. Klikněte na tlačítko **Vytvořit**. Hlášení se okamžitě zobrazí. Čas potřebný k vytvoření hlášení se může lišit podle počtu zvolených virtuálních zařízení.

6.3.7. Přiřazování pravidel

Bezpečnostní nastavení virtuálních zařízení můžete spravovat prostřednictvím pravidel.

Na stránce **Síť** můžete prohlížet, změnit a přiřazovat pravidla pro každé virtuální zařízení nebo skupinu virtuálních zařízení.

Poznámka
Bezpečnostní nastavení jsou dostupná pouze pro spravovaná virtuální zařízení. Pro snazší prohlížení a správu bezpečnostních nastavení můžete filtrovat síťový inventář pouze podle spravovaných virtuálních zařízení.

Pro zobrazení bezpečnostních nastavení přiřazených ke konkrétnímu virtuálnímu zařízení:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.

3. Zvolte požadovaný kontejner z levého panelu. Všechny virtuální zařízení z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Klikněte na jméno požadovaného virtuálního zařízení. Zobrazí se informační okno.
5. Pod kartou **Obecné** v sekci **Pravidla** klikněte na název současného pravidla a prohlížejte jeho nastavení.
6. Bezpečnostní nastavení můžete měnit dle potřeby, pod podmínkou, že majitel pravidel povolil ostatním uživatelům v nich provádět změny. Mějte prosím na vědomí, že veškeré vámi provedené změny ovlivní všechna virtuální zařízení se stejným přiřazeným pravidlem.

   Pro více informací o nastavení pravidel na virtuálních zařízeních se odkažte na„Zásady zabezpečení“ (str. 212)

Pro přiřazení pravidla k virtuálnímu zařízení nebo ke skupině virtuálních zařízení:

1. Jděte do záložky **Síť**.
2. Z možnosti zobrazení vyberte **Virtuální Stroje**.
3. Zvolte požadovaný kontejner z levého panelu. Všechny virtuální zařízení z vybraného kontejneru jsou zobrazeny v tabulce v pravém panelu.
4. Označte pole požadované jednotky. Jednu nebo více položek stejného typu můžete zvolit pouze na té samé úrovni.
5. Klikněte na tlačítko **Přiřadit pravidlo** v horní části tabulky.
6. Proveďte potřebná nastavení v okně **Přiřazení pravidel**.

   Další informace viz „Přiřazování pravidel“ (str. 215).

Varování
Pro pravidla s povoleným Hypervisor Memory Introspection, cílové stroje mohou po přiřazení pravidel vyžadovat restartování systému. Zařízení v tomto stavu jsou na stránce **Síť** označeny ikonou **Ve frontě na restart**.

6.3.8. Použití Správce obnovení pro šifrované svazky

Když koncoví uživatelé zapomenou svá šifrovací hesla a nemohou na svých počítačích přistupovat k šifrovaným svazkům, můžete jim pomoci načtením obnovovacích klíčů ze stránky **Síť** .

Pro získání klíče obnovy:

1. Jděte do záložky **Síť**.
2. Klikněte na tlačítko **Správce obnovení** na panelu nástrojů akcí na levé straně okna. Objeví se nové okno.
3. V části **Identifikátor** okna zadejte následující data:
   a. ID klíče pro obnovení šifrovaného svazku. ID klíče pro obnovení je řetězec čísel a písmen dostupných v koncovém bodě na obrazovce obnovy BitLocker.

      V systému Windows je ID klíče pro obnovení řetězec čísel a písmen dostupných v koncovém bodu na obrazovce pro obnovení BitLocker.

      Alternativně můžete použít možnost **Obnova** na kartě **Ochrana** podrobností virtuálního počítače Automaticky vyplnit ID klíče obnovy pro koncové body Windows i MacOS.
   b. Heslo vašeho účtu GravityZone.
4. Klikněte na **Odkrýt**. Okno se rozbalí.

   Informace o svazku vám představí následující údaje:
   a. Název svazku
   b. Typ svazku (boot nebo non-boot).
   c. Název koncového bodu (jak je uveden v síťovém inventáři)
   d. Obnovovací klíč. V systému Windows je klíčem pro obnovení heslo generované automaticky po zašifrování svazku. V systému Mac je klíčem pro obnovení heslo uživatele.
5. Odešlete klíč pro obnovení koncovému uživateli.

Pro více informací ohledně šifrování a dešifrování svazků s GravityZone se odkažte na „Šifrování“ (str. 370).

6.3.9. Uvolňování licenčních míst

V Active Directory, vCenter Serveru (bez vShieldu, NSX or HVI) a inventářích Xen Serveru můžete snadno uvolnit licencovaná místa využívaná virtuálními stroji tam, kde byl bezpečnostní agent odstraněn bez spuštění odinstalačního souboru.

Poté, co toto provedete, cílová zařízení budou v Síťovém inventáři jako nespravovaná.

Pro uvolnění místa v licenci:

1. Jděte do záložky **Síť**.
2. V nastavení zobrazení zvolte buď **Počítače a virtuální zařízení** nebo **Virtuální zařízení**.
3. Vyberte požadovanou skupinu v levém panelu. Všechna virtuální zařízení se zobrazí v tabulce na pravé straně.
4. Vyberte virtuální zařízení, ze kterého chcete odebrat licenci.
5. Klikněte na tlačítko ⊖ **Odebrat licenci** v horní části tabulky.
6. Pro pokračování klikněte na **Ano** v potvrzovacím okně.

6.4. Mobilní zařízení

Pro správu mobilních zařízení ve vaší společnosti je musíte nejprve přiřadit ke konkrétním uživatelům v Control Center, a poté nainstalovat a aktivovat aplikaci GravityZone Mobile Client na každém z nich.

Mobilní zařízení mohou být vlastněna společností, nebo jednotlivci. Můžete nainstalovat a aktivovat GravityZone Mobile Client na každém mobilním zařízení a to poté předat příslušnému uživateli. Uživatelé také mohou nainstalovat a aktivovat GravityZone Mobile Client sami podle instrukcí, které obdrží emailem. Více informací naleznete v instalačním průvodci GravityZone.

Pro zobrazení mobilních zařízení uživatelů pod vaším účtem přejděte do sekce **Síť** a z nastavení zobrazení vyberte **Mobilní zařízení**. Na stránce **Síť** jsou v levém panelu zobrazeny dostupné skupiny uživatelů, a v pravém panelu vidíte odpovídající uživatele a zařízení.

Pokud je nastavena integrace s Active Directory, můžete přidávat mobilní zařízení k existujícím uživatelům Active Directory. Můžete také vytvářet uživatele pod **Vlastními skupinami** a přidat k nim mobilní zařízení.

Můžete přepnout zobrazení pravého okna na **Uživatele**, nebo na **Zařízení** pomocí karty **Zobrazení** z nabídky **FIltry**, umístěného v horní části tabulky. V zobrazení **Uživatelů** můžete spravovat uživatele v Control Center, jako přidávat uživatele a mobilní zařízení a prohlížet počet zařízení na každého uživatele. Použijte zobrazení **Zařízení** pro snadnou správu a prohlížení podrobností o každém mobilním zařízení v Control Center.

Uživatele a mobilní zařízení můžete spravovat v Control Center následujícím způsobem:

- Přidat vlastní uživatele

- Přidat mobilní zařízení k uživatelům
- Organizovat vlastní uživatele do skupin
- Filtrování a vyhledávání uživatelů a zařízení
- Prohlížet stav a detaily uživatele nebo zařízení
- Spouštět úlohy na mobilních zařízeních
- Vytvořit rychlá hlášení o mobilních zařízeních
- Kontrolovat a měnit bezpečnostní nastavení zařízení
- Synchronizujte inventář Control Center s Active Directory
- Odstranit uživatele a mobilní zařízení

6.4.1. Přidávání vlastních uživatelů

Pokud je nastavena integrace s Active Directory, můžete přidávat mobilní zařízení k existujícím uživatelům Active Directory.

V situacích nesouvisejících s Active Directory musíte nejprve vytvořit vlastní uživatele, abyste získali prostředek pro identifikaci uživatelů mobilních zařízení.

Existují dva způsoby, jak vytvořit vlastní uživatele. Můžete buď přidávat jeden po druhém, nebo importovat CSV soubor.

Pro přidání vlastního uživatele:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Klikněte na nabídku **Filtry** v horní části tabulky a přejděte na kartu **Zobrazení**. Ujistěte se, že je možnost **Uživatelé** povolena.
4. V okně na levé straně vyberte **Vlastní skupiny**.
5. Klikněte na tlačítko **Přidat uživatele** v horní části tabulky. Zobrazí se konfigurační okno.
6. Určete požadované podrobnosti o uživateli:
   - Definující jméno (například celé jméno uživatele)
   - Emailová adresa uživatele

Důležité

- Ujistěte se, že zadáváte platnou emailovou adresu. Když přidáte zařízení, uživateli bude odeslán email s instrukcemi pro instalaci.
- Každá emailová adresa může být registrována pouze pro jednoho uživatele.

7. Klikněte **OK**.

Pro importování uživatelů mobilních zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Klikněte na nabídku **Filtry** v horní části tabulky a přejděte na kartu **Zobrazení**. Ujistěte se, že je možnost **Uživatelé** povolena.
4. V okně na levé straně vyberte **Vlastní skupiny**.
5. Klikněte na **Importovat uživatele**. Otevře se nové okno.
6. Zvolte CSV soubor a klikněte na **Importovat**. Okno se zavře a tabulka se zaplní importovanými uživateli.

> **Poznámka**
> Pokud dojde k jakýmkoli chybám, zobrazí se zpráva a v tabulce budou zobrazeni pouze platní uživatelé. Existující uživatelé budou přeskočeni.

Poté můžete pod **Vlastními skupinami** vytvořit skupiny uživatelů.

Pravidla a úlohy přiřazené k uživateli budou platit pro všechna zařízení ve vlastnictví daného uživatele.

6.4.2. Přidávání mobilních zařízení k uživatelům

Uživatel může mít neomezený počet mobilních zařízení. Můžete přidat zařízení jednomu nebo více uživatelům, ale zařízení můžete přidávat postupně pouze po jednom.

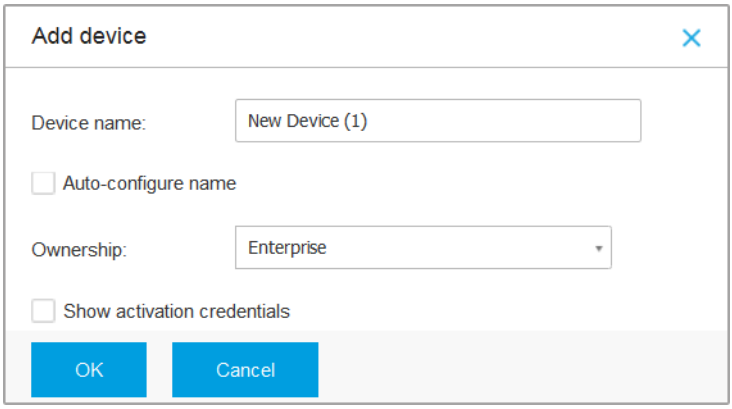
Přidání zařízení k jednomu uživateli

Pro přidání zařízení ke konkrétnímu uživateli:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Najděte uživatele ve skupině **Active Directory** nebo ve **Vlastních skupinách** a označte odpovídající pole na pravém panelu.

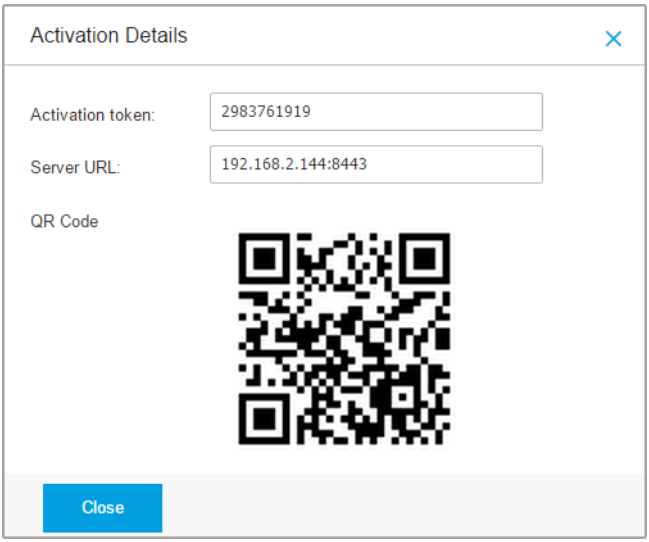
> **Poznámka**
> **Filtry** musí být nastaveny na **Uživatele** z karty **Zobrazení**.

4. Klikněte na tlačítko **Přidat uživatele** v horní části tabulky. Zobrazí se konfigurační okno.



Přidat mobilní zařízení k uživateli

5. Nastavte detaily mobilního zařízení:
   a. Zadejte pro zařízení definující jméno.
   b. Pokud chcete, aby byl název zařízení generován automaticky, použijte volbu **Automatické nastavení jména**. Poté, co je přidáno, má zařízení obecné jméno. Jakmile je zařízení aktivováno, je automaticky přejmenováno podle odpovídajícího výrobce a informace o modelu.
   c. Vyberte typ vlastnictví zařízení (podnikové nebo osobní). Mobilní zařízení můžete kdykoli filtrovat podle vlastnictví a spravovat je dle vašich potřeb.
   d. Zvolte možnost **Zobrazit aktivační pověření**, pokud hodláte nainstalovat GravityZone Mobile Client na zařízení uživatele.
6. Přidejte zařízení kliknutím na **OK**. Uživateli je okamžitě odeslán email s instrukcemi pro instalaci a podrobnosti pro aktivaci, které je potřeba nastavit na zařízení. Podrobnosti aktivace zahrnují aktivační token a adresu komunikačního serveru (a odpovídající QR kód).
7. Pokud jste zvolili volbu **Zobrazit aktivační pověření**, zobrazí se okno **Aktivační detaily**, které obsahuje unikátní aktivační token, adresu komunikačního serveru a odpovídající QR kód pro nové zařízení.



Aktivační detaily pro mobilní zařízení

Až budete po instalaci GravityZone Mobile Client vyzváni k aktivaci zařízení, zadejte aktivační token a adresu komunikačního serveru, nebo oskenujte obdržený QR kód.

Přidání zařízení více uživatelům

Pro přidání mobilních zařízení vybraným uživatelům a skupinám:

1. Jděte do záložky **Síť**.
2. Najděte uživatele ve složkách **Active Directory** nebo ve **Vlastních skupinách** a označte odpovídající pole na pravém panelu.

   Poznámka
   Filtry musí být nastaveny na **Uživatele** z karty **Zobrazení**.

3. Klikněte na tlačítko **Přidat zařízení** v horní části tabulky. V tomto případě musíte v konfiguračním okně definovat pouze vlastnictví zařízení.

   Pokud někteří uživatelé mají nespecifikovanou emailovou adresu, budete okamžitě upozorněni zprávou. Seznam odpovídajících uživatelů bude dostupný v **Oznamovací oblasti** v Control Center.

Mobilní zařízení vytvořená pomocí několikanásobného výběru mají v Control Center automaticky obecné jméno. Jakmile je zařízení aktivováno, je automaticky přejmenováno podle odpovídajícího výrobce a informace o modelu.

4. Přidejte zařízení kliknutím na **OK**. Uživatelům je okamžitě odeslán email s instrukcemi pro instalaci a podrobnosti pro aktivaci, které je potřeba nastavit na zařízení. Podrobnosti aktivace zahrnují aktivační token a adresu komunikačního serveru (a odpovídající QR kód).

Můžete zkontrolovat počet zařízení přiřazených ke každému uživateli na pravém panelu pod sloupcem **Zařízení**.

6.4.3. Organizace vlastních uživatelů do skupin

Dostupné skupiny uživatelů můžete prohlížet v panelu na levé straně stránky **Síť**.

Uživatelé Active Directory jsou seskupeni pod **Active Directory**. Skupiny Active Directory nemůžete upravovat. Můžete pouze prohlížet a přidávat zařízení příslušným uživatelům.

Všechny uživatele nepatřící k Active Directory můžete přidat pod **Vlastní skupiny**, kde můžete vytvářet a organizovat je do skupin dle potřeby. Hlavní výhodou této možnosti je, že můžete používat skupinová oprávnění pro splnění různých bezpečnostních požadavků.

Pod **Vlastními skupinami** můžete vytvořit, smazat, přejmenovat a přesunout skupiny uživatelů v rámci stromové struktury na míru.

Důležité
Mějte prosím na vědomí toto:

- Skupina může obsahovat jak uživatele, tak další skupiny.
- Při výběru skupiny v levém panelu můžete prohlížet všechny uživatele kromě těch, kteří jsou umístěni do jejích podskupin. Pro zobrazení všech uživatelů zahrnutých ve skupině a jejích podskupinách, klikněte na menu **Filtry** nacházející se v horní části tabulky a vyberte **Všechny objekty opakovaně** v sekci **Hloubka**.

Vytváření Skupin

Pro vytvoření vlastní skupiny:

1. V levém panelu vyberte **Vlastní skupiny**.
2. Klikněte na tlačítko ⊕ **Přidat skupinu** v horní části levého panelu.

3. Zadejte působivé jméno pro skupinu a klikněte na **OK**. Nová skupina je zobrazena pod **Vlastními skupinami**.

Přejmenování Skupin

Pro přejmenování vlastní skupiny:

1. Vyberte skupinu v levém panelu.
2. Klikněte na tlačítko **Upravit skupinu** v horní části levého panelu.
3. Zadejte nové jméno do odpovídajícího pole.
4. Potvrďte kliknutím na **OK**.

Přesouvání skupin a uživatelů

Skupiny a uživatele můžete přesouvat kamkoli v hierarchii **Vlastních skupin**. Pro přesunutí skupiny nebo uživatele je přetáhněte ze stávajícího umístění do nového.

Poznámka

Přesunutý objekt bude dědit nastavená práva nové rodičovské skupiny, pokud nejsou žádná jiné práva přidělena přímo k danému objektu.

Mazání Skupin

Skupina nemůže být odstraněna, pokud obsahuje alespoň jednoho uživatele. Přesuňte všechny uživatele ze skupiny, kterou chcete odstranit, do jiné skupiny. Pokud skupina obsahuje podskupiny, můžete místo přesouvání jednotlivých uživatelů hýbat s celými skupinami.

Pro smazání skupiny:

1. Zvolte prázdnou skupinu.
2. Klikněte na tlačítko **Odstranit skupinu** v horní části levého panelu. Je nutné potvrdit kliknutím na **Ano**.

6.4.4. Kontrolování Stavu mobilních zařízení

Každé mobilní zařízení je na stránce sítí reprezentováno ikonou specifickou pro jeho typ a stav.

Seznam všech dostupných ikon a stavů naleznete na „Typy a stavy síťových souborů“ (str. 564).

Mobilní zařízení mohou být v následujících stavech správy:

- **Spravované (Aktivní)**, když jsou naplněny všechny tyto podmínky:
  - Na zařízení je aktivovaný GravityZone Mobile Client.
  - GravityZone Mobile Client byl během posledních 48 hodin synchronizován s Control Center.
- **Spravované (Nečinné)**, když jsou naplněny všechny tyto podmínky:
  - Na zařízení je aktivovaný GravityZone Mobile Client.
  - GravityZone Mobile Client se během posledních 48 hodin nesynchronizoval s Control Center.
- **Nespravované**, v těchto situacích:
  - Na mobilním zařízení ještě nebyl nainstalován a aktivován GravityZone Mobile Client.
  - Ze zařízení byl odinstalován GravityZone Mobile Client (pouze pro zařízení Android).
  - Ze zařízení byl odstraněn profil Bitdefender MDM (pouze pro zařízení iOS).

Pro kontrolu stavu správy zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. V levém panelu vyberte požadovanou skupinu.
4. Klikněte na nabídku **Filtry** umístěnou v horní části tabulky a nastavte následující parametry:
   a. Přejděte na kartu **Zobrazení** a vyberte **Zařízení**.
   b. Přejděte na kartu **Zabezpečení** a vyberte požadovaný stav v sekci **Správa**. Můžete zvolit jedno, nebo více kritérií pro filtrování najednou.
   c. Můžete si také zvolit zobrazení všech zařízení rekurzivně tak, že zvolíte příslušnou volbu z karty **Hloubka**.
   d. Klikněte na tlačítko **Save**.

      V tabulce budou zobrazena všechna zařízení, která odpovídají zvoleným kritériím.

Můžete také vytvořit hlášení o stavu Synchronizace zařízení pro jedno nebo několik mobilních zařízení. Toto hlášení poskytuje podrobné informace ohledně stavu synchronizace každého zvoleného zařízení, včetně data a času poslední synchronizace. Další informace viz „Tvorba Rychlých hlášení“ (str. 182)

6.4.5. Vyhovující a nevyhovující Mobilní zařízení

Jakmile je na mobilním zařízení aktivována aplikace GravityZone Mobile Client, Control Center zkontroluje, zda dané zařízení vyhovuje všem podmínkám pro soulad. Mobilní zařízení mohou být v následujících stavech zabezpečení:

- **Bez bezpečnostních problémů**, když jsou naplněny všechny podmínky pro soulad.
- **S bezpečnostními problémy**, když je alespoň jedna z podmínek souladu nenaplněna. Když je zařízení prohlášeno za nevyhovující, uživatel je vyzván k nápravě problému, který působí nesoulad. Uživatel musí provést požadované změny během určité doby, nebo bude uplatněna akce pro nevyhovující zařízení určená v pravidle.

  Pro více informací ohledně akcí pro nesoulad a kritérií se podívejte na „Soulad“ (str. 386).

Pro kontrolu stavu souladu zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. V levém panelu vyberte požadovanou skupinu.
4. Klikněte na nabídku **Filtry** umístěnou v horní části tabulky a nastavte následující parametry:
   a. Přejděte na kartu **Zobrazení** a vyberte **Zařízení**.
   b. Přejděte na kartu **Zabezpečení**a vyberte požadovaný stav v sekci **Bezpečnostní problémy**. Můžete zvolit jedno, nebo více kritérií pro filtrování najednou.
   c. Můžete si také zvolit zobrazení všech zařízení rekurzivně tak, že zvolíte příslušnou volbu z karty **Hloubka**.
   d. Klikněte na tlačítko **Save**.

      V tabulce budou zobrazena všechna zařízení, která odpovídají zvoleným kritériím.

5. Uvidíte poměr souladu zařízení pro každého uživatele:
   a. Klikněte na nabídku **Filtry** v horní části tabulky a v kategorii **Zobrazení** vyberte **Uživatelé**. V tabulce se zobrazí všichni uživatelé z vybrané skupiny.
   b. Podívejte se na sloupec **Soulad** a prohlédněte si, kolik zařízení je v souladu z celkového počtu zařízení, která uživatel vlastní.

Můžete také vytvořit hlášení o Souladu zařízení na jednom nebo několika mobilních zařízeních. Toto hlášení poskytuje podrobné informace ohledně stavu souladu každého zvoleného zařízení, včetně důvodu pro nesoulad. Další informace viz „Tvorba Rychlých hlášení“ (str. 182)

6.4.6. Kontrolování podrobností o uživateli a mobilních zařízeních

Podrobné informace o každém uživateli a mobilním zařízení naleznete na stránce **Síť**.

Kontrolování detailů uživatele

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte požadovanou skupinu v levém panelu.
4. Klikněte na nabídku **Filtry** umístěnou v horní části tabulky, přejděte na **Zobrazení** a vyberte **Uživatelé**. Pro zobrazení uživatelů rekurzivně, přejděte na kartu **Hloubka** a vyberte **Všechny položky rekurzivně**. Klikněte na tlačítko **Save**. V tabulce se zobrazí všichni uživatelé z vybrané skupiny.
5. Zkontrolujte informace zobrazené ve sloupcích pro každého uživatele:
   - **Jméno**. Uživatelské jméno.
   - **Zařízení**. Počet zařízení připojených k uživateli. Klikněte na číslo pro přepnutí se na zobrazení **Zařízení** a prohlížejte pouze odpovídající zařízení.
   - **Soulad**. Poměr vyhovujících zařízení ku celkovému počtu zařízení vlastněných uživatelem. Klikněte na první hodnotu pro pro přepnutí se na zobrazení **Zařízení** a prohlížení pouze vyhovující zařízení.
6. Klikněte na jméno požadovaného uživatele. Zobrazí se konfigurační okno, ve kterém můžete prohlížet a upravovat uživatelské jméno a emailovou adresu.

Kontrolování detailů zařízení

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte požadovanou skupinu v levém panelu.
4. Klikněte na nabídku **Filtry** umístěnou v horní části tabulky, přejděte na **Zobrazení** a vyberte **Zařízení**. Klikněte na tlačítko **Save**. V tabulce jsou zobrazena všechna zařízení, která patří uživatelům vybrané skupiny.
5. Zkontrolujte informace zobrazené ve sloupcích tabulky pro každé zařízení:
   - **Jméno**. Název zařízení.
   - **Uživatel**. Jméno uživatele, který vlastní příslušné zařízení.
   - **OS**. Operační systém daného zařízení.
6. Pro více podrobností klikněte na název zařízení. Zobrazí se okno **Detaily mobilního zařízení**, ve kterém můžete prohlížet následující informace, seskupené po kartami **Přehled** a **Detaily**:
   - **Obecné**.
     - **Jméno**. Název určený při přidávání zařízení do Control Center.
     - **Uživatel**. Jméno vlastníka zařízení.
     - **Skupina**. Rodičovská skupina mobilního zařízení v síťovém inventáři.
     - **OS**. Operační systém mobilního zařízení.
     - **Vlastnictví**. Typ vlastnictví mobilního zařízení (podnikové nebo osobní).
   - **Zabezpečení**.
     - **Verze klienta**. Verze aplikace GravityZone Mobile Client nainstalované na zařízení, zjištěná až po registraci.
     - **Práva**. Pravidlo aktuálně přiřazené k mobilnímu zařízení. Klikněte na jméno pravidla pro přejití na odpovídající stránku **Pravidla** a zkontrolujte bezpečnostní nastavení.

       Důležité

       Ve výchozím nastavení může pravidla upravovat pouze uživatel, který je vytvořil. Pro změnu tohoto nastavení musí autor pravidla označit možnost **Povolit ostatním uživatelům měnit toto pravidlo** ze stránky **Podrobnosti**

pravidla. Změny provedené v pravidle budou platné pro všechna zařízení, ke kterým je dané pravidlo přiřazeno. Další informace viz „Přiřazování pravidel“ (str. 183).

- **Stav licence**. Zobrazíte informace o licenci pro dané zařízení.
- **Stav souladu**. Stav souladu je k dispozici pro spravovaná mobilní zařízení. Mobilní zařízení může být Vyhovující nebo Nevyhovující.

  Poznámka
  Pro nevyhovující zařízení se zobrazí výstražná ikona ! . Podívejte se na nápovědu ikony pro zobrazení důvodu nesouladu.
  Pro více podrobností ohledně souladu mobilních zařízení se podívejte na „Soulad“ (str. 386).

- **Malwarová činnost (posledních 24h)**. Rychlý přehled počtu malwarových detekcí pro příslušné zařízení za aktuální den.
- **Heslo zámku**. Unikátní heslo, automaticky generované při registraci zařízení, které je využíváno při uzamknutí zařízení na dálku (pouze pro zařízení Android).
- **Stav šifrování**. Některá zařízení s Android 3.0 a novějším podporují funkci šifrování zařízení. Abyste zjistili, zda dané zařízení podporuje funkci šifrování, zkontrolujte stav šifrování na stránce s detaily o zařízení. Pokud je šifrování vyžadováno pravidlem na zařízení, můžete prohlížet také stav aktivace šifrování.

- **Detaily aktivace**
  - **Aktivační kód**. Unikátní aktivační token přiřazený k zařízení.
  - Adresa komunikačního serveru.
  - **QR kód**. Unikátní QR kód obsahující aktivační token a adresu komunikačního serveru.
- **Hardware**. Zde můžete prohlížet informace o hardwaru zařízení, dostupné pouze pro spravovaná (aktivovaná) zařízení. Informace o hardwaru je kontrolována každých 12 hodin a aktualizována, když dojde ke změnám.

Důležité
Počínaje systémem Android 10 nemá GravityZone Mobile Client přístup k sériovému číslu, IMEI, IMSI a MAC adrese zařízení. Toto omezení vede k následujícím situacím:
- Pokud mobilní zařízení, které již má nainstalován GravityZone Mobile Client, upgraduje ze starší verze systému Android na Android 10, zobrazí Control Center správné podrobnosti o zařízení. Před upgradem musí zařízení spustit nejnovější verzi aplikace GravityZone Mobile Client.
- Pokud se aplikace GravityZone Mobile Client nainstaluje na zařízení se systémem Android 10, Control Center zobrazí nepřesné podrobnosti o tomto zařízení z důvodu omezení uloženého operačním systémem.

- **Síť**. Zde můžete prohlížet informace připojení k síti, dostupné pouze pro spravovaná (aktivovaná) zařízení.

6.4.7. Třídění, Filtrování a Hledání Mobilních zařízení

Tabulka inventáře mobilních zařízení může zabrat několik stránek, podle počtu uživatelů nebo zařízení (ve výchozím stavu se zobrazuje 10 položek na stránku). Pro pohyb mezi stránkami použijte navigační tlačítka ve spodní části tabulky. Můžete změnit počet položek zobrazených na stránku tak, že vyberete nějakou z menu umístěného vedle navigačních tlačítek.

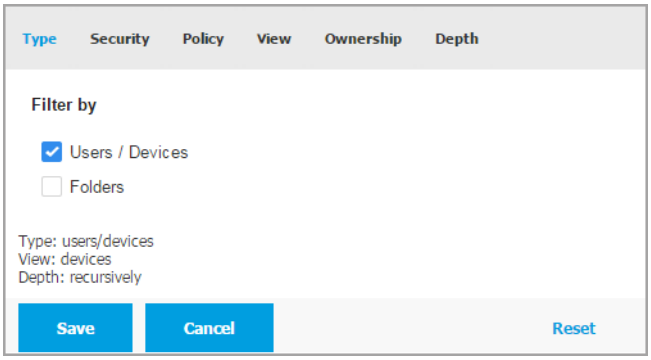
Pokud se zobrazuje moc velký počet položek, můžete použít možnosti filtrování a zobrazit pouze položky, které vás zajímají. Například, můžete vyhledat určité mobilní zařízení nebo zobrazit pouze spravovaná mobilní zařízení.

Třídění Inventáře mobilních zařízení

Pro třídění dat podle určitého sloupce, klikněte na hlavičku slupce. Například, pokud chcete mobilní zařízení seřadit podle jména, klikněte na hlavičku **Název**. Pokud kliknete na hlavičku znovu, mobilní zařízení budou zobrazena v opačném pořadí.

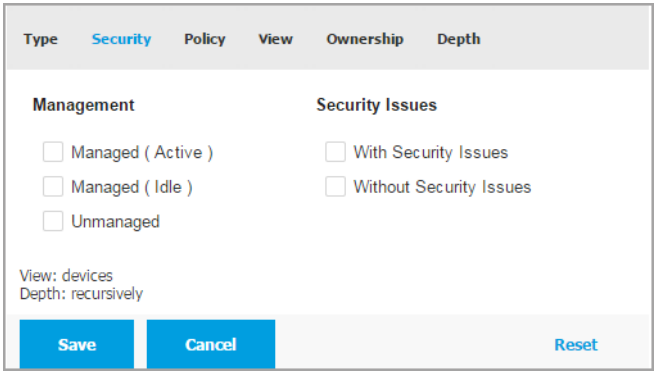
Filtrování Inventáře mobilních zařízení

1. Vyberte skupinu v levém panelu.
2. Klikněte na menu **Filtry** navrchu od oblasti panelů sítě.
3. Použijte následující filtrovací kriteria:
   - **Typ**. Vyberte typ objektů, které chcete zobrazit (Uživatelé/Zařízení a složky).



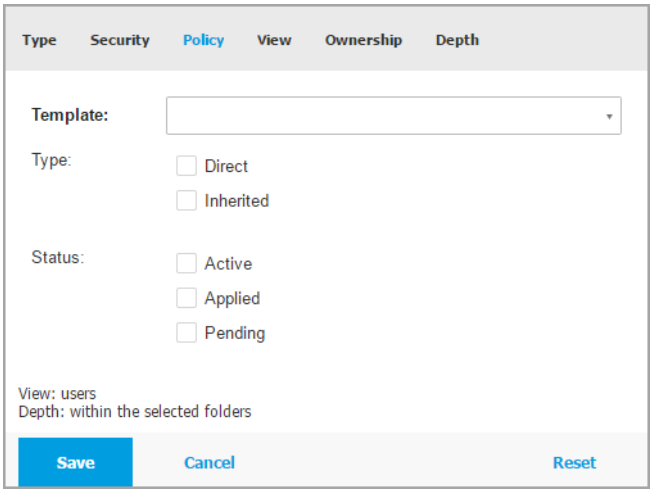
Mobilní zařízení - Filtrovat podle typu

- **Zabezpečení**. Počítače můžete zobrazit podle stavu správy a zabezpečení.



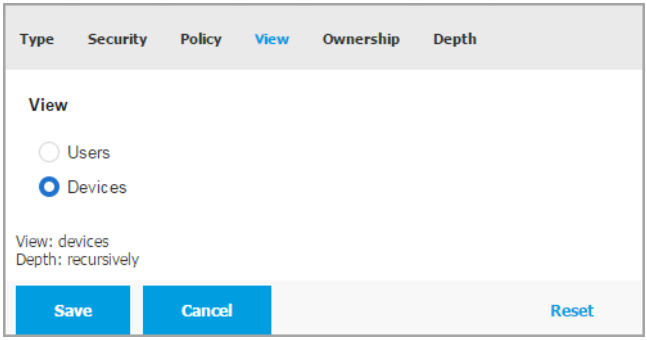
Mobilní zařízení - Filtrovat podle zabezpečení

- **Práva**. Vyberte předlohu práv, podle toho která mobilní zařízení chcete filtrovat, práva která byla přidělena (Přímo nebo Zděděná), a samozřejmě přiřazený status (Aktivní, Aplikován nebo Čekající).



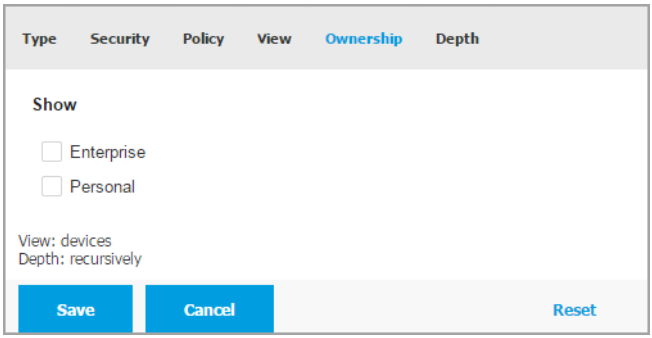
Mobilní zařízení - Filtrovat podle pravidla

- **Zobrazení**. Vyberte **Uživatelé** pro zobrazení pouze uživatelů v rámci zvolené skupiny. Vyberte **Zařízení** pro zobrazení pouze zařízení v rámci zvolené skupiny.



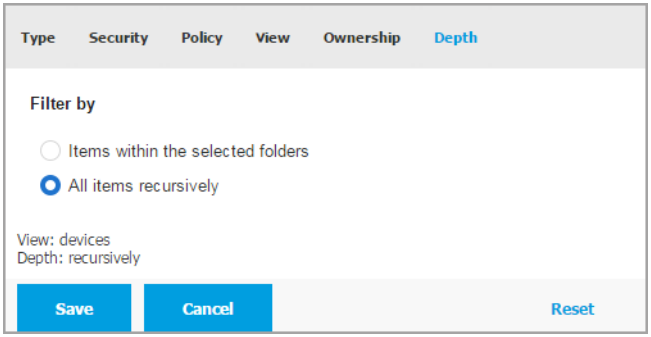
Mobilní zařízení - Filtrovat podle zobrazení

- **Vlastnictví**. Mobilní zařízení můžete filtrovat podle vlastnictví a zvolit buď zobrazení **Podnikových** zařízení, nebo **Osobních** zařízení. Charakteristika vlastnictví je určena v detailech mobilního zařízení.



Mobilní zařízení - Filtrovat podle vlastnictví

- **Struktura**. Při spravování stromové struktury sítě, mobilní zařízení nebo uživatelé umístění do podskupin se při výběru hlavní skupiny nezobrazí. Pro zobrazení všech objektů v aktuální skupině a všech jejích podskupinách vyberte **Všechny objekty opakovaně**.



Mobilní zařízení - Filtrovat podle hloubky

4. Klikněte na **Uložit** pro filtrování mobilních zařízení podle zvolených kritérií.
   Filtr zůstává aktivní v záložce **Síť** dokud se neodhlásíte nebo neresetujete filtr.

Vyhledávání mobilních zařízení

Tabulka na pravém panelu poskytuje specifické informace o uživatelích a mobilních zařízeních. Obsah tabulky můžete filtrovat pomocí kategorií dostupných v každém sloupci.

1. Vyberte požadovanou skupinu v levém panelu.
2. Přepněte na požadované zobrazení (Uživatelé nebo Mobilní zařízení) pomocí nabídky **Filtry** v horní části oblasti síťových tabulek.
3. Vyhledávejte požadované objekty pomocí vyhledávacích polí pod hlavičkou každého sloupce na pravém panelu:
   - Zadejte požadovaný termín vyhledávání do příslušného vyhledávacího pole.

     Například přepněte na zobrazení **Zařízení** a zadejte jméno hledaného uživatele do pole **Uživatel**. V tabulce se zobrazí pouze odpovídající mobilní zařízení.
   - Vyberte vlastnost, kterou chcete hledat, v příslušných polích s rozbalovacím seznamem.

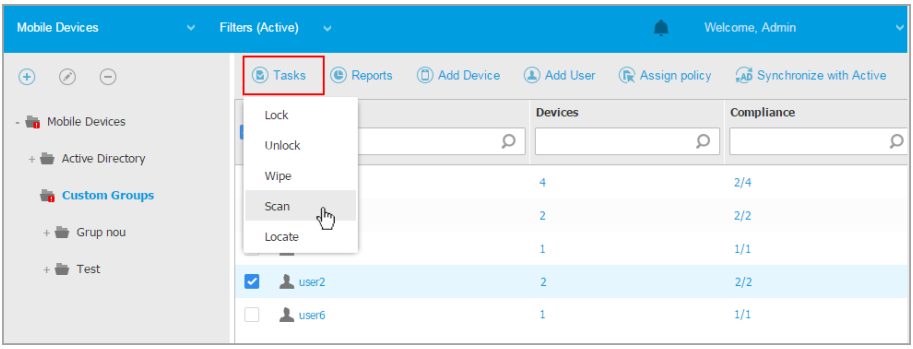
     Například, přepněte na zobrazení **Zařízení**, klikněte na pole seznamu **OS** a zvolte **Android** pro zobrazení pouze mobilních zařízení s Android.

> **Poznámka**
> Pro smazání vyhledávaného termínu a zobrazení všech položek ukažte kurzorem myši na příslušné pole a klikněte na ikonu ×.

6.4.8. Spouštění úloh na mobilních zařízeních

Ze stránky **Síť** můžete na mobilních zařízeních na dálku spouštět několik administrativních úloh. Můžete provádět následující akce:

- „Uzamčení“ (str. 178)
- „Vymazání“ (str. 179)
- „Sken“ (str. 180)
- „Lokalizace“ (str. 181)



Úlohy na mobilních zařízeních

Pro možnost spouštění vzdálených úloh na mobilních zařízeních musí být naplněny určité předpoklady. Pro více informací se odkažte na kapitolu Požadavky pro instalaci v Průvodci instalací GravityZone.

Můžete si vybrat vytváření úloh individuálně pro každé mobilní zařízení, každého uživatele, nebo pro skupiny uživatelů. Například, můžete vzdáleně skenovat pro malware na mobilních zařízeních ve skupině uživatelů. Můžete také spustit úlohu pro lokalizaci konkrétního mobilního zařízení.

Síťový inventář může obsahovat aktivní, nečinná nebo nespravovaná mobilní zařízení. Jakmile jsou vytvořeny, úlohy se spustí automaticky na všech aktivních mobilních zařízeních. Na nečinných zařízeních budou úlohy zahájeny, jakmile bude zařízení znovu online. Pro nespravovaná mobilní zařízení nelze vytvářet úlohy. V tomto případě se zobrazí upozornění s tím, že úloha nemohla být vytvořena.

Úlohy můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Uzamčení

Úloha Uzamknout okamžitě zamkne obrazovku cílených mobilních zařízení. Chování úlohy Uzamknout je závisí na operačním systému:

- Úloha Uzamknout pro zařízení Android (7.0 a novější) prosadí heslo nastavené ve vaší konzoli GravityZone pouze v případě, že na zařízená není nastavena žádná ochrana pomocí zámku. V opačném případě budou jako ochrana zařízení použita současná nastavení zámku obrazovky, jako je vzor, PIN, heslo, otisk prstu nebo Smart Lock.

Poznámka

- Heslo zámku obrazovky vygenerované v Control Center je zobrazeno v okně Detaily mobilního zařízení.
- Úloha Odemknout je již nedostupná pro zařízení s Android (7.0 a novější). Místo toho mohou uživatelé zařízení odemknout ručně. Musíte se však předem ujistit, že tato zařízení podporují očekávané požadavky na složitost hesla pro odemčení.
- Z důvodu technických omezení není úloha zámku v systému Android 11 k dispozici.

- Na iOS, pokud má zařízení nastavený zámek obrazovky, je vyžadován pro jeho odemčení.

Pro vzdálené uzamčení mobilních zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte skupinu, kterou chcete z levého panelu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Uživatelé**. Klikněte na tlačítko **Save**. V tabulce se zobrazí všichni uživatelé z vybrané skupiny.
5. Označte zaškrtávací pole odpovídající požadovaným uživatelům. Můžete vybrat jednoho nebo několik uživatelů najednou.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Uzamknout**.
7. Je nutné potvrdit kliknutím na **Ano**. Zpráva vás informuje, zda úloha byla či nebyla vytvořena.
8. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Vymazání

Úloha **Vymazání** obnoví cílená mobilní zařízení do továrního nastavení. Spusťte tuto úlohu pro vzdálené vymazání všech citlivých informací a aplikací uložených na cílených mobilních zařízeních.

Varování

Úlohu **Vymazání** používejte s rozvahou. Zkontrolujte vlastnictví cílených zařízení (pokud se chcete vyhnout smazání mobilních zařízení v osobním vlastnictví) a ujistěte se, že skutečně chcete vymazat obsah zvolených zařízení. Jakmile je odeslána, úloha **Wipe** nemůže být přerušena.

Poznámka

Z důvodu technických omezení není úloha Vymazat v systému Android 11 k dispozici.

Pro vzdálené vymazání mobilního zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte skupinu, kterou chcete z levého panelu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**. Klikněte na tlačítko **Save**. V tabulce se zobrazí všechna zařízení z vybrané skupiny.

   Poznámka

   V sekci **Hloubka** můžete také zvolit **Všechny položky rekurzivně** pro zobrazení všech zařízení v dané skupině.

5. Označte zaškrtávací pole odpovídající zařízení, jehož obsah chcete vymazat.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Vymazat**.
7. Je nutné potvrdit kliknutím na **Ano**. Zpráva vás informuje, zda úloha byla či nebyla vytvořena.
8. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

Sken

Úloha **Skenování** vám umožňuje zkontrolovat přítomnost malwaru na zvolených zařízeních. Uživatel zařízení je upozorněn na jakýkoli zjištěný malware a je vyzván k jeho odstranění. Skenování probíhá v cloudu, proto musí být zařízení připojené k internetu.

Poznámka

Skenování na dálku nefunguje na zařízeních s iOS (omezení platformy)

Pro vzdálené skenování mobilních zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte skupinu, kterou chcete z levého panelu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**. Klikněte na tlačítko **Save**. V tabulce se zobrazí všechna zařízení z vybrané skupiny.

   Poznámka
   V sekci **Hloubka** můžete také zvolit **Všechny položky rekurzivně** pro zobrazení všech zařízení v dané skupině.
   Pro zobrazení pouze zařízení Android v rámci zvolené skupiny, přejděte k hlavičce sloupce **OS** v pravém panelu, a z příslušného seznamu vyberte **Android**.

5. Označte zaškrtávací pole odpovídající zařízením, která chcete skenovat.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Sken**.
7. Je nutné potvrdit kliknutím na **Ano**. Zpráva vás informuje, zda úloha byla či nebyla vytvořena.
8. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Výpis ze skenování je k dispozici po dokončení úlohy. Klikněte na příslušnou ikonu ve sloupci **Hlášení** pro vytvoření okamžitého hlášení.

   Další informace viz „Prohlížení a správa úloh“ (str. 200).

Lokalizace

Úloha Lokalizovat otevře mapu, na které jsou vyznačena zvolená zařízení. Můžete lokalizovat jedno nebo více zařízení najednou.

Aby úloha Lokalizace mohla pracovat, na mobilních zařízeních musí být povoleny lokalizační služby.

Pro lokalizaci mobilních zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte skupinu, kterou chcete z levého panelu.

4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**. Klikněte na tlačítko **Save**. V tabulce se zobrazí všechna zařízení z vybrané skupiny.

   Poznámka
   V sekci **Hloubka** můžete také zvolit **Všechny položky rekurzivně** pro zobrazení všech zařízení v dané skupině.

5. Označte zaškrtávací pole odpovídající zařízení, které chcete lokalizovat.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Lokalizovat**.
7. Otevře se okno **Umístění** s následujícími informacemi:
   - Mapa, která ukazuje polohu zvolených mobilních zařízení. Pokud zařízení není synchronizováno, mapa ho zobrazí v jeho naposledy známém umístění.
   - Tabulka s detaily o vybraných zařízeních (název, uživatel, datum a čas poslední synchronizace). Pro zobrazení umístění na mapě pro konkrétní zařízení z tabulky stačí označit jeho zaškrtávací pole. Mapa bude okamžitě zaměřena na umístění daného zaměření.
   - Možnost **Automatické obnovování** automaticky aktualizuje umístění vybraných mobilních zařízení každých 10 sekund.
8. Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**. Další informace viz „Prohlížení a správa úloh“ (str. 200).

6.4.9. Tvorba Rychlých hlášení

Můžete vytvářet okamžitá hlášení pro mobilní zařízení, počínaje ze stránky **Síť**.

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyberte požadovanou skupinu v levém panelu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**. Můžete také zvolit Spravované možnosti z karty **Zabezpečení** pro filtrování zvolené skupiny pouze podle spravovaných zařízení. Klikněte na tlačítko **Save**. V tabulce se zobrazí všechna zařízení odpovídající kritériím filtrování ze zvolené skupiny.

5. Označte pole odpovídající mobilním zařízením, která vás zajímají. Můžete vybrat jedno nebo více zařízení najednou.
6. Klikněte na tlačítko **Hlášení** v horní části tabulky a z nabídky zvolte typ hlášení. Další informace viz „Hlášení o mobilních zařízeních“ (str. 495)
7. Nastavte parametry hlášení. Další informace viz „Vytváření hlášení“ (str. 497)
8. Klikněte na tlačítko **Vytvořit**. Hlášení se okamžitě zobrazí. Čas potřebný k vytvoření hlášení se může lišit podle počtu zvolených mobilních zařízení.

6.4.10. Přiřazování pravidel

Bezpečnostní nastavení na mobilních zařízeních můžete spravovat prostřednictvím pravidel.

V sekci **Síť** můžete prohlížet, měnit a přiřazovat pravidla pro mobilní zařízení patřící pod váš účet.

Můžete přiřazovat pravidla ke skupinám, uživatelům nebo konkrétním mobilním zařízením.

Poznámka

Pravidlo přiřazené k uživateli platí pro všechna zařízení, která daný uživatel vlastní. Další informace viz „Přiřazování Politik Lokálně“ (str. 215).

Pro zobrazení bezpečnostních nastavení přiřazených k zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**. Klikněte na tlačítko **Save**. V tabulce jsou zobrazena všechna zařízení, která patří uživatelům vybrané skupiny.
4. Klikněte na jméno požadovaného mobilního zařízení. Objeví se okno s podrobnostmi.
5. V sekci **Zabezpečení** na stránce **Přehled** klikněte na název momentálně přiřazeného pravidla pro zobrazení jeho nastavení.
6. Bezpečnostní nastavení můžete měnit dle potřeby. Mějte prosím na paměti, že každá provedená změna bude platit také na všech ostatních zařízeních, pro která je pravidlo aktivní.

Další informace viz „Politiky Mobilních Zařízení“ (str. 381)

Pro přiřazení pravidla k mobilnímu zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. V levém panelu vyberte požadovanou skupinu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**. Klikněte na tlačítko **Save**. V tabulce jsou zobrazena všechna zařízení, která patří uživatelům vybrané skupiny.
5. V pravém panelu označte zaškrtávací pole požadovaného mobilního zařízení.
6. Klikněte na tlačítko **Přiřadit pravidlo** v horní části tabulky.
7. Proveďte potřebná nastavení v okně **Přiřazení pravidel**. Další informace viz „Přiřazování Politik Lokálně“ (str. 215).

6.4.11. Synchronizace s Active Directory

Síťový inventář se automaticky synchronizuje s Active Directory podle časového intervalu určeném v konfigurační sekci Control Center. Pro více informací se odkažte na kapitolu Instalace a Nastavení GravityZone v Průvodci instalací GravityZone.

Pro ruční synchronizaci aktuálně zobrazených uživatelů s Active Directory:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Klikněte na tlačítko **Synchronizovat s Active Directory** v horní části tabulky.
4. Je nutné potvrdit kliknutím na **Ano**.

Poznámka

V rozsáhlých sítích Active Directory může dokončení synchronizace trvat déle.

6.4.12. Mazání uživatelů a mobilních zařízení

Pokud síťový inventář zahrnuje zastaralé uživatele nebo mobilní zařízení, doporučujeme je odstranit.

Mazání mobilních zařízení ze Síťového inventáře

Když smažete zařízení z Control Center:

- GravityZone Mobile Client je odpojen, ale není odstraněn ze zařízení.
- Pro zařízení iOS je odstraněn profil MDM. Pokud zařízení není připojeno k internetu, profil MDM zůstane nainstalovaný tak dlouho, dokud není nové připojení k dispozici.
- Všechny výpisy týkající se odstraněného zařízení jsou stále dostupné.
- Vaše osobní informace a aplikace nejsou nijak ovlivněny.

Varování

- Smazaná mobilní zařízení není možné obnovit.
- Pokud omylem odstraníte uzamčené zařízení, musíte ho pro jeho odemčení obnovit do továrního nastavení.

Pro odstranění mobilního zařízení:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. V levém panelu vyberte požadovanou skupinu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Zařízení**.
5. Klikněte na tlačítko **Save**.
6. Označte zaškrtávací pole odpovídající zařízením, která chcete odstranit.
7. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

Mazání uživatelů ze Síťového inventáře

Uživatele, kteří jsou aktuálně připojeni k mobilním zařízením nelze odstranit. Nejdřív musíte odstranit příslušná mobilní zařízení.

Poznámka
Můžete mazat pouze uživatele z Vlastních skupin.

Pro odstranění uživatele:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. V levém panelu vyberte požadovanou skupinu.
4. Klikněte na nabídku **Filtry** v horní části oblasti síťových panelů a v kategorii **Zobrazení** vyberte **Uživatelé**.
5. Klikněte na tlačítko **Save**.
6. Označte zaškrtávací pole odpovídající uživateli, kterého chcete odstranit.
7. Klikněte na tlačítko ⊖ **Smazat** na pravé straně tabulky. Je nutné potvrdit kliknutím na **Ano**.

6.5. Inventář aplikací

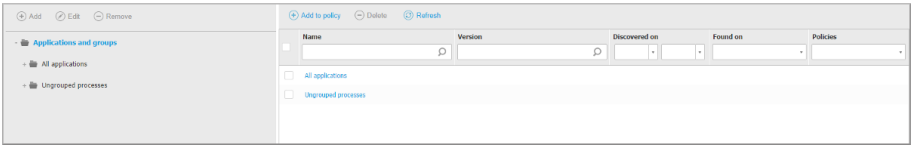
Můžete prohlížet všechny aplikace nalezené ve vaší síti pomocí úlohy **Vyhledání aplikací** v sekci **Aplikace a skupiny**. Další informace viz „Vyhledání aplikací“ (str. 99).

Aplikace a procesy jsou automaticky přidávány do složky **Aplikace a skupiny** na levém panelu.

Aplikace a procesy můžete řadit do vlastních skupin.

Všechny aplikace/procesy ze zvolené složky budou zobrazeny v tabulce na pravém panelu. Můžete vyhledávat podle názvu, verze, vydavatele/autora, zdroj aktualizací, umístění a pravidel.

Pro zobrazení těch nejnovějších informací v tabulce klikněte na tlačítko ⟳ **Obnovit** v horní části tabulky. Toto může být potřeba, když na stránce strávíte více času.



Inventář aplikací

Důležité

Aplikace, nově objevené při každém spuštění úlohy **Vyhledání aplikací**, jsou automaticky umisťovány do složky **Nezařazené aplikace**. Procesy, které nepatří ke konkrétním aplikacím, budou umístěny do složky **Nezařazené procesy**.

Strom aplikací a skupin

Pro přidání vlastní skupiny do stromu **Aplikací a skupin**:

1. Vyberte složku **Všechny aplikace**.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části stromu.
3. V novém okně zadejte název.
4. Klikněte na **OK** pro vytvoření nové skupiny.
5. Vyberte složku **Nezařazené aplikace**. Všechny aplikace seskupené pod zvolenou složkou jsou zobrazeny v pravém panelu.
6. Vyberte požadované aplikace z tabulky na pravém panelu. Pro přesunutí do požadované vlastní složky na levém panelu, přetáhněte zvolené položky z pravého panelu.

Pro přidání vlastní aplikace:

1. Vyberte cílovou složku pod **Všechny aplikace**.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části stromu.
3. V novém okně zadejte název.
4. Klikněte na **OK** pro vytvoření vlastní aplikace.
5. Můžete přidávat procesy patřící k nové vlastní aplikaci ze složky **Nezařazené procesy** nebo z ostatních složek zobrazených ve stromu **Aplikace a skupiny**. Po zvolení složky se všechny procesy zobrazí v tabulce na pravém panelu.
6. Vyberte požadované procesy z tabulky na pravém panelu. Pro přesunutí požadovaných položek do vlastní aplikace je přetáhněte do levého panelu.

Poznámka
Aplikace může být součástí pouze jedné skupiny.

Pro přejmenování složky nebo aplikace:

1. Vyberte je ve stromu **Aplikace a skupiny**.
2. Klikněte na tlačítko ✎ **Upravit** v horní části stromu.
3. Změňte jméno, které potřebujete.
4. Klikněte **OK**.

Můžete libovolně přesouvat skupiny a aplikace kamkoliv rámci hierarchie **Aplikací a skupin**. Pro přesunutí skupiny nebo aplikace je přetáhněte ze stávajícího umístění do nového.

Pro odstranění vlastní skupiny nebo aplikace ji vyberte ve stromu **Aplikace a skupiny** a poté klikněte na tlačítko ⊖ **Odstranit** v horní části stromu.

Přidávání aplikací k pravidlům

Pro přidání aplikace nebo procesu k pravidlu přímo z Inventáře aplikací:

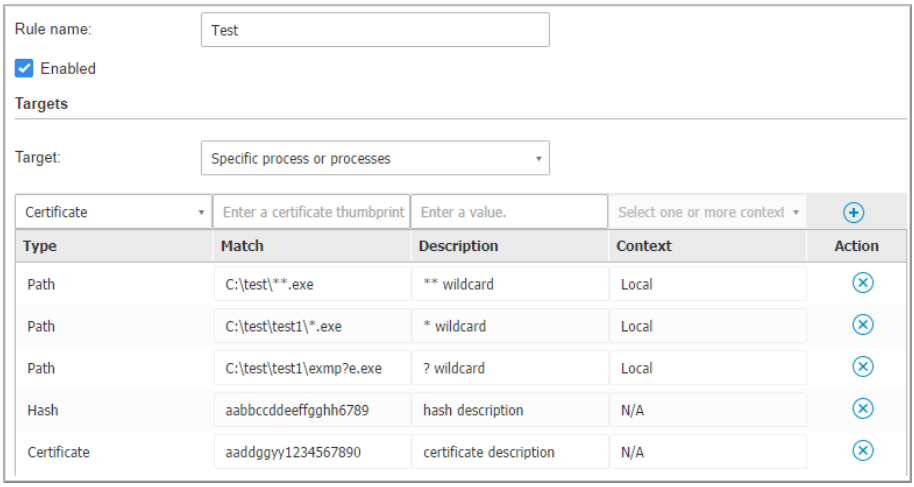
1. Vyberte požadovanou složku ze stromu **Aplikace a skupiny**. Obsah složky je zobrazen na pravém panelu.
2. Vyberte požadované procesy nebo aplikace z pravého panelu.
3. Klikněte na tlačítko ⊕ **Přidat k pravidlu** pro otevření konfiguračního okna.
4. V sekci **Přidat pravidlo k těmto zásadám** zadejte jméno existující zásady. Použijte vyhledávací pole pro vyhledávání podle jména zásady nebo uživatele.
5. V sekci **Detaily pravidla** zadejte **Název pravidla**.
6. Označte zaškrtávací políčko **Povoleno** pro aktivaci pravidla.
7. Typ cíle je automaticky rozpoznán. Pokud je třeba, upravte současná kritéria:
   - **Konkrétní proces nebo procesy**, pro určení procesu, kterému je povoleno nebo zakázáno spuštění. Můžete autorizovat pomocí cesty, hashe nebo certifikátu. Podmínky uvnitř pravidel jsou spojovány pomocí logických AND.
     – Pro autorizování aplikace z určité cesty:
       a. Vyberte **Path** ve sloupci **Type**. Specifikujte cestu k objektu. Můžete poskytnout absolutní nebo relativní cestu a používat speciální znaky. Symbol hvězdičky (*) spojí všechny soubory v rámci adresáře. Dvě hvězdičky (**) spojí všechny soubory a adresáře v definovaném adresáři. Otazník (?) zastupuje přesně jeden znak. Můžete také přidat vysvětlení pro zjednodušení identifikování procesu.
       b. Z rozbalovací nabídky **Select one or more contexts** můžete vybrat mezi lokálním, CD-ROM, odpojitelné nebo síť. Můžete zablokovat spuštění aplikace z odnímatelných zařízení nebo je povolit pokud je aplikace lokálně spuštěna.

– Pro autorizování aplikace na základě hashe, vyberte **Hash** ve sloupci **Type** a zadejte hashovou hodnotu. Můžete také přidat vysvětlení pro zjednodušení identifikování procesu.

> **Důležité**
> Pro vygenerování hashové hodnoty, stáhněte nástroj Fingerprint. Další informace viz „Nástroje Kontroly aplikací“ (str. 569)

– Pro autorizování na základě certifikátu, vyberte **Certificate** ze sloupce **Type** a zadejte thumbprint certifikátu. Můžete také přidat vysvětlení pro zjednodušení identifikování procesu.

> **Důležité**
> Pro získání thumbprint certifikátu, stáhněte nástroj Thumbprint. Další informace viz „Nástroje Kontroly aplikací“ (str. 569)



Pravidla aplikací

Klikněte na ⊕ **Add** pro přidání pravidla. Nově přidaná pravidla budou mít nejvyšší prioritu v této politice.

- **Inventory applications or groups**, pro přidání skupiny nebo nějaké aplikace objevené v síti. Můžete zobrazit aplikace běžící ve vaší síti v záložce **Network > Application Invertory**.

  Vlože aplikace nebo názvy skupin do pole, odděleně pomocí čárky. Funkce automatické vyplnění zobrazuje návrhy podle toho jak píšete.

8. Vyberte zaškrtávací pole **Include subprocesses** pro aplikování pravidla pro spuštěné podprocesy.

   Varování
   Při nastavování pravidel pro aplikace prohlížečů, doporučujeme tuto možnost vypnout, pro předejití bezpečnostních rizik.

9. Optimálně, můžete také definovat výjimky z pravidla procesu start. Operace přidání je podobná jako jedné, která byla vysvětlena již předtím.
10. V sekci **Permissions**, vyberte zda bude povolená nebo zamezená pro spuštění.
11. Kliknutím na tlačítko **Uložit** aplikujete změny.

Pro smazání aplikace nebo procesu:

1. Vyberte požadovanou složku ze stromu **Aplikace a skupiny**.
2. Vyberte požadované procesy nebo aplikace z pravého panelu.
3. Klikněte na tlačítko **Odstranit**.

Zdroje Updatu

Musíte definovat zdroje updatu pro zobrazené aplikace ve vaší síti.

Varování
Pokud není přidělen žádný zdroj updatu, povolené aplikace se nebudou moci aktualizovat.

Přiřazení zdroje updatu:

1. Vyberte požadované složky ve stromu **Applications and groups**. Obsah složky je zobrazen v pravém panelu.
2. V pravém panelu, vyberte soubor, který chcete použít jako zdroj updatu.
3. Klikněte na tlačítko **Assign updaters**.

4. Klikněte na **Yes** pro potvrzení přiřazení. Zdroje updatu jsou označeny pomocí specifické ikony:

Zdroj updatu

Pro zamítnutí nějakého zdroje updatu:

1. Vyberte požadované složky ve stromu **Applications and groups**. Obsah složky je zobrazen v pravém panelu.
2. V pravém panelu, vyberte zdroj updatu, který chcete zamítnout.
3. Klikněte na tlačítko **Dismiss updater**.
4. Potvrďte kliknutím na **Ano**.

6.6. Inventář Balíčků

GravityZone najde záplaty které váš software potřebuje pomocí úlohy **Sken aktualizací a záplat (Patch Scan)** a následně je přidá do inventáře aktualizací a záplat.

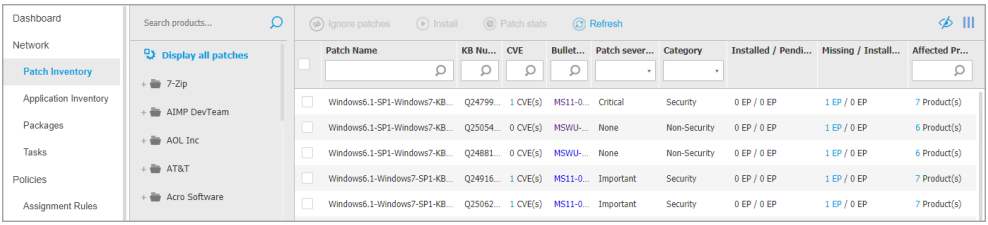
Stránka **Inventář aktualizací a záplat (Patch Inventory)** zobrazuje veškeré odhalené záplaty a aktualizace pro software , který je nainstalován na vašich koncových bodech a umožňuje provést různé akce s těmito zápatami , či aktualizacemi.

Použijte Inventář Balíčků vždy, když potřebujete okamžitě nasadit určité balíčky. Tato alternativa vám umožňuje jednoduché vyřešení některých problémů, o kterých víte. Například, četli jste nějaký článek o zranitelnosti softwaru a víte CVE ID. Můžete vyhledat v inventáři balíčky adresované k tomuto CVE a pak zobrazit, která koncová zařízení mohou být aktualizována.

Inventář Balíčků naleznete, kliknutím na možnost **Síť > Inventář Balíčků** v hlavním menu Control Center.

Stránka je uspořádána ve dvou panelech:

- Panel nalevo ukazuje instalované softwarové produkty ve vaší síti, seskupené podle prodejce.
- Panel napravo zobrazuje tabulku s dostupnými balíčky a detaily o nich.



Inventář Balíčků

Dále se naučíte jak využívat tento inventář. Můžete provádět následující akce:

- Detailni informace k záplatám a aktualizacím
- Vyhledávání a filtrování záplat či aktualizací
- Ignorovat balíčky
- Instalace záplat či aktualizací
- Odinstalace záplat či aktualizací
- Vytvoření statistik o záplatách a aktualizacích

6.6.1. Zobrazování Detailů o Balíčku

Tabulka záplaty a aktualizace obsahuje informace , které vám pomohou identifikovat záplaty a aktualizace, zjišťovat jejich důležitost, zobrazt si jejich stav a rozsah. Detaily jsou vysvětleny zde:

- **Název Balíčku.** Toto je název spustitelného souboru, obsahující balíček.
- **KB Číslo.** Toto číslo identifikuje články KB, které oznamují vydání balíčku.
- **CVE.** Toto je číslo CVE adresovaných k určitému balíčku. Kliknutím na číslo se zobrazí seznam CVE ID.
- **Bulletin ID.** Toto je ID bezpečnostního bulletin problému od prodejce. Toto ID propojuje aktuální článek, které popisuje balíček a poskytuje detaily instalace.
- **Důležitost Balíčku.** Toto hodnocení vás informuje o důležitosti balíčku vzhledem k poškození, kterému může zabránit.
- **Kategorie.** Na základě typu problému vyhodnotí, balíčky a skupiny ve dvou kategoriích: zabezpečené a nezabezpečené. Toto pole vás informuje, do které kategorie balíček patří.

- **Instalované / Čekající na instalaci.** Tato čísla ukazují, na kolika koncových bodech je balíček nainstalovaný, a kolik jich čeká na jeho instalaci. Čísla odkazují na seznam těchto koncových bodů.
- **Chybějící / Instalace se nezdařila.** Tato čísla ukazují, na kolika koncových bodech balíček není nainstalován, a na kolika instalace selhala. Čísla odkazují na seznam těchto koncových bodů.
- **Ovlivněné produkty.** Jde o počet produktů, pro které byl balíček vydán. Číslo odkazuje na seznam těchto softwarových produktů.
- **Odtsranitelná (Removable).** Pokud potřebujete vrátit zpět konkrétní záplatu či aktualizaci, tak se musíte nejprve ujistit zda lze vůbec záplatu nebo aktualizaci odinstalovat. Použijte tento filtr k zjištění, které z aktualizací či záplat jsou odinstalovatelné či odstranitelné. Pro více informací čtěte Odinstalace aktualizací či záplat (Uninstall patches).

Pro úpravu detailů zobrazených v tabulce:

1. Klikněte na III tlačítko **Sloupce** napravo od Panel Nástrojů.
2. Vyberte sloupce, které chcete zobrazit.
3. Klikněte na tlačítko **Resetovat** pro návrat pro zobrazení standardních sloupců.

Když jste na záložce, GravityZone procesy, které běží na pozadí mohou ovlivnit databázi. Ujistěte se, že se zobrazují ty nejnovější informace v tabulce kliknutím na tlačítko **Obnovit** v horní části tabulky.

GravityZone jednou týdně posoudí seznam dostupných oprav a odstraní ty, které již nejsou použitelné, protože související aplikace nebo koncové body již neexistují.

GravityZone také denně kontroluje a odstraňuje záplaty, které nejsou v seznamu k dispozici, ačkoli mohou být na některých koncových bodech.

6.6.2. Vyhledávání a Filtrování Balíčků

Běžně Control Center zobrazuje všechny dostupné balíčky pro váš software. GravityZone vám poskytuje pomocí pár možností rychle nalézt balíček, který potřebujete.

Filtrování balíčků podle produktu

1. Vyberte produkt z levého panelu.

   Můžete to provést buď procházením seznamu a vyhledáním dodavatele nebo zadáním jeho jména do vyhledávače na horní straně pod okna.

2. Klikněte na jméno prodejce pro rozšířený seznam jejich produktů.
3. Vyberte produkt, pro který chcete zobrazit dostupné balíčky nebo jej od označte pro skrytí jeho balíčků.
4. Opakujte předchozí krok pro ostatní produkty, které vás zajímají.

Pokud chcete znovu zobrazit balíčky pro všechny produkty, klikněte na tlačítko **Zobrazit vše** v navrchu levého panelu.

Filtrování balíčků podle užitečnosti

Balíček se stává zbytečným, jestliže je například vlastní nebo novější verze je již zavedena na koncových zařízeních. Protože inventář může v určitém bodě obsahovat podobné balíčky, GravityZone vám umožňuje je ignorovat. Vyberte balíčky a pak klikněte na tlačítko **Ignorovat balíčky** navrchu tabulky.

Control Center zobrazuje ignorované balíčky jinak. Klikněte na tlačítko **Spravované/Ignorované** v napravo od Panelu Nástrojů pro změnu zobrazení:

- - Pro zobrazení ignorovaných balíčků.
- - Pro zobrazení spravovaných balíčků.

Filtrování balíčků podle detailů

Využijte výhody vyhledávače pro filtrování balíčků podle určitých kritérií nebo podle známých detailů. Zadejte vyhledávané termíny do vyhledávače nahoře od tabulky s balíčky. Při psaní se v tabulce zobrazuj odpovídající balíčky nebo při provedené volbě.

Vymazáním vyhledávače se veškeré vyhledávání resetuje.

6.6.3. Ignorování záplat či aktualizací

Můžete si vyjmout konkrétní záplaty či aktualizace z inventáře, pokud je neplánujete instalovat na koncových bodech, použitím příkazu **Ignorovat záplaty či aktualizace (Ignore patches)**.

Ignorovaná zápata bude vyjmuta z automatických aktualizačních úloh a také z reportů a zároveň nebude počítána do seznamu chybějících aktualizací a záplat.

Pro ignorování záplaty či aktualizace:

1. Na stránce **Inventář záplat a aktualizací (Patch Inventory)** si vyberte vícero záplat či aktualizací, které chcete ignorovat.
2. Klikněte na tlačítko **Ignorovat záplatu či aktualizaci** na vrchní straně tabulky.

Zobrazí se vám konfigurační okno , kde si můžete prohlédnbout detailní infomace ohledně vybraných záplat či aktualizací spolu s informacemi o případných podřízených záplatách či aktualizacích.

3. Klikněte na **Ignorovat (Ignore)**. Záplata či aktualizace bude vyjmuta ze seznamu inventáře.

Můžete malézt ignorované záplaty či aktualizace ve speciálním náhledu a následně na nich provádět akce:

- Klikněte na tlačítko **Zobrazit ignorované záplaty či aktualizace (Display ignored patches)** na vrchní straně tabulky. Zobrazí se Vám seznam všech ignorovaných záplat a aktualizací.
- Můžete také získat více informací o konkrétních ignorovaných záplatách či aktualizacích vygenerováním statistického reportu o záplatách a aktualizacích (patch statistics report). Vyberte si ignorovanou záplatu či aktualizaci a klikněte na tlačítko **Statistické údaje k záplatám a aktualizacím (Patch stats)** na horní straně tabulky. Pro více informací čtěte „Vytváření Statistik Balíčků“ (str. 199)
- Pro obnovení ignorovaných záplat , si je vyberte a pak klikněte , na tlačítko **Obnovení záplat a aktualizací (Restore patches)** na vrchní straně tabulky.

  Zobrazí se konfigurační okno, kde můžete shlédnout detailní informace o vybraných záplatách a aktualizacích.

  Klikněte na tlačítko **Obnovit (Restore)** za účelem zaslání záplaty nebo aktualizace do inventáře.

6.6.4. Instalování Balíčků

Pro instalaci balíčků z Inventáře Balíčků:

1. Přejděte na **Síť (Network) > Inventář záplat a aktualizací (Patch Inventory)**.
2. Lokalizujte balíčky, které chcete nainstalovat. Pokud je to nutné, použijte filtrovací možnosti pro jejich rychlé nalezení.
3. Vyberte si záplati či aktualizaci a klikněte na tlačítko **Instalace (Install)** na vrchní straně tabulky. Zorazí se vám konfigurační okno, kde si můžete zeditovat detaily k instalaci záplat a aktualizací.

   Zobrazí se Vám vybrané záplaty či aktualizace, spolu s případnými podřízenými záplatami a aktualizacemi.

   - Zvolte cílovou skupinu koncových bodů.

- **Dle potřeby restarujte koncové body po instalaci záplat či aktualizací** Tato volba restaruje koncové body okamžitě po instalaci záplaty nebo aktualizace, v případě že bude restart systému nutný. Berte v úvahu, že tato akce může přerušit uživatelské aktivity.

  Ponechání této volby ve stavu vypnuto znamená, že pokud bude potřeba restartu na cílových koncových bodech, tak se ohledně nich zobrazí notifikace Ikona stavu Čekající na restart v síťovém inventáři (network inventory) GravityZone . V takovémto případě máte následující možnosti:

  – Poslat úlohu **Restartovat stroj (Restart machine)** na koncové body čekající na restart kdykoliv se rozhodnete. Více informací naleznete na „Restartovat stroj“ (str. 98).

  – Nastavit aktivní politiku pro notifikaci uživatele koncového bodu, že je nutný restart stroje. Abyste to udělali, musíte vstoupit do aktivní politiky na cílovém koncovém bodu a přejít na **Všeobecné (General) > Notifikace (Notifications)** a zapnout volbu **Notifikace nutnosti restartu koncového bodu (Endpoint Restart Notification)**. V tomto případě , uživatel obdrží hlášení pokaždé, když bude potřebovat restartovat stroj podle změn uvedených v GravityZone komponentech. Jakožto například tady ve správě záplat a aktualizací (Patch Managementu). Vyskakovací okno umožní posunout časově restart stroje. Pokud se uživatel rozhodne odložit restart, bude se na obrazovce pravidelně zobrazovat oznámení o nutnosti restartu, a to do doby než uživatel restartuje systém nebo dokud neuplyne čas stanovený správcem společnosti.

    Více informací naleznete na „Oznámení o Restartu Koncového zařízení“ (str. 233).

4. Klikněte na **Instalovat**.

   Vytvoří se instalační úloha, společně s pod-úlohami pro každý cílový koncový bod.

Poznámka

- Můžete také nainstalovat záplatu či aktualizaci přímo ze stránky **Síť (Network)** počínaje od konkrétního koncového bodu kterého chcete spravovat. V tomto případě vyberte koncové body ze síťového inventáře, klikněte na tlačítko **Úlohy (Tasks)** na horní straně tabulky a vyberte **Instalace záplaty či aktualizace (Patch Install)**. Další informace viz „Instalace balíčků“ (str. 83).

- Poté co nainstalujete záplatu či aktualizaci, doporučujeme zaslat úlohu Sken hledání záplat či aktualizací (Patch Scan) na všechny cílené koncové body. Tato úloha akttualizuje informace o záplatách a aktualizacích uložené v GravityZone pro vaše spravované sítě.

6.6.5. Odinstalace záplat či aktualizací

Můžete odebrat záplatu či aktualizaci, která způsobila poruchu na cílených koncových bodech. GravityZone umožňuje funkci zpětné deinstalace (rollback feature)pro záplaty a aktualizace nainstalované ve vaší síti,která obnoví software do původního stavu před použitím záplaty či aktualizace.

Tato funkce pro deinstalaci je dostupná pouze na těch záplatách a aktualizacích, které lze odebrat. GravityZone inventář záplat a aktualizací (patch inventory) obsahje sloupec **Odebíratelné (Removable)** kde si můžete vyfiltrovat záplaty a aktualizace podle jejich odebíratelnosti.

Poznámka
Atribut odebíratelnosti závísí na to zda záplata či aktualizace byla výrobcem vyrobena nebo změněna tak aby bylo možné záplaty a aktualizace software odebírat. Pro záplaty či aktualizace, ktereé nelze odebrat budete muset reinstalovat celý software.

Pro odinstalaci záplaty či aktualizace:

1. Přejděte na **Síť (Network) > Inventář záplat a aktualizací (Patch Inventory)**.
2. Vyberte záplatu či aktualizaci (patch), kterou chcete odinstalovat. Za účelem vyhledávání ve specifickém adresáři, použijte filtry ve slouopci jako třeba KB číslo nebo CVE. Použijte sloupec **Odstranitelné (Removable)** pro zobrazení dostupných záplat a aktualizací, které se dají odinstalovat.

   Poznámka
   Můžete odinstalovat pouze jednu záplatu nebo aktualizaci zároveň na vícero koncových bodech.

3. Klikněte na tlačítko ⊗ **Odinstalace (Uninstall)** na vrchní straně tabulky. Zobrazí se vám konfigurační okno, kde můžete editovat detaily odinstalačnich úloh.
   - **Název úlohy (Task name)**. Pokud chcete, můžete editovat standartní jméno úlohy pro deinstalaci záplaty či aktualizace. Ovšem budete moci identifikovat jednodušeji úlohu na stránce e **Úlohy (Tasks)**.

- **Přidejte záplatu do seznamu ignorovaných záplat a aktualizací**. Normálně nebudete potřebovat nikdy více záplaty či aktualizaci deinstalovat. Tato volba automaticky přidá záplatu či aktualizaci do seznamu ignorovaných (ignored list), jakmile je záplata či aktualizace odinstalována.
- **Restartujte koncové body poté co byla deinstalována záplata či aktualizace , vždycky když je to potřeba** Tato vola restartuje koncové body okamžitě po deinstalaci záplaty či aktualizace, v případě že systémový restart budy vyžadován. Berte v úvahu, že tato akce může přerušit uživatelské aktivity.

  Ponechání této volby ve stavu vypnuto znamená, že pokud bude potřeba restartu na cílových koncových bodech, tak se ohledně nich zobrazí notifikace Ikona stavu Čekající na restart v síťovém inventáři (network inventory) GravityZone . V takovémto případě máte následující možnosti:

  – Poslat úlohu **Restartovat stroj (Restart machine)** na koncové body čekající na restart kdykoliv se rozhodnete. Více informací naleznete na „Restartovat stroj“ (str. 98).

  – Nastavit aktivní politiku pro notifikaci uživatele koncového bodu, že je nutný restart stroje. Abyste to udělali, musíte vstoupit do aktivní politiky na cílovém koncovém bodu a přejít na **Všeobecné (General) > Notifikace (Notifications)** a zapnout volbu **Notifikace nutnosti restartu koncového bodu (Endpoint Restart Notification)**. V tomto případě , uživatel obdrží hlášení pokaždé, když bude potřebovat restartovat stroj podle změn uvedených v GravityZone komponentech. Jakožto například tady ve správě záplat a aktualizací (Patch Managementu). Vyskakovací okno umožní posunout časově restart stroje. Pokud se uživatel rozhodne odložit restart, bude se na obrazovce pravidelně zobrazovat oznámení o nutnosti restartu, a to do doby než uživatel restartuje systém nebo dokud neuplyne čas stanovený správcem společnosti.

    Více informací naleznete na „Oznámení o Restartu Koncového zařízení“ (str. 233).
- V tabulce **Navrácení do původního stavu (Rollback targets)** vyberte koncové body na kterých chcete odinstalovat záplatu či aktualizaci.

  Můžete vybrat jeden nebo více koncových bodů v síti. Použijte dostupné filtry k lokalizaci koncového bodu vaší volby.

Poznámka
Tabulka zobrazuje koncové body na kterých jsou záplaty či aktualizace nainstalovány.

4. Klikněte na **Potvrdit (Confirm)**. Bude vytvořena úloha **Odinstalace záplat a aktualizací (Patch Uninstall)** a následně bude tato úloha zaslána na cílové koncové body.

   Report o **Odinstalovaných záplatatách (Patch Uninstall Report)** se generuje ihned automaticky pro každou ukončenou úlohu odinstalovaných záplat, a informuje tak o detailech k záplatám, cílovým koncovým bodům a stavu odinstalací záplat či aktualizací.

Poznámka
Ihned po ukončení instalace záplaty doporučujeme poslat úlohu Proskenovat a najít záplaty (Patch Scan) na cílové koncové body. Tato úloha akttualizuje informace o záplatách a aktualizacích uložené v GravityZone pro vaše spravované sítě.

6.6.6. Vytváření Statistik Balíčků

Pokud potřebujete detaily o statusu u určitého balíčku pro všechna koncová zařízení, použijte funkci **Statistiky Balíčku**, která generuje okamžitou zprávu o vybraném balíčku:

1. Na záložce **Inventář Balíčků** vyberte jakýkoliv balíček z pravého panelu.
2. Klikněte na tlačítko **Statistika Balíčku** v horní části tabulky.

   Zpráva statistik balíčku ukazuje, poskytující různé detaily stavu balíčku, zahrnuje:

   - Koláčový graf ukazující procenta nainstalovaných neúspěšně, chybějící a čekající status u balíčku pro koncové zařízení, které hlásili dostupnost balíčeku.
   - Tabulka ukazující následující informace:
     - **Název**, **FQDN**, **IP** a **OS** každého koncového zařízení, které hlásilo zařízení.
     - **Poslední Kontrola**: čas kdy balíček byl naposledy zkontrolován koncovým zařízením.
     - **Status Balíčku**: nainstalován, neúspěšně, chybějící nebo ignorován.

Poznámka
Funkce Status balíčku je dostupná pro spravovaná a ignorované balíčky.

6.7. Prohlížení a správa úloh

Stránka **Síť > úlohy** vám umožňuje prohlížet a spravovat všechny vámi vytvořené úlohy.

Když vytvoříte úlohu pro jeden z několika síťových objektů, můžete ji prohlížet v tabulce úloh.

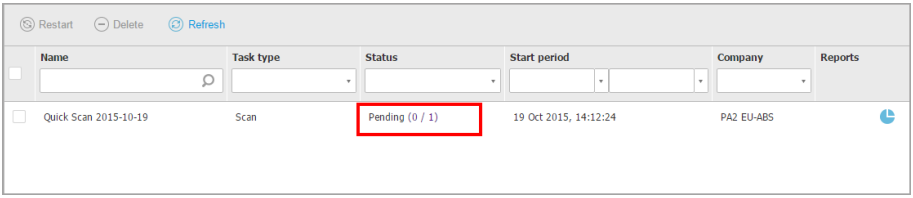
Na stránce **Síť > úlohy** můžete provádět následující:

- Kontrolovat stav úlohy
- Prohlížet přehledy úloh
- Restartovat úlohy
- Zastavit úlohy skenování Exchange
- Mazat úlohy

6.7.1. Kontrolovat stav úloh

Při každém vytvoření úlohy pro jeden nebo více síťových objektů budete chtít ověřit její průběh a být upozorněni v případě, že se vyskytnou problémy.

Přejděte na stránku **Síť > úlohy** a podívejte se na sloupec **Stav** u každé úlohy, která vás zajímá. Můžete zkontrolovat stav hlavní úlohy, a můžete také obdržet podrobné informace o každé podřízené úloze.



Stránka Úlohy

- **Kontrola stavu hlavní úlohy**.

  Hlavní úloha se týká akce spuštěné na síťových objektech (jako je instalace klienta nebo skenování) a obsahuje určitý počet podřízených úloh, jednu pro každý zvolený síťový objekt. Například, hlavní instalační úloha vytvořená pro osm počítačů obsahuje osm podřízených úloh. Čísla v závorkách představují podíl dokončení podřízených úloh. Například, (2/8) znamená, že jsou dokončené dvě z celkového počtu osmi podřízených úloh.

  Stav hlavní úlohy může být:

- **Čekající**, když ještě žádná z dílčích úloh nezačala, nebo když je přesažen počet možných souběžných zavádění. Maximální počet souběžných zavedení lze nastavit z nabídky **Konfigurace**. Více informací naleznete v instalačním průvodci GravityZone.
- **V průběhu**, když všechny podřízené úlohy pracují. Stav hlavní úlohy zůstane jako Probíhá, dokud se nedokončí poslední podřízená úloha.
- **Hotovo**, když jsou všechny podřízené úlohy (úspěšně nebo neúspěšně) dokončeny. V případě neúspěšných podřízených úloh se zobrazí varovný symbol.

- **Kontrolování stavu hlavní úlohy**.

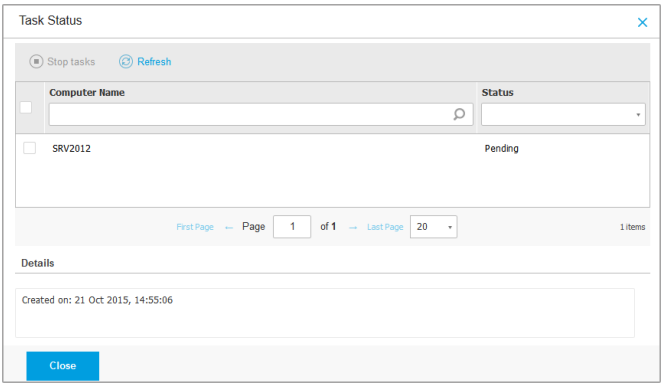
  Přejděte k požadované úloze a klikněte na odkaz dostupný ve sloupci **Stav**, čímž otevřete okno **Stav**. Uvidíte seznam síťových objektů přiřazených k hlavní úloze a stav příslušných podřízených úloh. Stav podřízených úloh může být:

  - **V průběhu**, když všechny podřízené úlohy stále pracují.

    Navíc, v případě skenování Exchange na vyžádání můžete prohlížet také stav dokončení.

  - **Hotovo**, když byla podřízená úloha úspěšně dokončena.
  - **Ve frontě**, pokud se podřízená úloha ještě nespustila. Toto se může stát v následujících situacích:
    - Podřízená úloha čeká ve frontě.
    - Mezi Control Center a síťovým objektem jsou problémy v připojení.
    - V případě mobilních zařízení je cílové zařízení Nečinné (offline). Úloha bude na zvoleném zařízení spuštěna, jakmile bude znovu online.
  - **Neúspěšný**, když se podřízená úloha nemohla spustit nebo se zastavila kvůli potížím, jako jsou chybná autentifikační pověření a nízká paměť.
  - **Zastavování**, když dokončení skenování na vyžádání trvá moc dlouho a vy jste se rozhodli ho zastavit.

  Pro zobrazení detailů každé podřízené úlohy ji vyberte a podívejte se na sekci **Podrobnosti** ve spodní části tabulky.



Podrobnosti o stavu úlohy

Obdržíte informace ohledně:

- Data a času začátku úlohy.
- Data a času dokončení úlohy.
- Popisu zaznamenaných chyb.

6.7.2. Prohlížení hlášení o úlohách

Na stránce **Síť > úlohy** máte možnost prohlížet hlášení úloh rychlého skenování.

1. Přejděte na stránku **Síť > úlohy**.
2. Vyberte požadovaný síťový objekt z nastavení zobrazení.
3. Označte zaškrtávací pole odpovídající požadované úloze skenování.
4. Klikněte na příslušné tlačítko v sloupci **Hlášení**. Počkejte, dokud se hlášení nezobrazí. Další informace viz „Používání Hlášení“ (str. 477).

6.7.3. Restartování úloh

Úlohy instalace klienta, odinstalace nebo aktualizace se z různých důvodů nemusí povést dokončit. Místo vytváření nových úloh můžete restartovat ty neúspěšné, pomocí následujících kroků:

1. Přejděte na stránku **Síť > úlohy**.
2. Vyberte požadovaný síťový objekt z nastavení zobrazení.

3. Označte zaškrtávací pole odpovídající neúspěšným úlohám.
4. Klikněte na tlačítko **Restartovat** v horní části tabulky. Zvolené úlohy se restartují a jejich stav se změní na **Opakuji pokus**.

Poznámka
Pro úlohy s několika podřízenými úlohami je možnost **Restartovat** dostupná pouze tehdy, když jsou všechny podřízené úlohy dokončeny, a restartuje pouze neúspěšné podřízené úlohy.

6.7.4. Zastavení úloh skenování Exchange

Skenování Exchange Store může zabrat značné množství času. Pokud si z jakéhokoli důvodu přejete zastavit úlohu skenování Exchange na vyžádání, následujte zde popsané kroky:

1. Přejděte na stránku **Síť > úlohy**.
2. Vyberte vhodné zobrazení sítě z nastavení zobrazení.
3. Klikněte na odkaz ve sloupci **Stav** pro otevření okna **Stav úloh**.
4. Označte pole odpovídající podřízeným úlohám, ve frontě nebo probíhajícím, které chcete zastavit.
5. Klikněte na tlačítko **Zastavit úlohy** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

Poznámka
Skenování Exchange Store na vyžádání můžete zastavit také z oblasti událostí v Bitdefender Endpoint Security Tools.

6.7.5. Mazání úloh

GravityZone automaticky maže úlohy ve frontě po dvou dnech a dokončené úlohy po 30 dnech. Pokud stále máte velké množství úloh, doporučujeme mazat již nepotřebné úlohy pro zamezení přeplnění seznamu.

1. Přejděte na stránku **Síť > úlohy**.
2. Vyberte požadovaný síťový objekt z nastavení zobrazení.
3. Označte pole odpovídající úloze, kterou chcete odstranit.
4. Klikněte na tlačítko **Smazat** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

Varování
Odstranění úlohy ve frontě úlohu také zruší.
Pokud mažete probíhající úlohu, všechny podřízené úlohy ve frontě budou zrušeny. V tomto případě nemohou být dokončené podřízené úlohy vráceny zpět.

6.8. Odstranění koncových bodů ze Síťového inventáře

Síťový inventář obsahuje standartně **Smazané (Deleted)** složky, určené pro ukládání koncových bodů, které nechcete spravovat.

Akce **Vymazat (Delete)** má následující důsledky:

- Když jsou nespravované koncové body vymazány, tak jsou přímo přemístěny do složky **Smazané (Deleted)**.
- Když jsou spravované koncové body smazány:
  - Vytvoří se odinstalační úloha
  - A jejich původní licence se uvolní k novému použití
  - Koncové body se přesunou do složky **Smazané (Deleted)**

Pro odstranění koncových bodů ze síťového inventáře:

1. Jděte do záložky **Síť**.
2. Vyberte vhodné zobrazení sítě z nastavení zobrazení.
3. V levém panelu vyberte **Vlastní skupiny**. Všechny dostupné koncové body v této skupině jsou zobrazeny v tabulce na pravém panelu.

   Poznámka
   Můžete mazat pouze koncové body zobrazené pod **Vlastními skupinami**, které jsou detekovány mimo jakoukoli integrovanou síťovou infrastrukturu.

4. V pravém panelu si vyberte pomocí odznačovacího rámečku koncový bod, který chcete vymazat.
5. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

   Pokud jem mazaný koncový bod spravován, tak se vytvoří úloha **Odinstalace klienta (Uninstall client)** na stránce **Úlohy (Tasks)** a bezpečnotní agent se odinstaluje z koncového bodu, přičemž se uvolní jeho licence pro další použití.

6. Koncový bod je přenesen do složky **Smazané (Deleted)**.

Můžete kdykoliv přenést koncové body ze složky **Smazané** do**Vlastní skupina**, použitím principu přetáhni myší a polož.

Poznámka

- Pokud chcete permanentně exkludovat konkrétní koncové body ze správy, tak je musíte držet ve složce **Smazané (Deleted)**.
- Pokud smažete koncové body ze sožky **Smazané (Deleted)** tak budou úplně smazány z databáze GravityZone. Nicméně, exckludované koncové body, které jsou online , budou detekovány další úlohou síťové detekce (Network Discovery) a zobrazí se v siťovém inventáři (Network Inventory) jakožto nové koncové body.

6.9. Konfigurace nastavení sítě

Na stránce **Konfigurace > Síťové nastavení** můžete nakonfigurovat nastavení související se síťovým inventářem, jako například: ukládání filtrů, zachování posledního prohlíženého umístění, vytváření a správa plánovaných pravidel pro odstraňování nepoužívaných virtuálních počítačů.

Možnosti jsou uspořádány do následujících sekcí:

- Nastavení síťového inventáře
- Vyčištění offline strojů

6.9.1. Nastavení síťového inventáře

V části **Nastavení síťového inventáře** jsou k dispozici následující možnosti:

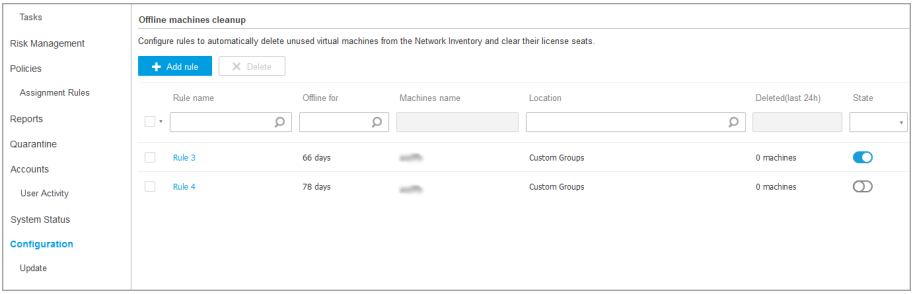
- **Uložit filtry Síťového Inventáře**. Zaškrtnutím tohoto políčka uložíte filtry na stránce **Síť** mezi relacemi Control Center.
- **Pamatovat si naposledy prohlížené místo v Síťovém inventáři, dokud se neodhlásím**. Zaškrtnutím tohoto políčka uložíte poslední místo, ke kterému jste při odchodu ze stránky **Síť** přistoupili. Umístění se mezi relacemi neukládá.
- **Vyhněte se duplikátům klonovaných koncových bodů** . Tuto možnost vyberte, chcete-li povolit nový typ síťových objektů v GravityZone, zvaných zlaté obrazy. Tímto způsobem můžete odlišit koncové body zdroje od jejich klonů. Dále musíte označit každý koncový bod, který klonujete:

  1. Jděte do záložky **Síť**.

2. Vyberte koncový bod, který chcete klonovat.
3. Z kontextové nabídky vyberte **Označit jako zlatý obraz** .

6.9.2. Vyčištění offline strojů

V části **Vyčištění offline počítačů** můžete naplánovat pravidla tak, aby se automaticky nepoužívané virtuální počítače ze Síťového inventáře automaticky odstraňovaly.



Konfigurace - Nastavení sítě - Vyčištění offline počítačů

Vytváření pravidel

Postup vytvoření pravidla čištění:

1. V části **Vyčištění offline počítačů** klikněte na tlačítko **Přidat pravidlo**.
2. Na konfigurační stránce:
   a. Zadejte název pravidla.
   b. Vyberte hodinu pro každodenní vyčištění.
   c. Definujte kritéria čištění:
      - Počet dní, kdy byly stroje offline (od 1 do 90).
      - Vzor názvu, který se může vztahovat na jeden virtuální stroj nebo na více virtuálních strojů.

        Například pomocí `machine_ 1` vymažte stroj s tímto názvem. Případně můžete použít `machine_ *` a odstranit všechny počítače, jejichž jméno začíná na `machine_`.

Toto pole rozlišuje velká a malá písmena a přijímá pouze písmena, číslice a speciální znaky hvězdičku (*), podtržítko (_) a pomlčku (-). Název nemůže začínat hvězdičkou (*).

d. Vyberte cílové skupiny koncových bodů v Network Inventory, kde se má pravidlo použít.

3. Klikněte na tlačítko **Save**.

Zobrazení a správa pravidel

Nastavení sítě > Čištění offline počítačů zobrazuje všechna pravidla, která jste vytvořili. Speciální tabulka vám poskytne následující podrobnosti:

- Jméno pravidla.
- Počet dní v offline režimu.
- Vzor názvu stroje.
- Umístění v síťovém inventáři.
- Počet smazaných strojů za posledních 24 hodin.
- Stav: povoleno, zakázáno nebo neplatné.

Poznámka
Pravidlo je neplatné, pokud cíle z určitých důvodů již nejsou platné. Virtuální stroje byly například odstraněny nebo k nim již nemáte přístup.

Nově vytvořené pravidlo je ve výchozím nastavení povoleno. Pravidla můžete kdykoli povolit nebo zakázat pomocí přepínače Zapnuto/Vypnuto ve sloupci **Status** .

V případě potřeby vyhledejte konkrétní pravidla pomocí možností třídění a filtrování v horní části tabulky.

Chcete-li upravit pravidlo:

1. Klikněte na název pravidla.
2. Na stránce konfigurace upravte podrobnosti pravidla.
3. Klikněte na tlačítko **Save**.

Odstranění jednoho nebo více pravidel:

1. Pomocí zaškrtávacích políček vyberte jedno nebo více pravidel.
2. Klikněte na tlačítko **Smazat** v horní části tabulky.

6.10. Konfigurace nastavení Security Server

Security Server používají svůj mechanismus ukládání do mezipaměti k deduplikování skenování antimalwaru, což optimalizuje tento proces. Dalším krokem s optimalizací skenování je sdílení této mezipaměti s ostatními Security Server.

Sdílení mezipaměti/cache funguje pouze mezi Security Servery stejného typu. Například multiplatforma Security Server bude sdílet svou mezipaměť pouze s jinou platformou Security Server a ne s Security Server pro NSX.

Pro povolení a konfiguraci sdílení mezipaměti:

1. Přejděte na stranu **konfigurace > Security Server nastavení** .
2. Zaškrtněte políčko **Security Server zdílení Cache** .
3. Vyberte rozsah sdílení:
   - Všechny dostupné Security Server

     Doporučuje se použít tuto možnost, pokud jsou všechny Security Server ve stejné síti.
   - Security Server je k dispozici v seznamu přiřazení.

     Tuto možnost použijte, pokud jsou Security Server rozšířeny v různých sítích a sdílení mezipaměti může generovat velké množství provozu.
4. Pokud omezujete rozsah, vytvořte skupinu Security Server. V rozevíracím seznamu vyberte Security Server a klikněte na **Přidat** .

   Mezipaměť budou sdílet pouze Security Server v tabulce.

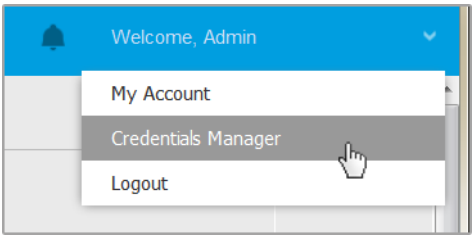
   Poznámka
   Security Server pro NSX-T a NSX-V si vyměňují informace o mezipaměti pouze na stejném serveru vCenter.

5. Klikněte na tlačítko **Save**.

6.11. Správce přihlašovacích údajů

Správce pověření vám pomáhá definovat pověření nezbytná pro přístup k dostupným inventářům vCenter Server a také pro autentizaci na dálku na různých operačních systémech ve vaší síti.

Pro otevření Správce pověření klikněte na své uživatelské jméno v pravém horním rohu stránky a zvolte **Správce pověření**.



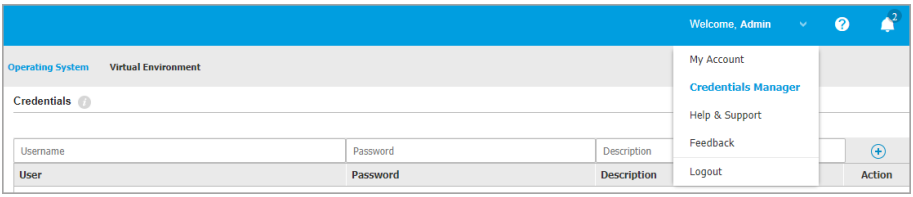
Nabídka Správce pověření

Okno **Správce pověření** obsahuje dvě karty:

- Operační systém
- Virtuální prostředí

6.11.1. Operační systém

Pro přidání sady pověření:



Správce přihlašovacích údajů

1. Zadejte uživatelské jméno a heslo administrátorského účtu pro každý cílový operační systém do příslušných polí v horní části záhlaví tabulky. Můžete také přidat popis, který vám usnadní identifikaci jednotlivých účtů. Pokud jsou počítače v doméně, stačí zadat pověření administrátora domény.

   Při zadávání jména uživatelského účtu použijte konvence systému Windows:

   - Pro stroje s Active Directory použijte tyto syntaxe: `username@domain.com` a `domain\username`. Abyste si mohli být jisti, že pověření budou fungovat, zadejte je v obou tvarech (`username@domain.com` a `domain\username`).
   - Pro stroje Pracovní skupiny stačí zadat pouze uživatelské jméno bez jména pracovní skupiny.

2. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky. Nová sada pověření je přidána do tabulky.

> **Poznámka**
> Pokud jste neurčili autentifikační pověření, budete je muset zadat při spouštění instalační úlohy. Zadaná pověření jsou automaticky uložena do vašeho Správce pověření, takže je příště už nemusíte zadávat.

6.11.2. Virtuální prostředí

Z karty Virtuální prostředí můžete spravovat autentizační pověření pro dostupné systémy virtualizovaných serverů.

Pro přístup do virtualizované infrastruktůry integrované s Control Center, si musíte pro každý dostupný virtualizační serverový systém vytvořit uživatelské přístupové údaje. Control Center používá vaše přihlašovací údaje pro připojení se k virtualizované infrastruktuře, a zobrazuje pouze zdroje, ke kterým máte přístup (jak je definováno ve virtualizačním serveru).

Pro určení pověření nutných pro připojení se k virtualizovanému serveru:

1. Vyberte server z příslušné nabídky.

> **Poznámka**
> Pokud nabídka není k dispozici, tak buď ještě nebyla nastavena žádná integrace, nebo již byla nastavena všechna potřebná pověření.

2. Zadejte své uživatelské jméno a heslo a definující popis.
3. Klikněte na tlačítko ⊕ **Přidat**. Nová sada pověření je přidána do tabulky.

> **Poznámka**
> Pokud nenastavíte vaše autentizační pověření ve Správci pověření, budete je muset zadat ve chvíli, kdy se pokusíte prohlížet inventář jakéhokoli systému virtualizovaných serverů. Jakmile zadáte svá pověření, uloží se do Správce pověření a příště je už zadávat nemusíte.

> **Důležité**
> Kdykoli změníte uživatelské heslo pro váš virtualizovaný serverový systém, nezapomeňte ho aktualizovat také ve Správci pověření.

6.11.3. Odstranění pověření ze Správce pověření

Pro odstranění starých pověření ze Správce pověření:

1. Ukažte na řádek v tabulce obsahující pověření, která chcete odstranit.
2. Klikněte na tlačítko ⊗ **Odstranit** na pravé straně odpovídajícího řádku tabulky. Zvolený účet bude odstraněn.

7. ZÁSADY ZABEZPEČENÍ

Jakmile nainstalované, zabezpečení Bitdefender může být nastaveno a spravováno z Control Center za použití bezpečnostních zásad. Pravidlo určuje bezpečnostní nastavení, která mají být zavedena na cílových objektech síťového inventáře (počítače, virtuální zařízení nebo mobilní zařízení).

Neprodleně po instalaci je k objektům síťového inventáře přiřazeno výchozí pravidlo, které je přednastaveno s doporučeným nastavením ochrany. Za předpokladu, že je povolena integrace s NSX, jsou k dispozici další tři bezpečností zásady pro NSX, jedno pro každou úroveň zabezpečení: tolerantní, normální a agresivní. Tyto zásady jsou přednastaveny podle doporučeného bezpečnostního nastavení. Výchozí pravidla nemůžete upravovat ani smazat.

Na základě bezpečnostních požadavků můžete vytvořit tolik zásad, kolik potřebujete, pro každý typ spravovaného síťového souboru.

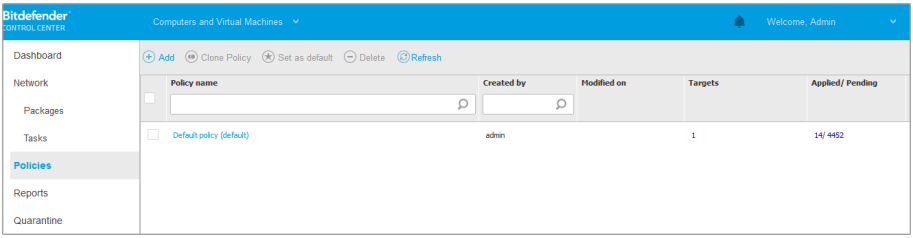
O pravidlech je nutné vědět následující:

- Pravidla se vytváří na stránce **Pravidla** a jsou přiřazována k síťovým objektům ze stránky **Síť**.
- Pravidla mohou dědit několik modulových nastavení z jiných pravidel.
- Můžete nastavit přiřazování pravidel ke koncovým bodům tak, aby platilo pouze za určitých podmínek, podle polohy nebo přihlášeného uživatele. Tím pádem může mít koncový bod více přiřazených pravidel.
- Koncové body mohou mít v jednu chvíli aktivní pouze jedno pravidlo.
- Pravidlo můžete přiřadit jednotlivým koncovým bodům, nebo skupinám koncových bodů. Při přiřazování pravidla definujte také možnosti přejímání pravidel. Ve výchozím nastavení koncový bod dědí pravidla své rodičovské skupiny.
- Pravidla jsou prosazeny na cílových síťových objektech okamžitě po jejich vytvoření nebo úpravě. Nastavení by měla být aplikována na síťové objekty za méně než minutu (pokud jsou online). Pokud síťový objekt není online, v nastavení se objeví, jakmile bude opět online.
- Práva se aplikují pouze pro nainstalované ochranné moduly.
- Záložka **Práva** ukazuje pouze následující typy práv:
  - Práva vytvořená vámi.
  - Další práva (jako základní práva nebo šablony vytvořené jinými uživateli), která jsou přiřazena ke koncovým zařízením pod vaším účtem.
- Nemůžete upravovat práva vytvořená jinými uživateli (pokud není to umožněno v nastavení práv), ale mohou být přepsána přiřazením jiných oprávnění objektu.

Varování
Pouze podporované moduly práv budou aplikovány na cílová koncová zařízení. Upozorňujeme, že pro servery je podporován pouze modul Antimalware.

7.1. Přiřazování pravidel

Můžete si zobrazit a spravovat práva na záložce **Práva**.



Záložka Práv

Každý typ koncového zařízení má zvláštní nastavení zásad. Pro spravování zásad musíte nejprve zvolit typ koncového zařízení **Počítače a Virtuální zařízení** nebo **Mobilní zařízení**) z nastavení zobrazení.

Existující práva jsou zobrazeny v tabulce. Pro každé právo, můžete zobrazit:

- Název práva.
- Uživatele, který právo vytvořil.
- Datum a čas, kdy bylo právo naposledy upraveno.
- Počet cílů, na který bylo právo posláno.*
- Počet cílů, na které bylo právo aplikováno / čeká.*

Pro pravidla s povoleným modulem NSX jsou k dispozici doplňující informace:

- Název NSX pravidla, používané pro identifikaci pravidla Bitdefender v VMware vSphere.
- Viditelnost pravidla ve správních konzolích, umožňující vám filtrovat pravidla pro NSX. Tím pádem, zatímco **Místní** pravidla jsou viditelná pouze v Bitdefender Control Center, **Globální** pravidla jsou viditelná také v VMware NSX.

Všechny podrobnosti jsou ve výchozím stavu skryté.

Pro úpravu zobrazených detailů práva v tabulce:

1. Klikněte na III tlačítko **Sloupce** napravo od Panel Nástrojů.
2. Vyberte sloupce, které chcete zobrazit.
3. Klikněte na tlačítko **Resetovat** pro návrat pro zobrazení standardních sloupců.

* Kliknutím na číslo budete přesměrováni na stránku **Síť**, kde můžete prohlížet příslušná koncová zařízení. Budete vyzváni ke zvolení nastavení zobrazení. Tím bude podle kritérií pravidla vytvořen filtr.

Můžete třídit dostupná práva a také vyhledávat pro určitá práva pomocí dostupných kritérií.

7.1.1. Vytváření Práv

Práva můžete také vytvářet pomocí přidávání nového nebo duplikování (klonování) existujícího práva.

Pro vytvoření bezpečnostního pravidla:

1. Jděte na záložku **Práva**
2. Zvolte požadovaný typ koncového zařízení v nastavení zobrazení.
3. Vyberte si metodu vytvoření oprávnění:
   - **Přidat nové oprávnění.**
     - Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Tento příkaz vytvoří nové oprávnění ve formě základní předlohy pro oprávnění.
   - **Klování existujícího oprávnění**.
     a. Vyberte zaškrtávací pole práva, které chcete duplikovat.
     b. Klikněte na tlačítko ⊕ **Klonovat** navrchu tabulky.
4. Konfigurace nastavení oprávnění. Pro podrobné informace se odkažte na:
   - „Pravidla pro počítače a virtuální stroje“ (str. 227)
   - „Politiky Mobilních Zařízení“ (str. 381)
5. Klikněte na **Uložit** pro vytvoření oprávnění a vraťte se do seznamu oprávnění.

Při určování pravidel pro užití v VMware NSX, kromě nastavení parametrů antimalwarové ochrany v GravityZone Control Center musíte také vytvořit pravidlo v NSX a nastavit ho tak, aby používalo zásady GravityZone jako služební profil. Pro vytvoření bezpečnostního pravidla pro NSX:

1. Přihlašte se do vSphere Web Client.

2. Přejděte na kartu **Síť & Zabezpečení > Service Composer > Bezpečnostní pravidla**.
3. Klikněte na tlačítko **Vytvořit bezpečnostní pravidlo** na liště v horní části tabulky pravidel. Zobrazí se konfigurační okno.
4. Zadejte jméno pravidla a poté klikněte na **Další**.

   Případně můžete přidat krátký popisek.
5. Klikněte na **Add Guest Introspection service** v horní části tabulky. Okno Guest Introspection Service se zobrazí.
6. Zadejte název a popis služby.
7. Ponechejte výchozí akce vybrané, pro povolení Bitdefender služebního profilu, aby byl aplikován na bezpečnostní skupinu.
8. Z nabídky **Service Name**, vyberte **Bitdefender**.
9. Z nabídky **Service Profile**, vyberte existující GravityZone bezpečnostní politiku.
10. Nepřepisujte výchozí hodnoty **State** a možnosti **Enforce**.

    Poznámka
    Pro více informací o nastavení bezpečnostní politiky, obraťte se na VMware NSX documentation.

11. Klikněte na **OK** pro přidání služby.
12. Klikejte na **Next** dokud se nedostanete k poslednímu kroku a poté klikněte na **Finish**.

7.1.2. Přiřazování pravidel

Koncovým zařízení jsou zpočátku přiřazena základní oprávnění. Jednou jakmile máte nadefinovány nezbytná oprávnění v záložce **Práva**, můžete je přiřadit na koncová zařízení.

Proces přiřazování politiky je vázaný k různým prostředím, která jsou připojena ke GravityZone. Pro určitá propojení, jako například VMware NSX, jsou politiky dostupné z GravityZone Control Center. Také referují k externím politikám.

Přiřazování Politik Lokálně

Můžete přiřadit lokální politiky dvěma způsoby:

- Přiřazování podle zařízení, znamená že manuálně vyberete cílová koncová zařízení, pro které chcete přiřadit oprávnění. Tato oprávnění jsou známá také jako oprávnění zařízení.
- Přiřazení na základě pravidel znamená, že zásada je přiřazena k spravovanému koncovému bodu, pokud se jeho síťová nastavení shodují s podmínkami určenými existujícím přiřazovacím pravidlem.

Poznámka

- Můžete přiřadit pouze vámi vytvořená pravidla. Pro přiřazení pravidla vytvořeného jiným uživatelem ji musíte nejprve naklonovat na stránce **Pravidla**.
- Na virtuálních strojích chráněných pouze s HVI můžete přiřadit pouze pravidla zařízení. Když je Bitdefender Endpoint Security Tools také nainstalovaný také na nich, můžete přiřadit také politiky založených na pravidlech, bezpečnostní agent spravující politiku aktivace.

  Poznámka
  Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Přiřazování pravidel zařízení

V GravityZone můžete přiřadit zásady více způsoby:

- Přiřaďte pravidlo přímo k cíli.
- Přiřaďte pravidlo rodičovské skupiny prostřednictvím dědičnosti.
- Vynutit dědění politiky na cíli.

Ve výchozím nastavení koncový bod dědí pravidla své rodičovské skupiny. Pokud jste změnili politiku v rodičovské skupině (parent group), tak to bude mít vliv na všechny podskupiny, s vyjímkou těch které mají vynucenou politiku.

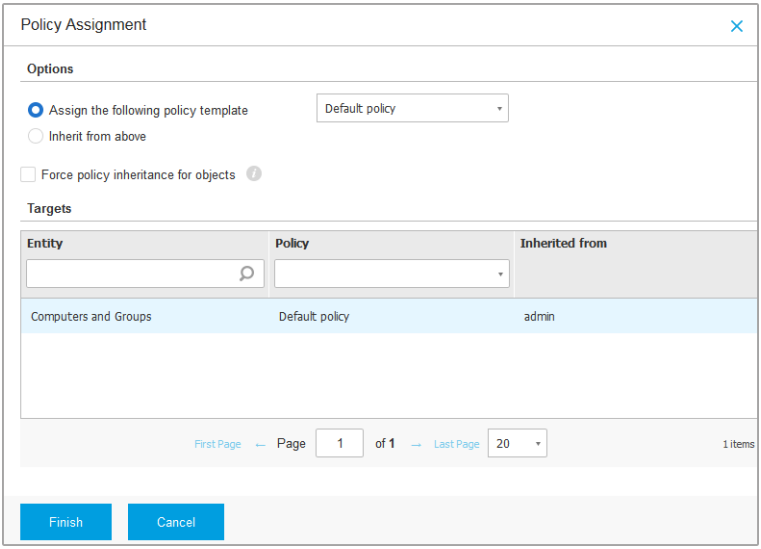
Pro přiřazení pravidla zařízení:

1. Jděte do záložky **Síť**.
2. Vyberte vhodné zobrazení sítě z nastavení zobrazení.
3. Zvolte cílové koncové body. Můžete vybrat jeden či skupinu koncových bodů.

   Pro účel dědění, nemůžete změnit výchozí politiku v kořenové skupině. Například, **Počítač a Virtuální Stroj** budou mít vždy **Výchozí politiku** přiřazenou.

4. Klikněte na tlačítko **Přiřadit pravidlo** na horní straně tabulky nebo vyberte možnost **Přiřadit pravidla** z kontextového menu.

   Zobrazí se okno **Přiřazení pravidel**:



Nastavení přiřazování pravidel

5. Zkontrolujte tabulku s cílovými koncovými body Pro každý koncový bod můžete zobrazit:

   - Přidělená pravidla.
   - Rodičovská skupina (parent group), ze které cíl dědí případně pravidla (politiky).

     Pokud si skupina toto pravidlo vynucuje, můžete kliknutím na její název zobrazit stránku **Přiřazení pravidel** s touto skupinou jako cíl.
   - Stav vynucení.

     Tento stav ukazuje, zda cíl vynucuje dědičnost pravidla nebo zda je nucen toto pravidlo zdědit.

     Všimněte si cílů s vynucenými pravidly (politiky) (**Je vynucena** stav). Jejich pravidla nelze nahradit. V takovém případě se zobrazí varovná zpráva.

6. V případě varování klikněte na odkaz **Vyloučit tyto cíle** a pokračujte.
7. Vyberte jednu z dostupných možností pro přiřazení pravidla:
   - **Přiřaďit následující šablonu pravidla** - chcete-li určit konkrétní zásady přímo na cílové koncové body.
   - **Zdědit z vrchu** - pro použití pravidla (politiky) rodičovské skupiny (parent group).
8. Pokud jste se rozhodli přiřadit šablonu pravidla:
   a. Vyberte pravidlo z rozevíracího seznamu.
   b. Chcete-li dosáhnout následujících cílů, vyberte možnost **Vynutit dědičnost pravidel pro podřízené skupiny**.
      - Přiřadit pravidlo (politiku) všem následným potomkům cílových skupin bez vyjímky.
      - Zabraňte tomu, aby se změnila z jiné úrovně hierarchie.

      Nová tabulka rekurzivně zobrazuje všechny ovlivněné koncové body a skupiny koncových bodů spolu s politikami, které budou nahrazeny.
9. Klikněte na **Dokončit** pro uložení a použití změn. V opačném případě se k předchozí stránce vrátíte klepnutím na tlačítko **Zpět** nebo **Zrušit**.

Po dokončení jsou pravidla okamžitě přesunuty do cílových koncových bodů. Nastavení by měla být aplikována na síťové objekty za méně než minutu (pokud jsou online). Pokud síťový objekt není online, v nastavení se objeví, jakmile bude opět online.

Chcete-li zjistit, zda bylo pravidlo úspěšně přiřazeno:

1. Na stránce **Síť** klikněte na název koncového bodu, který vás zajímá. Control Center zobrazí okno **Informace**.
2. V sekci **Zásady** můžete zkontrolovat stav současné zásady. Musí se zobrazit **Použito** .

Další metodou ke kontrole stavu přiřazení je podrobností pravidel:

1. Jděte na záložku **Práva**
2. Vyhledejte zásady, které jste přiřadili.

   Ve sloupci **Aktivní/Aplikovaný/Čekající** můžete zobrazit počet koncových bodů pro každý ze tří stavů.

3. Kliknutím na libovolné číslo zobrazíte seznam koncových bodů s příslušným stavem na stránce **Síť**.

Přiřazování na pravidlech založených zásad

Stránka **Práva > Pravidla přiřazování** vám umožňuje nastavit pravidla, která jsou si vědoma uživatele a umístění. Například můžete aplikovat více omezující pravidla pro firewall, když se uživatelé připojují k internetu mimo firmu, nebo můžete povolit Kontrolu přístupu k webu pro uživatele, kteří nepatří do skupiny administrátorů.

O pravidlech přiřazování je nutné vědět následující:

- Koncové body mohou mít v jednu chvíli aktivní pouze jedno pravidlo.
- Zásada aplikovaná skrze pravidlo přepíše zásady zařízení nastavené na koncovém bodě.
- Pokud žádné z pravidel přiřazování není uplatnitelné, budou aplikovány zásady zařízení.
- Pravidla jsou nařizována a zpracovávána podle priority, přičemž `1` znamená nejvyšší. Pro jeden cíl můžete mít více pravidel. V tomto případě bude uplatněno první pravidlo, které se shoduje s aktivními nastaveními připojení na cílovém koncovém bodě.

  Například, pokud se koncové zařízení shoduje s uživatelským pravidlem s prioritou 4 a s pravidlem polohy s prioritou 3, bude platit pravidlo pro polohu.

Varování
Ujistěte se, že při tvorbě pravidel myslíte na citlivá nastavení, jako jsou výjimky, podrobnosti komunikace a proxy.
Jako nejlepší možný postup doporučujeme používat dědění zásad, čímž uchováte důležitá nastavení ze zásad zařízení také v zásadě používané pravidly pro přiřazování.

Pro vytvoření nového pravidla:

1. Přejděte na stránku **Pravidla přiřazování**.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky.
3. Vyberte typ pravidla:
   - Pravidlo umístění
   - Pravidlo uživatele
   - Pravidla Tagu

4. Nakonfigurujte nastavení pravidla dle potřeby.
5. Kliknutím na **Uložit** uložíte změny a aplikujete pravidlo na cílové koncové body patřící k zásadě.

Pro změnu nastavení existujícího pravidla:

1. Na stránce **Pravidla přiřazování** najděte požadované pravidlo a klikněte na jeho jméno, abyste ho mohli upravit.
2. Nakonfigurujte nastavení pravidla dle potřeby.
3. Kliknutím na **Uložit** uložíte změny a zavřete okno. Pro opuštění okna bez uložení změn klikněte na **Zrušit**.

Pokud pravidlo již nechcete používat, vyberte ho a klikněte na tlačítko ⊖ **Odstranit** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

Ujistěte se, že se zobrazují ty nejnovější informace kliknutím na tlačítko ⟳ **Obnovit** v horní části tabulky.

Nastavení Pravidel umístění

Umístění je úsek sítě, určený jedním nebo několika síťovými nastaveními, jako je specifická brána, DNS používané pro řešení URL, nebo podmnožina IP adres. Například, můžete určit umístění jako je firemní LAN, serverová farma nebo oddělení.

V okně nastavení pravidel postupujte podle následujících kroků:

1. Zadejte definující jméno a popis pro pravidlo, které chcete vytvořit.
2. Nastavte prioritu pravidla. Pravidla jsou řazena podle priority, přičemž první pravidlo má nejvyšší prioritu. Tu samou prioritu nelze nastavit dvakrát nebo více.
3. Zvolte zásadu, pro kterou tvoříte přiřazovací pravidlo.
4. Definujte umístění, pro která má pravidlo platit.
   a. Vyberte typ nastavení sítě z menu navrchu tabulky Umístění. Dostupné typy:

Typ	Hodnota
Rozsah IP/IP adres	Specifická IP adresa v síti nebo podsíti. Pro podsíť použijte formát CIDRu. Například: `10.10.0.12` nebo `10.10.0.0/16`
Adresa výchozí brány	IP adresa výchozí brány

Typ	Hodnota
Adresa WINS serveru	IP adresa WINS serveru **Důležité** Tato možnost neplatí pro Linux a Mac.
adresa DNS serveru	IP adresa DNS serveru
Připojování DHCP k DNS suffixu	Název DNS bez názvu pro určité připojení DHCP Například: `hq.company.biz`
Koncové zařízení vidí na hostitele	Název hosta. Například: `fileserv.company.biz`
Koncový bod se může připojit ke GravityZone.	Ano/Ne
Typ sítě	WiFi/Ethernet Při výběru WiFi, můžete přidat SSID sítě. **Důležité** Tato možnost neplatí pro Linux a Mac.

Hostname	Hostname
	Například: `cmp.bitdefender.com`
	
	Důležité
	Můžete také použít zástupné znaky. Hvězdička (*) nahrazuje nulu nebo více znaků a otazník (?) nahrazuje přesně jeden znak. Příklady:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

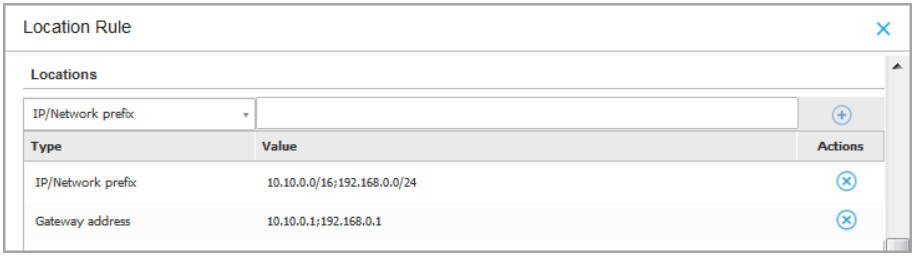
b. Zadejte hodnotu pro vybraný typ. Kde je možné zadat více hodnot do příslušného pole, oddělujte je pomocí středníků (;) a bez dalších mezer.

Například, když zadáte `10.10.0.0/16;192.168.0.0/24`, pravidla se aplikují na cílové koncová zařízení s příslušnými IP adresami v podsíti.

Varování
Můžete použít pouze jeden typ síťového nastavení pro pravidlo umístění. Například, pokud jste přidali umístění pomocí **IP/prefixu sítě**, toto nastavení už nemůžete použít znovu pro to samé pravidlo.

c. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.

Pro aplikování pravidla na koncové body se jejich nastavení sítě musí shodovat se VŠEMI umístěními. Například, pro identifikaci sítě LAN můžete zadat bránu, typ sítě a DNS; navíc, pokud přidáte podsíť, identifikujete oddělení v rámci firemní LAN.



Pravidlo umístění

Klikněte na pole **Hodnota** pro úpravu současných parametrů, a poté stiskněte `Enter` pro uložení změn.

Pro smazání umístění ho vyberte a klikněte na tlačítko ⊗ **Odstranit**.

5. Možná budete chtít některá umístění z pravidla vynechat. Pro vytvoření výjimky definujte umístění, která mají být vyloučena z pravidla:
   a. Označte pole **Výjimky** pod tabulkou Umístění.
   b. Vyberte typ nastavení sítě z menu v horní části tabulky Výjimky. Další informace o možnostech naleznete na stránce „Nastavení Pravidel umístění“ (str. 220).
   c. Zadejte hodnotu pro vybraný typ. Do příslušného pole můžete zadat více hodnot, oddělených středníkem (;) a bez dalších mezer.

d. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.

Pro aplikování výjimky se musí síťová nastavení koncových bodů shodovat se VŠEMI podmínkami uvedenými v tabulce Výjimky.

Klikněte na pole **Hodnota** pro úpravu současných parametrů, a poté stiskněte `Enter` pro uložení změn.

Pro smazání výjimky klikněte na tlačítko ⊗ **Odstranit** na pravé straně tabulky.

6. Klikněte na **Uložit** pro uložení a aplikaci přiřazovacího pravidla.

Jakmile je vytvořeno, pravidlo umístění se automaticky uplatní na všech spravovaných koncových bodech.

Nastavení uživatelských pravidel

Důležité

- Pravidla pro uživatele můžete vytvářet pouze v případě, že je integrace s Active Directory k dispozici.
- Můžete určit uživatelská pravidla pouze pro uživatele Active Directory a skupiny. Pravidla založená na skupinách Active Directory nejsou podporována na systémech Linux.

V okně nastavení pravidel postupujte podle následujících kroků:

1. Zadejte definující jméno a popis pro pravidlo, které chcete vytvořit.
2. Nastavte prioritu. Pravidla jsou řazena podle priority, přičemž první pravidlo má nejvyšší prioritu. Tu samou prioritu nelze nastavit dvakrát nebo více.
3. Zvolte zásadu, pro kterou tvoříte přiřazovací pravidlo.
4. V sekci **Cíle** vyberte uživatele a bezpečnostní skupiny, na které chcete aplikovat pravidlo. Prohlížejte svůj výběr v tabulce napravo.
5. Klikněte na tlačítko **Save**.

Jakmile je vytvořeno, pravidlo vědomé si uživatele je aplikováno na spravovaná zvolená zařízení při přihlášení uživatele.

Konfigurace pravidel tagů (značení)

Důležité
Pravidla pro tagy můžete vytvářet jen tehdy, pokud máte k dispozici integraci s Amazon EC2 nebo Microsoft Azure.

Můžete použít tagy definované v cloudové infrastruktuře k přiřazení a specifikování GravityZone politik k vaším virtuálním strojům hostovaným v cloudu. Všechny virtuální stroje které mají své tagy specifikované v pravidlech tagování budou aplikovány přímo s politikou přiřazenou tímto pravidlem.

Poznámka
Podle cloudové infrastruktury můžete definovat značky virtuálních strojů následovně:

- Pro Amazon EC2: v záložce **Tagy** dané instance EC2.
- Pro Microsoft Azure: v sekci **Přehled** daného virtuálního stroje.

Pravidlo tagu obsahuje jednen nebo vícero tagů. Pro vytvoření pravidla tagu:

1. Zadejte definující jméno a popis pro pravidlo, které chcete vytvořit.
2. Nastavte prioritu pravidla. Pravidla jsou řazena podle priority, přičemž první pravidlo má nejvyšší prioritu. Tu samou prioritu nelze nastavit dvakrát nebo více.
3. Vyberte politiku pro kterou vytváříte pravidlo tagu.
4. V tabulce **Tag** přidejte jeden či více tagů.

   Tag se skládá z páru klíčových hodnot obsahujících malá či velká písmena (case-sensitive key-value pair). Ujistěte se že zadáváte tagy definované ve vaší cloudové infrastruktuře. Pouze platné páry klíčových hodnot budou brány v potaz.

   Pro přidání tagu:

   a. Zadejte v poli **Klíč Tagu** jméno klíče.

   b. V poli **Hodnota Tagu** zadejte hodnotu jména.

   c. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.

Přiřazování Politik v NSX

V NSX, jsou bezpečnostní politiky přiřazeny k bezpečnostním skupinám. Bezpečnostní skupina může obsahovat důležité objekty vCenter, jako například datacentra, clustery a virtuální stroje.

Přiřazení bezpečnostní politiky k bezpečnostní skupině:

1. Přihlašte se do vSphere Web Client.
2. Přejděte do **Network & Security > Service Composer** a klikněte na záložku **Security Groups**.
3. Můžete vytvořit tolik bezpečnostních skupin, kolik je potřeba. Pro více informací se obraťte na VMware documentation.

   Můžete vytvořit dynamické bezpečnostní skupiny, pomocí bezpečnostních tagů. Tímto způsobem můžete seskupit všechny virtuální stroje vyhodnocené jako infikované.
4. Pravým kliknutím na bezpečnostní skupinu, která vás zajímá a kliknutím **Apply Policy**.
5. Vyberte politiku, kterou chcete aplikovat a klikněte na **OK**.

7.1.3. Změna nastavení pravidel

Nastavení pravidel může být nastaveno na začátku jejich tvorby. Později je můžete změnit podle svých potřeb.

Poznámka
Ve výchozím nastavení může pravidla upravovat pouze uživatel, který je vytvořil. Pro změnu tohoto nastavení musí autor pravidla označit možnost **Povolit ostatním uživatelům měnit toto pravidlo** ze stránky **Podrobnosti** pravidla.

Pro změnu nastavení existujícího pravidla:

1. Jděte na záložku **Práva**
2. Zvolte požadovaný typ koncového zařízení v nastavení zobrazení.
3. Najděte požadované pravidlo v seznamu a klikněte na jeho jméno pro zahájení úprav.
4. Nakonfigurujte nastavení pravidla dle potřeby. Pro podrobné informace se odkažte na:

- „Pravidla pro počítače a virtuální stroje“ (str. 227)
- „Politiky Mobilních Zařízení“ (str. 381)

5. Klikněte na tlačítko **Save**.

   Zásady jsou zavedeny na cílové síťové objekty neprodleně po provedení změn v přiřazování zásad nebo po úpravě přiřazovacích nastavení. Nastavení by měla být aplikována na síťové objekty za méně než minutu (pokud jsou online). Pokud síťový objekt není online, v nastavení se objeví, jakmile bude opět online.

7.1.4. Přejmenování pravidel

Pravidla by měla mít definující jména, aby jste je vy nebo jiný administrátor mohli snadno rozpoznat.

Pro přejmenování pravidla:

1. Jděte na záložku **Práva**
2. Zvolte požadovaný typ koncového zařízení v nastavení zobrazení.
3. Klikněte na název pravidla. Tím se otevře stránka pravidel.
4. Zadejte název nového pravidla.
5. Klikněte na tlačítko **Save**.

Poznámka
Jméno pravidla je unikátní. Pro každé nové pravidlo musíte zadat jiné jméno.

7.1.5. Mazání pravidel

Pokud pravidlo již nepotřebujete, odstraňte ho. Jakmile je pravidlo odstraněno, na síťové objekty, ke kterým bylo přiřazeno, se uplatní nastavení jejich rodičovské skupiny. Pokud se neaplikuje žádné další pravidlo, bude nakonec vynuceno výchozí. Při mazání pravidla, které má sekce děděné jinými pravidly, nastavení těchto sekcí je uchováno v podřízených pravidlech.

Poznámka
Ve výchozím nastavení může pravidla mazat pouze uživatel, který je vytvořil. Pro změnu tohoto nastavení musí autor pravidla označit možnost **Povolit ostatním uživatelům měnit toto pravidlo** ze stránky **Podrobnosti** pravidla.

Aby jste mohly smazat nějakou NSX politiku ze GravityZone Control Center, musíte se ujistit, že politika není nikde použitá. Proto, přiřaďte cílové bezpečnostní skupině jiný bezpečnostní profil. Další informace viz „Přiřazování Politik v NSX“ (str. 225).

Pro smazání pravidla:

1. Jděte na záložku **Práva**
2. Zvolte požadovaný typ koncového zařízení v nastavení zobrazení.
3. Označte pole pravidla, které chcete odstranit.
4. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

7.2. Pravidla pro počítače a virtuální stroje

Nastavení pravidel může být nastaveno na začátku jejich tvorby. Později je můžete změnit podle svých potřeb.

Pro nastavení parametrů pravidla:

1. Jděte na záložku **Práva**
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Klikněte na název pravidla. Toto otevře stránku nastavení pravidel.
4. Nakonfigurujte nastavení pravidla dle potřeby. Nastavení jsou uspořádána v následujících sekcích:
   - Hlavní
   - HVI
   - Antimalware
   - Sandbox Analyzer
   - Firewall
   - Ochrana sítě
   - Patch Management
   - Kontrola aplikací
   - Kontrola zařízení
   - Relay
   - Exchange Ochrana
   - Šifrování
   - NSX
   - Ochrana Úložiště
   - Senzor incidentů

Pohybujte se mezi sekcemi pomocí menu na levé straně stránky.

5. Klikněte na **Uložit** pro uložení změn a jejich aplikaci na cílové počítače. Pro opuštění stránky pravidel bez uložení změn klikněte na **Zrušit**.

Poznámka
Pro naučení se práci s pravidly se odkažte na „Přiřazování pravidel“ (str. 213).

7.2.1. Hlavní

Obecná nastavení vám umožňují spravovat možnosti zobrazení uživatelského rozhraní, ochranu hesel, proxy nastavení, nastavení pokročilého uživatele, možnosti komunikace a preference pro aktualizace pro cílové koncové body.

Nastavení jsou uspořádána do následujících sekcí:

- Podrobnosti
- Upozornění
- Nastavení
- Komunikace
- Aktualizace
- Bezpečnostní telemetrie

Podrobnosti

Stránka **Podrobnosti** obsahuje obecné podrobnosti pravidel:

- Název politiky
- Uživatel, který pravidlo vytvořil
- Datum a čas, kdy bylo pravidlo vytvořeno
- Datum a čas, kdy bylo právo naposledy upraveno

Pravidla pro počítače a virtuální stroje

Můžete oprávnění přejmenovat zadáním nového jména do příslušného pole a následným kliknutím na tlačítko **Uložit** ve spodní části stránky. Pravidla by měla mít definující jména, aby jste je vy nebo jiný administrátor mohli snadno rozpoznat.

Poznámka
Ve výchozím nastavení může pravidla upravovat pouze uživatel, který je vytvořil. Pro změnu tohoto nastavení musí autor pravidla označit možnost **Povolit ostatním uživatelům měnit toto pravidlo** ze stránky **Podrobnosti** pravidla.

Dědičná Pravidla

Můžete nastavit oblast, aby dědila od ostatních práv. To uděláte následovně:

1. Vyberte modul a sekci, podle kterého chcete aby současné pravidlo dědilo. Všechny sekce mohou dědit, až na **Všeobecná > Detaily** .
2. Zdejte pravidlo, které chcete aby dědilo ze sekce.
3. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.

Pokud zdrojové pravidlo bude smazáno, vazba dědičnosti a nastavení dědičnosti sekce bude uloženo v child policy.

Dědičná sekce nemůže nadále dědit z ostatních práv Zvažte následující příklad:

Zásada A dědí sekci **Antimalware > Na vyžádání** z práva B. Právo C nemůže dědit sekci **Antimalware > Na vyžádání** z práva A.

Informace o Technické Podpoře

Můžete upravit technickou podporu a kontaktní informace dostupné v bezpečnostní agentovi v okně **About** vyplněním do příslušného pole.

Pro správnou konfiguraci emailové adresy v okně **Informace o (About)**, aby se otevřel standartní emailový klient na koncovém bodu, tak musíte před emailovou

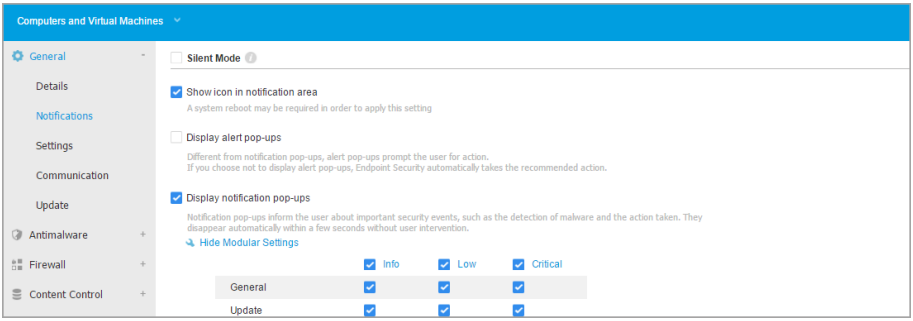
adresu přidat v zadávacím poli **Email** předponu "mailto:". Příklad: `mailto:name@domain.com`.

Uživatelé mohou přistupovat k této informaci z bezpečnostní konzole agenta pravým kliknutím ikony Bitdefender v systémové liště a vybráním **About**.

Upozornění

V této sekci můžete konfigurovat Bitdefender bezpečnostního agenta v uživatelském rozhraní zobrazením nastavení v rozsáhlou a intuitivní cestou.

Pomocí jednoho kliknutí, můžete povolit nebo zakázat celý typ oznámení a nechat jen ty které jsou pro vás opravdu důležité. Také na stejné stránce, můžete spravovat všechny viditelné problémy na koncových zařízeních.



Práva - Zobrazení Nastavení

- **Tichý režim.** Použijte zaškrtávací pole pro Zapnutí nebo vypnutí Tichého módu. Tichý mód je navržen tak, aby vám pomohl k jednoduchému znemožnění interakce uživatele v bezpečnostním agentovi. Pokud zapnete Tichý mód, provedou se následující změny v konfiguraci práv:
  - Možnosti **Zobrazit Ikonu v oznamovací oblasti**, **Zobrazit pop-up notifikaci** a **Zobrazit upozornění pop-upu** v této sekci bude deaktivováno.
  - Pokud úroveň ochrany firewallu byla nastavena na **Ruleset and ask** nebo **Ruleset, known files and ask** bude změněna na **Ruleset, known files and allow**. Jinak, nastavení úrovně ochrany zůstane nezměněné.
- **Zobrazit ikonu v oblasti oznámenání.** Vyberte tuto možnost pro zobrazení ikony Bitdefender v oblasti oznámení (také známé jako systémová lišta) Ikona

informuje uživatele o jejich stavu ochrany měněním její podoby a zobrazováním příslušné pop-up notifikace. Navíc, kliknutím na ni pravým tlačítkem můžete rychle otevřít hlavní okno bezpečnostního agenta nebo okno **About**.

- **Zobrazit pop-up notifikace.** Výstražné pop-ups upozorňují uživatele na bezpečnostní události, které vyžadují pozornost. Pokud se rozhodnete nezobrazovat výstražné pop-ups, bezpečnostní agent automaticky provede doporučená opatření. Výstražné pop-ups jsou generovány v následujících případech:
  - Pokud je firewall nastavený tak, aby vyzval uživatele k akci kdykoli neznámé aplikace požadují přístup k síti nebo internetu.
  - Pokud je Pokročilá ochrana před hrozbami / Systém detekce průniků povolen, pokaždé, když je nalezena potenciálně nebezpečná aplikace.
  - Pokud je povoleno skenování zařízení, pokaždé, když je k počítači připojeno externí paměťové zařízení. Toto nastavení můžete konfigurovat v sekci **Antimalware > Na vyžádání**.
- **Zobrazit pop-up notifikace.** Jiné oproti upozorňujícímu pop-upu, pop-up oznámení informuje uživatele o všelijaké bezpečnostní události. Pop-upy zmizí automaticky během pár vteřin bez zásahu uživatele.

  Zvolte **Zobrazit notifikační pop-upy**, poté klikněte na odkaz **Zobrazit modulární nastavení** a vyberte, o kterých událostech chcete, aby modul informoval uživatele. Existují tři typy notifikačních pop-upů podle míry závažnosti událostí:
  - **Informace**. Uživatelé jsou informováni o významné, ale neškodné bepečnostní události. Například aplikace, která se připojila k internetu.
  - **Nízký**. Uživatelé jsou informováni o důležité bezpečnostní události, která potřebuje pozornost. Například, Skenování při přístupu rozpoznalo hrozbu a soubor byl odstraněn nebo vložen do karantény.
  - **Kritická**. Tyto notifikační pop-upy informují uživatele o nebezpečných situacích, jako když Skenování při přístupu rozpozná hrozbu a výchozí nastavené pravidlo akce je **Nedělat nic**, takže malware je stále přítomen na koncovém bodě, nebo když se nepodaří dokončit aktualizační proces.

  Vyberte zaškrtávací pole spojené se názvem typu pro povolení tohoto typu pop-upu pro všechny moduly najednou. Klikněte na zaškrtávací pole odpovídající jednotlivým modulům pro zapnutí nebo vypnutí specifických notifikací.

Například, po označení polí přiřazených k Sandbox Analyzeru, Bitdefender Endpoint Security Tools klient informuje uživatele o podání souboru k analýze chování.

Seznam modulů se může lišit podle vaší licence.

- **Viditelnost problémů na koncových bodech.** Na základě stavových výstrah uživatelé vyhodnotí, kdy má jejich koncový bod problémy s nastavením zabezpečení nebo jiné bezpečnostní hrozby. Například, uživatelé uvidí každý problém týkající se jejich antimalwarové ochrany, jako je: modul Skenování při přístupu je vypnutý nebo Kompletní systémový sken je opožděný. Uživatelé jsou informováni o jejich stavu ochrany dvěma způsoby:
  - Kontrolou stavové oblasti hlavního okna, kde je zobrazena příslušná zpráva o stavu, a mění barvu podle závažnosti bezpečnostních problémů. Uživatelé mohou také prohlížet podrobnosti o problémech kliknutím na příslušné tlačítko.
  - Kontrolou ikony Bitdefender na systémové liště, která změní svůj vzhled v případě rozpoznaných problémů.

  Bezpečnostní agent Bitdefender používá v notifikační oblasti následující barevné schéma:
  - Zelená: Nebyly nalezeny žádné problémy.
  - Žlutá: Koncový bod má nekiritické problémy, které mají vliv na jeho zabezpečení. Uživatelé nemusí přerušovat jejich současnou práci pro vyřešení daného problému.
  - Červená: Koncový bod má problémy, které vyžadují okamžitý zásah uživatele.

  Zvolte **Viditelnost problémů na koncovém bodě**, poté klikněte na odkaz **Zobrazit modulární nastavení** a upravujte stavové výstrahy zobrazené v uživatelském rozhraní agenta Bitdefender.

  Pro každý modul můžete zvolit, zda zobrazovat výstrahy jako varování nebo kritický problém, nebo je nezobrazovat vůbec. Možnosti jsou vysvětleny zde:
  - **Obecné**. Stavová výstraha je generována pokaždé, když je nutné restartovat systém během nebo po instalaci produktu, a také, když se bezpečnostní agent nemohl připojit k Bitdefender cloudovým službám.
  - **Antimalware**. Stavové výstrahy jsou generovány v následujících případech:

- Skenování při přístupu je zapnuté, ale mnoho lokálních souborů je přeskočeno.
- Uplynul určitý počet dní od posledního provedení kompletního skenování systému stroje.

  Můžete zvolit, jak zobrazovat výstrahy a určit počet dní od posledního systémového skenu.
- Restartování je nutné pro dokončení dezinfikačního procesu.

– **Firewall**. Tato stavová výstraha je generována, když je modul Firewall vypnutý.

– **Application Control**. Ten to status upozornění je generován, když modul Řízení Aplikací je upraven.

– **Kontrola obsahu**. Tato stavová výstraha je generována, když je modul Kontrola obsahu vypnutý.

– **Aktualizace**. Stavová výstraha je generována pokaždé, když je nutné restartování systému pro dokončení aktualizace.

- **Oznámení o Restartu Koncového zařízení.** Tato volba zobrazí hlášku upozornění ohledně restartu na koncovém bodu pokaždé, když je potřeba provést systémový restart kvůli provedeným změnám na koncovém bodu v GravityZone modulech vybraných v modulárních nastaveních.

  Poznámka
  Koncové body, které potřebují restartovat mají specifickou stavovou ikonu ( ) v inventáři GravityZone.

  Upozornění na restart můžete dále přizpůsobit kliknutím na **Show modular settings**. K dispozici jsou následující možnosti:

  – **Update** - Tuto možnost vyberte, chcete-li aktivovat agenta pro upozornění na restart po aktualizaci.

  – **Patch Management** - Tuto možnost vyberte, chcete-li aktivovat upozornění o restartu po instalaci opravy.

  Poznámka
  Můžete také nastavit limit, o kolik hodin může uživatel odložit restart. Chcete-li, vyberte **Auto-restart machine after** a vložte hodnotu od 1 do 46.

Upozornění na restart potřebuje aby si uživatel vybral některou z následujících akcí:

- **Restart teď (Reboot now)**. V tomto případě, se systém restartuje okamžitě.
- **Odložit restart**. V takovém případě se bude pravidelně zobrazovat oznámení o restartu, dokud uživatel nerestartuje systém nebo dokud neuplyne čas stanovený správcem společnosti.

Nastavení

V této sekci můžete konfigurovat následující parametry:

- **Konfigurace hesla.** Abyste zabránili uživatelům s oprávněními správce v odinstalování zabezpečení, musíte nastavit heslo.

  Heslo pro odinstalaci lze nastavit před instalací upravením instalačního balíčku. Pokud jste tak učinili, zvolte **Ponechat instalační nastavení** pro zachování současného hesla.

  Pro nastavení hesla nebo pro změnu současného hesla zvolte **Povolit heslo** a zadejte požadované heslo. Pro odstranění zabezpečení heslem, zvolte **Zrušit heslo**.

- **Nastavení Proxy**

  Pokud je vaše síť za serverem proxy, musíte určit proxy nastavení, která umožní vašim koncovým bodům komunikovat s komponenty řešení GravityZone. V tomto případě musíte povolit možnost **Nastavení proxy** a vyplnit požadované parametry:
  - **Server** - zadejte IP proxy serveru
  - **Port** - zadejte port, který slouží k připojení k proxy serveru.
  - **Uživatelské jméno** - zadejte uživatelské jméno rozpoznávané proxy serverem.
  - **Heslo** - zadejte platné heslo pro určeného uživatele

- **Pokročilý uživatel**

  Modul Pokročilý uživatel aktivuje administrátorská práva na uživatelské úrovni, čímž umožní uživateli koncového bodu přístup a možnost úpravy bezpečnostních nastavení prostřednictvím lokální konzole skrze uživatelské rozhraní Bitdefender Endpoint Security Tools.

  Pokud chcete určitým koncovým bodům udělit oprávnění pokročilého uživatele, musíte tento modul nejprve zahrnout v bezpečnostním agentovi nainstalovaném

na cílových koncových bodech. Poté musíte nastavit Nastavení pokročilého uživatele v pravidlech aplikovaných na tyto koncové body:

Důležité
Modul Pokročilý uživatel je dostupný pouze pro počítače a servery s podporovaným systémem Windows.

1. Povolte možnost **Pokročilý uživatel**.
2. V polích níže definujte heslo Pokročilého uživatele.

   Uživatelé, kteří přistupují do módu Pokročilého uživatele z místního koncového bodu budou vyzváni k zadání určeného hesla.

Pro přístupu k modulu Pokročilý uživatel musí uživatelé kliknout pravým tlačítkem na ikonu Bitdefender na jejich systémové liště a z kontextového menu zvolit **Pokročilý uživatel**. Po zadání hesla v přihlašovacím okně se zobrazí konzole obsahující současně aplikované nastavení pravidel, ve které koncový uživatel může prohlížet a upravovat nastavení pravidel.

Poznámka
Pouze některé bezpečnostní funkce umožňují lokální přístup prostřednictvím konzole Pokročilého uživatele, což se týká modulů Antimalware, Firewall, Kontrola obsahu a Kontrola zařízení.

Pro navrácení změn provedených v režimu Pokročilého uživatele:

– V Control Center otevřete šablonu pravidel přiřazenou ke koncovému bodu s oprávněními Pokročilého uživatele a klikněte na **Uložit**. Tímto způsobem budou ke koncovému bodu znovu přiřazena původní nastavení.
– Přiřaďte nová pravidla ke koncovému bodu s oprávněními Pokročilého uživatele.
– Přihlašte se k místnímu koncovému bodu, otevřete konzoli Pokročilý uživatel a zvolte **Resync**.

Pro snadné nalezení koncových bodů s pravidly upravenými v režimu Pokročilého uživatele:

– Na stránce **Síť** klikněte na nabídku **Filtry** a zvolte možnost **Upraveno pokročilým uživatelem** z karty **Pravidla**.

– Na stránce **Síť** klikněte na požadovaný koncový bod pro zobrazení **Informačního** okna. Pokud bylo pravidlo upraveno v režimu Pokročilého uživatele, v sekci **karta Obecné** > **Pravidla** se zobrazí upozornění.

> **Důležité**
> Modul Pokročilý uživatel je speciálně navržený pro řešení problémů, čímž umožňuje správci sítě snadné prohlížení a měnění pravidel na místních počítačích. Přiřazení oprávnění Pokročilého uživatele ostatním uživatelům ve společnosti musí být omezeno pouze na oprávněné osoby pro zaručení, že bezpečnostní pravidla budou vždy aplikována na všechny koncové body ve firemní síti.

- **Nastavení**

  V této sekci můžete konfigurovat následující parametry:

  – **Odstranit události starší než (dní).** Bezpečnostní agent Bitdefender vede podrobný záznam událostí svých aktivit na vašem počítači (včetně činností monitorovaných Kontrolou obsahu.) Ve výchozím nastavení jsou události ze seznamu mazány po 30 dnech. Pokud chcete tento interval změnit, zvolte jinou možnost z nabídky.

  – **Odesílání hlášení o selhání pro Bitdefender.** Zvolte tuto možnost, aby v případě selhání bezpečnostního agenta byla odeslána hlášení do laboratoří společnosti Bitdefender. Hlášení pomohou našim technikům při zjišťování příčiny problému a při zabraňování v jeho opětovném výskytu. Nebudou odeslány žádné osobní informace.

  – **Odeslat podezřelé spustitelné soubory k analýze.** Zvolte tuto možnost, aby podezřele vyhlížející soubory nebo soubory vykazující podezřelé chování byly odesílány do Laboratoří společnosti Bitdefender na analýzu.

  – **Nahlaste narušení paměti HVI společnosti Bitdefender.** Dle výchozího nastavení HVI odesílá anonymní informace ohledně zjištěných narušení Cloudovým serverům Bitdefender, aby byly použity pro statistiku a vylepšení míry detekce produktu. Můžete tuto možnost odškrtnou pokud nechcete posílat informace o vaší síti.

  > **Poznámka**
  > Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Komunikace

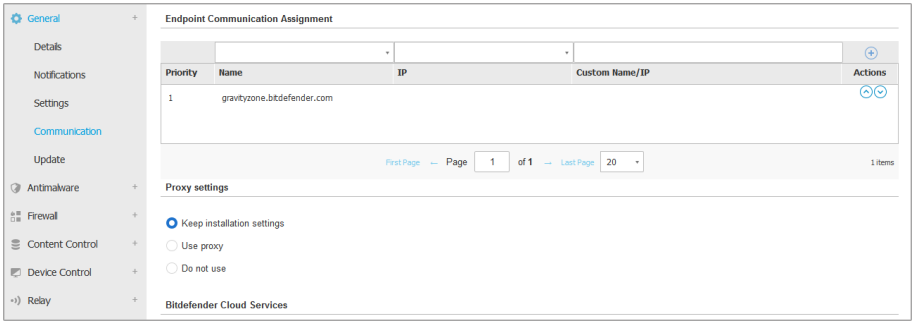
V této sekci můžete přiřadit jedno nebo více relay zařízení k cílovým koncovým bodům, a poté konfigurovat nastavení proxy pro komunikaci mezi koncovými body a GravityZone.

Přiřazení komunikace s koncovým bodem

Pokud je na zařízení GravityZone nainstalováno několik informačních serverů, můžete cílovým počítačům přiřadit jeden nebo několik komunikačních serverů prostřednictvím pravidla. V potaz jsou brány také dostupné relay koncové body, které fungují jako komunikační servery.

Pro přiřazení komunikačních serverů k cílovým počítačům:

1. V tabulce **Přiřazení komunikace s koncovým bodem** klikněte na pole **Název**. Zobrazí se seznam zjištěných komunikačních serverů.
2. Zvolte jednotku.



Politiky Počítačů a Virtuálních Strojů - Komunikační nastavení

3. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.

   Komunikační server bude přidán do seznamu. Všechny cílové počítače budou komunikovat s Control Center prostřednictvím zvoleného komunikačního serveru.
4. Postupujte stejným způsobem por přidání více komunikačních serverů, pokud jsou k dispozici.
5. Prioritu komunikačních serverů můžete nastavit pomocí směrových šipek nahoru a dolů, které najdete na pravé straně každé položky. Komunikace s cílovými počítači bude prováděna prostřednictvím jednotky uvedené na prvním místě v

seznamu. Pokud se nepodaří provést komunikaci s touto jednotkou, v potaz bude brána ta následující.

6. Pro odstranění jedné jednotky ze seznamu, klikněte na odpovídající tlačítko ⊗ **Odstranit** na pravé straně tabulky.

Komunikace mezi koncovými body a relayi / GravityZone

V této sekci můžete nastavit preference proxy pro komunikaci mezi cílovými koncovými body a přiřazenými relay stroji, nebo mezi cílovými koncovými body a GravityZone (v případě, že nebyl přiřazen žádný relay):

- **Ponechat instalační nastavení** pro použití stejných nastavení proxy, která jsou definována v instalačním balíčku.
- **Použít proxy definovanou v sekci Obecné** pro použití nastavení proxy definovaného v současném pravidle pod sekcí **Obecné > Nastavení**.
- **Nepoužívat**, když cílové koncové body nekomunikují s určitými komponenty GravityZone přes proxy.

Komunikace mezi koncovými body a Cloudovými službami

V této sekci můžete nastavit preference proxy pro komunikaci mezi cílovými koncovými body a Cloudovými službami Bitdefender (vyžaduje připojení k internetu).

- **Ponechat instalační nastavení** pro použití stejných nastavení proxy, která jsou definována v instalačním balíčku.
- **Použít proxy definovanou v sekci Obecné** pro použití nastavení proxy definovaného v současném pravidle pod sekcí **Obecné > Nastavení**.
- **Nepoužívat**, když cílové koncové body nekomunikují s určitými komponenty GravityZone přes proxy.

Aktualizace

Aktualizace jsou velmi důležité, protože pomáhají v obraně proti nejnovějším hrozbám. Bitdefender zveřejňuje všechny aktualizace obsahu produktů a zabezpečení prostřednictvím serverů Bitdefender na internetu. Všechny aktualizace jsou šifrované a digitálně podepsané, aby s nimi nemohlo být manipulováno. Jakmile je k dispozici aktualizace, bezpečnostní agent Bitdefender kontroluje její signaturu pro autenticitu a obsah balíčku pro neporušenost. Poté je každý soubor aktualizace rozebrán a jeho verze je porovnána s nainstalovanou verzí. Novější soubory jsou staženy lokálně a porovnány s jejich MD5 hashem pro zajištění, že nejsou měněny.

V této sekci můžete konfigurovat Bitdefender bezpečnostního agenta a nastavení aktualizace obsahu zabezpečení.

Politiky Počítačů a Virtuálních Strojů - možnost Aktualizace

- **Aktualizace produktu.** Bezpečnostní agent Bitdefender automaticky kontroluje dostupnost, stahuje a instaluje aktualizace každou hodinu (výchozí nastavení). Automatické aktualizace probíhají tiše na pozadí.
  - **Opakování**. Pro změnu automatického opakování aktualizací zvolte z nabídky jinou možnost a nastavte ji dle svých potřeb v následných polích.
  - **Odložit restart**. Aby se mohly nainstalovat a správně fungovat, některé aktualizace vyžadují restartování systému. Ve výchozím nastavení bude počítač nadále pracovat se starými soubory, dokud není restartován, a poté aplikuje nejnovější aktualizace. Upozornění v uživatelském rozhraní vybídne uživatele k restartování systému kdykoli to bude aktualizace vyžadovat. Doporučujeme ponechat tuto možnost povolenou. V opačném případě se systém automaticky restartuje po instalaci aktualizace, která vyžaduje restart. Uživatelé budou vyzváni k uložení své práce, ale restartování nemůže být zastaveno.
  - Pokud se rozhodnete restartování odložit, můžete pro restartování počítačů zvolit vhodnější čas, kdy se restartují automaticky, pokud je to (stále) potřeba. Toto může být velmi užitečné pro servery. Zvolte **Pokud potřebné, restartovat po instalaci aktualizací** a určete, kdy je restartování vhodné (denně nebo každý týden v určitý den, v určitý čas).
  - Chcete-li získat větší kontrolu nad změnou konfigurace a aktualizací fázovacího procesu, můžete nakonfigurovat BEST agenta na vašich počítačích se systémem Linux, aby spouštěl aktualizace modulu jádra EDR prostřednictvím **Aktualizace produktu** .

    Když je zaškrtnuto políčko **Aktualizace produktu** :

    - Pokud zaškrtnete políčko **Aktualizovat moduly Linux EDR pomocí aktualizace produktu** , GravityZone aktualizuje verze jádra prostřednictvím **Aktualizace produktu** .
    - Pokud necháte tuto možnost vypnutou, verze jádra budou aktualizovány prostřednictvím **Aktualizace bezpečnostního obsahu** .

Poznámka
Pokud zaškrtnete políčko **Aktualizovat moduly Linux EDR pomocí aktualizace produktu** , ale zakážete možnost **Aktualizace produktu** , moduly Linux EDR nebudou aktualizováno.

- **Aktualizace obsahu zabezpečení.** Bezpečnostní obsah označuje statické a dynamické prostředky detekce hrozeb, jako jsou například skenovací enginy, modely strojového učení, heuristika, pravidla, signatury a černé listiny. Bezpečnostní agent Bitdefender automaticky vyhledává aktualizace signatur každou hodinu (výchozí nastavení). Automatické aktualizace probíhají tiše na pozadí. Pro změnu automatického opakování aktualizací zvolte z nabídky jinou možnost a nastavte ji dle svých potřeb v následných polích.
- **Umístění aktualizací**. Výchozí aktualizační umístění bezpečnostního agenta Bitdefender je místní aktualizační server GravityZone. Přidejte umístění aktualizací buď zvolením z předem definovaných umístění z rozbalovací nabídky, nebo přidáním IP nebo jména hosta jednoho nebo více aktualizačních serverů ve vaší síti. Nastavte jejich prioritu použitím směrových šipek nahoru a dolů, které se zobrazí při ukázání myší. Pokud je první umístění aktualizací nedostupné, bude použito to další, a tak dále.

  Pro nastavení místní aktualizační adresy:

  1. Zadejte adresu aktualizačního serveru do pole **Přidat umístění**. Můžete:
     - Zvolte předem definované umístění.
       - **Relay servery**. Koncový bod se automaticky připojí k přiřazenému relay serveru.

         Varování
         Relay servery nejsou podporovány na legacy operačních systémech. Více informací naleznete v Instalační příručce.

         Poznámka
         Přiřazený Relay server můžete prohlížet v okně **Informace**. Pro další podrobnosti se podívejte na Prohlížení podrobností o počítači.

       - **Lokální aktualizační server**
     - Zadejte IP nebo jméno hosta jednoho nebo více aktualizačních serverů ve vaší síti. Použijte jednu z těchto syntaxí:

- `update_server_ip:port`
- `update_server_name:port`

Výchozí port je 7074.

Pole **Používat servery Bitdefender jako záložní umístění** je ve výchozím stavu označeno. Pokud jsou aktualizační umístění nedostupná, bude použito záložní umístění.

Varování
Vypnutí záložního umístění zastaví automatické aktualizace, čímž v případě, že jsou uvedená umístění nedostupná, ponechá vaši síť zranitelnou.

2. Pokud se klientské počítače připojují k lokálnímu aktualizačnímu serveru prostřednictvím proxy serveru, zvolte **Použít proxy**.
3. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.
4. Použijte šipky ⌃ Nahoru / ⌄ Dolů ve sloupci **Akce** pro nastavení priority definovaných aktualizačních umístění. V případě, že je první aktualizační umístění nedostupné, v potaz bude bráno to následující, a tak dále.

Klikněte na odpovídající tlačítko ⊗ **Odstranit** pro odstranění umístění ze seznamu. Přestože výchozí aktualizační umístění můžete odebrat, nedoporučujeme to.

- **Aktualizační okruh.** Aktualizace produktů můžete provádět ve fázích pomocí aktualizačních kruhů:
  - **Pomalý kruh**. Stroje s pravidlem pomalého kruhu obdrží aktualizace v pozdějším datu, podle odpovědi, kterou obdrží od koncových bodů s rychlým kruhem. Je to preventivní opatření v aktualizačním procesu. Toto je výchozí nastavení.
  - **Rychlý kruh**. Stroje s pravidlem rychlého kruhu obdrží ty nejnovější dostupné aktualizace. Toto nastavení je doporučeno pro nekritické stroje ve výrobě.

Důležité
- V nepravděpodobném případě, že na rychlém kruhu na strojích s určitým nastavením dojde k problému, tento problém bude napraven před aktualizací na pomalém kruhu.
- BEST for Windows Legacy nepodporuje staging. Legacy koncové body v staging lokaci musí být přeneseny do produkční lokace.

Bezpečnostní telemetrie

Poznámka
Tato funkce vyžaduje licenci EDR a je k dispozici pouze pro koncové body Windows.

S telemetrií zabezpečení máte přístup k základním datům souvisejícím s událostmi zabezpečení, abyste mohli vytvářet vlastní korelace.

Aby byl zajištěn optimální výkon a stopa dat, agenti odesílají pouze události relevantní pro zabezpečení vaší sítě. Takové události se týkají:

- Procesy: vytvořit, ukončit
- Soubory: vytvořit, číst, upravit, přesunout, smazat
- Registr: vytvořit a smazat klíče, upravit a smazat hodnotu
- Přístup uživatele: přihlášení
- Síťové připojení

Agent Bitdefender odesílá tyto informace ve standardním průmyslovém formátu (JSON, CEF) přímo do vámi používaného řešení SIEM.

Chcete-li odeslat události zabezpečení z cílových koncových bodů do řešení SIEM, nakonfigurujte zásadu následujícím způsobem:

- Zaškrtnutím políčka **Telemetrie zabezpečení** funkci povolíte.
- Vyberte řešení SIEM, ke kterému se chcete připojit.
- Zadejte adresu URL serveru SIEM.

  Varování
  Je vyžadován protokol HTTPS s TLS 1.2 nebo vyšší. Jinak se odeslání události nezdaří.

- Zadejte autorizační token, který zajišťuje připojení.
- V části **Komunikace mezi koncovými body a SIEM** zvolte, zda použít proxy server.

  Poznámka
  Agent používá pro komunikaci se SIEM stejný proxy server jako pro komunikaci s GravityZone. Jeho nastavení můžete zkontrolovat v sekci **Obecná Nastavení** .

Jakmile se zásada použije na koncové body, agent začne odesílat události tak, jak se vyskytnou, na nakonfigurovaný server SIEM.

7.2.2. HVI

Poznámka
HVI poskytuje ochranu pouze pro virtuální stroje na Citrix Xen hypervizorech. Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Hypervisor Memory Introspection chrání virtuální stroje proti pokročilým hrozbám, se kterými si stroje na základě signatur neumí poradit. Zajišťuje detekci útočníků v reálném časem, monitorováním procesů ze vnějšího hostujícího operačního systému. Ochranný mechanizmus zahrnuje několik možností pro blokování útoků hned jak mile se stanou a okamžitě odstraní hrozbu.

V souladu s principem oddělení paměti operačních systémů, HVI zahrnuje dva ochranné moduly uspořádané v souvisejících kategoriích:

- User Space, adresuje normální procesy uživatelských aplikací.
- Kernel Space, adresuje procesy rezervované pro jádro operačního systému.

Navíc, pravidla HVI zahrnují dvě funkce, které vám pomáhají při správě zabezpečení a udržování chráněných virtuálních strojů:

- Exclusions, pro zobrazení a spravování procesů vyjmutých ze skenování.
- Custom Tools, pro připojované nástroje, které jsou nezbytné v operačních a forenzních aktivitách, uvnitř hostitelských operačních systémech.

Uživatelský Prostor

V této sekci můžete konfigurovat ochranná nastavení pro běžící procesy v prostoru paměti pro uživatele.

Použijte zaškrtávací pole **User Space Memory Introspection** pro povolení nebo zakázaní ochrany.

Funkcionalita tohoto modulu spoléhá na pravidlech, povoluje vím konfigurovat ochranu odděleně mezi různými skupinami procesů. Navíc, můžete vybrat možnost sbírání podrobnějších forenzních informací.

- Pravidla Uživatelského Prostředí
- Forenzní Informace

Pravidla Uživatelského Prostředí

Modul přijde se předdefinovanými pravidly, které adresují nejvíce zranitelné aplikace. Tabulka v této sekci uvádí existující pravidla, poskytuje důležité informace o každé z nich:

- Jméno pravidla
- Procesy pravidla se aplikují k
- Monitorování
- Akci, které blokuje detekované útoky
- Akce ke smazání hrozby

Také můžete poskytnout seznam vlastních pravidel pro procesy, které chcete monitorovat. Pro vytvoření nového pravidla:

1. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Tato akce otevře konfigurační okno pravidla.
2. Nakonfigurujte modul podle následujících nastavení pravidel:
   - **Rule name.** Zadejte název pod kterým bude pravidlo uvedeno v tabulce pravidel. Například, pro procesy jako `firefox.exe` nebo `chrome.exe`, můžete pojmenovat pravidlo `Browsers`.
   - **Processes.** Zadejte název procesů, které chcete sledovat a oddělte je středníkem (;).
   - **Monitoring mode.** Pro rychlou konfiguraci, klikněte na úroveň zabezpečení, která nejvíce vyhovuje vaším požadavkům (**Aggressive**, **Normal** nebo **Permissive**). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

     Můžete konfigurovat nastavení modulu detailně vybraním **Custom** úrovně ochrany a vybráním jedné nebo vice z následujících možností:
     - **Hooks nastaveny na kritický uživatelský režim DLLs.** Detekujte injekce DLL, které nahrávají škodlivý kód do procesu volání.
     - **Unpacking/decrypting attempts in the main executable.** Detekoval pokus o rozluštění kódu v hlavním spouštěcím procesu a ochránil proces před pozměněním za škodlivé instrukce.
     - **Foreign writes inside the target process.** Chrání před infikováním kódu ve chráněných procesech.

- **Exploits.** Detekoval podivné chování procesu způsobené exploitem bugu nebo předchozí nevyřešenou zranitelností. Použijte tuto možnost pokud chcete monitorovat spuštění kódu z haldy nebo stacku chráněných aplikací.
- **Hooking pro WinSock.** Blokujte zásahy do síťových knihoven (DLL) využívaných operačním systémem a zajistěte tak bezproblémovou TCP/IP komunikaci.

- **Akce.** Je několik akcí, které můžete provádět na odhalených hrozbách. Každá akce má, jakmile přijde na řadu, několik proveditelných možností nebo sekundárních akcí. Jejich popis naleznete níže:
  - **Primary action.** Toto je okamžitá akce, kterou můžete použít, při zjištění útoku na hostitelský stroj. umožní vám ho zablokovat. Zde jsou dostupné možnosti:
    - **Protokol.** Zaznamenat pouze událost v databázi. V tomto případě obdržíte pouze upozornění (pokud je nastaveno) a incident si budete moci prohlédnout v hlášení **Činnosti HVI**.
    - **Deny.** Odmítá jakýkoliv pokus hrozby k ovlivnění cílového procesu.
    - **Shut Down Machine.** Vypne virtuální stroj na kterém je cílový proces spuštěn.

      Důležité
      Je doporučeno nastavit primární akci nejprve na **Protokol**. Poté po nějakou dobu používejte zásady, abyste měli jistotu, že všechno funguje podle vašich představ. Později, můžete vybrat kteroukoliv akci chcete, aby byla provedena v případě detekce narušení paměti.

  - **Nápravná opatření.** V závislosti na zvolené možnosti, Security Server zavede nástroj pro nápravu na hostitelský operační systém. Nástroj automaticky startuje skenování proti malware a poté proti detekovaným hrozbám, proběhne přesně podle vybrané akce. Zde jsou dostupné možnosti:
    - **Disinfect.** Odebere škodlivý kód ze infikovaného souboru. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech.

- **Odstranit.** Odstraní odhalené soubory z disku, bez jakéhokoli upozornění. Této akci se doporučujeme vyhýbat.
- **Ignorovat.** Nástroj pro nápravu detekuje a hlásí pouze detekované soubory.
- **None.** Nápravný nástroj se nebude plést do hostujícího operačního systému.

> **Poznámka**
> Zavření nástroje ho také odstraní z hostitelského operačního systému, a nezanechá v něm po sobě žádné stopy.

– **Backup remediation action.** Jakmile akce nápravy neuspěje, můžete vybrat jinou možnost nápravy z dostupných možností.

3. Klikněte na tlačítko **Save**.

Jakmile je vytvořeno, můžete pravidlo kdykoli upravovat. Kliknutím na název pravidla otevřete konfigurační okno.

GravityZone také vám umožňuje rychle konfigurovat chování Pamětní Introspekce při detekci, změněním několika pravidel najednou. Pro nastavení několika pravidel s těmi samými akcemi:

1. Vyberte pravidla, která chcete změnit.
2. Klikněte na tlačítko **Action and Remediation** v horní části tabulky.
3. Pro každou akci vyberte tu možnost, kterou chcete.
4. Klikněte na tlačítko **Save**. Nová opatření budou uplatněna okamžitě po uložení zásady, za předpokladu, že jsou cílová zařízení online.

Pro odstranění jednoho nebo více pravidel ze seznamu, vyberte je a poté klikněte na tlačítko ⊗ **Delete** v horní části tabulky.

Forenzní Informace

Vyberte zaškrtávací pole **Application crash events** pod tabulkou s pravidly uživatelského rozhraní pro povolení sbírání detailních informací, když jsou aplikace ukončovány.

Tyto informace si můžete prohlédnout v hlášení o Činnosti HVI a najít příčinu, která způsobila ukončení aplikace. Pokud událost je podobná útoku, její detaily se zobrazí

seskupené s dalšími událostmi pod příslušným incidentem, který vedl k danné události.

Prostor jádra

HVI chrání klíčové prvky operačního systému, jako jsou například:

- Důležité ovladače Kernelu a přidružené ovladače objektů, vyžadují rychlí I/O odesílaní tabulek společně se základními ovladači.
- Ovladače sítě, jejichž změna by mohla umožnit malwaru narušení provozu a zavedení škodlivých komponentů do přenosového proudu.
- Obraz jádra operačního systému, včetně následujících: kódová sekce, datová sekce a sekce pouze pro čtení, včetně Tabulky importovaných adres (IAT), Tabulky exportovaných adres (EAT) a zdrojů.

V této sekci můžete konfigurovat nastavení ochrany pro procesy spuštěné v jádrové paměti.

Použijte zaškrtávací pole **Introspekce jádrové paměti** pro povolení nebo zakázaní ochrany.

Pro rychlou konfiguraci klikněte na úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (**Agresivní**, **Normální** nebo **Tolerantní**). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

Můžete konfigurovat nastavení modulu detailně vybraním **Custom** úrovně ochrany a vybráním jedné nebo vice z následujících možností:

- **Kontrolní registry**. Kontrolní registry (CR) jsou procesorové registry, které kontrolují obecné chování procesoru nebo jiných digitálních zařízení. Vyberte tuto možnost pro detekci pokusů o načtení neplatných hodnot do určitých Kontrolních registrů.
- **Registry specifické podle modelu**. Tyto registry odkazují ke kterémukoli z různých kontrolních registrů v sadě x86 pro debugging, sledování spouštění programů, monitorování výkonu počítače, a přepínání určitých funkcí procesoru. Vyberte tuto možnost pro detekci pokusů o změnu těchto registrů.
- **Integrita IDT/GDT**. Globální nebo Tabulky deskriptorů přerušení (IDT/GDT) jsou používány procesorem pro určení správné odezvy na přerušení a výjimky. Vyberte tuto možnost pro detekci všech pokusů o změnu těchto tabulek.
- **Ochrana antimalwarových ovladačů.** Vyberte tuto možnost pro detekci pokusů o změnu ovladačů používaných antimalwarovým softwarem.

- **Ochrana ovladačů Xen.** Vyberte tuto možnost pro detekci pokusů o změnu ovladačů Citrix XenServer hypervisor.

Na odhalené hrozby můžete uplatnit několik možných akcí. Každá akce má, jakmile přijde na řadu, několik proveditelných možností nebo sekundárních akcí. Jejich popis naleznete níže:

- **Primární akce.**
  - **Protokol.** Zaznamenat pouze událost v databázi. V tomto případě obdržíte pouze upozornění (pokud je nastaveno) a incident si budete moci prohlédnout v hlášení **Činnost Introspekce paměti**.
  - **Deny.** Odmítá jakýkoliv pokus hrozby k ovlivnění cílového procesu.
  - **Shut Down Machine.** Vypne virtuální stroj na kterém je cílový proces spuštěn.

  Důležité
  Je doporučeno nastavit primární akci nejprve na **Protokol**. Poté po nějakou dobu používejte zásady, abyste měli jistotu, že všechno funguje podle vašich představ. Později, můžete vybrat kteroukoliv akci chcete, aby byla provedena v případě detekce narušení paměti.

- **Nápravné opatření.**
  - **Disinfect.** Odebere škodlivý kód ze infikovaného souboru. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech.
  - **Odstranit.** Odstraní odhalené soubory z disku, bez jakéhokoli upozornění. Této akci se doporučujeme vyhýbat.
  - **Ignorovat.** Nástroj pro nápravu detekuje a hlásí pouze detekované soubory.
  - **None.** Nápravný nástroj se nebude plést do hostujícího operačního systému.
- **Backup remediation action.** Jakmile akce nápravy neuspěje, můžete vybrat jinou možnost nápravy z dostupných možností.

Můžete si také zvolit sběr informací, které obohatí údaje podávané forenzním týmům. Označte zaškrtávací pole **Události selhání operačního systému** a **Události ovladače** pro povolení sběru informací týkajících se selhání hostitelských operačních systémů, nebo událostí vyvolaných přídatnými moduly načtenými operačním systémem. Tyto události, předcházející problému, pomohou forenznímu vyšetřování v rychlejším odhalení kořenové příčiny útoku.

Tyto události jsou seskupeny v hlášení o Činnosti HVI pod incidentem, který je zapříčinil.

Výjimky

GravityZone vám umožňuje vyloučit procesy ze skenování HVI pomocí **Blokovaných aplikací** a hlášení o **Činnosti HVI**. V sekci **Výjimky** jsou shromažďovány všechny tyto procesy ze zmíněných hlášení a jsou zobrazeny ve formě tabulky.

Pro každý vyloučený proces si můžete prohlédnout komentář s důvodem pro vyloučení.

Pokud si to ohledně některého z vyloučených procesů rozmyslíte, klikněte na tlačítko **Odstranit** v horní části tabulky, a proces bude zahrnut v příštích skenováních.

Vlastní nástroje

V této sekci můžete nastavit zavádění nástrojů dovnitř cílových hostitelských operačních systémů. Tyto nástroje musí být před použitím nahrány do GravityZone. Další informace viz „Zavedení vlastních nástrojů s HVI“ (str. 532).

Pro nastavení zavádění:

1. Použijte zaškrtávací pole **Aktivovat zavádění** pro povolení nebo zakázání funkce.
2. Pro přidání nového nástroje klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.
3. Vyberte nástroj, který chcete použít, z rozbalovací nabídky **Výběr nástroje**.

   Tyto nástroje byli předtím nahrány do GravityZone. Pokud nemůžete najít správný nástroj v seznamu, přejděte do **Tools Management Center** a odtud je přidejte. Další informace viz „Zavedení vlastních nástrojů s HVI“ (str. 532).
4. Pod **Popisem nástroje** zadejte zamýšlené využití nástroje nebo jakékoli jiné informace, které shledáte užitečnými.
5. Zadejte příkazovou řádku nástroje, společně se všemi potřebnými parametry, stejně jako v Příkazovém Řádku nebo Terminálu. Například:

   ```
   bash script.sh <param1> <param2>
   ```

   .

   Pro BD Remediation Tools můžete vybrat pouze nápravu akce a zálohovat nápravnou akci ze dvou rozbalujících menu.

6. Umístění od kut Security Server by měl získávat logy:
   - **stdout**. Vyberte toto zaškrtávací pole pro získávání logů ze standardního odchozího komunikačního kanálu.
   - **Output file**. Vyberte toto zaškrtávací pole pro sbírání souborů logu na koncových zařízeních. V tomto případě, potřebujete zadat cestu, kde Security Server nalezne soubor. Můžete použít absolutní cesty nebo systémové proměnné.

     Zde jsou dvě volitelné možnosti navíc:

     a. **Odstranit soubory protokolu z hosta, jakmile byly přesunuty**. Vyberte tuto možnost, pokud již nepotřebujete soubory na koncovém zařízení.

     b. **Přesunout protokoly na**. Vyberte tuto možnost pro přesunutí protokolového souboru z Security Server do jiného umístění. V tomto případě musíte uvést cestu k cílovému umístění a autorizační pověření.
7. Zvolte, čím bude spuštění zavádění vyvoláno. K dispozici jsou následující možnosti:
   - **Poté, co je na hostitelském virtuálním zařízení zjištěno narušení.** Nástroj je zaveden okamžitě, jakmile je na virtuálním stroji nalezena hrozba.
   - **Podle zvláštního plánu.** Použijte možnosti plánování pro nastavení zaváděcího plánu. Můžete nastavit nástroj tak, aby byl spouštěn každých pár hodin, dnů nebo týdnů, počínaje od určeného data a času.

     Mějte prosím na paměti, že virtuální zařízení musí být v naplánované době zapnuté. Naplánované zavádění v daný čas neproběhne, pokud je zařízení vypnuté nebo pozastavené. V takových situacích doporučujeme povolit zaškrtávací políčko **V případě propasení naplánovaného zaváděcího času spustit úlohu co nejdříve je to možné**.
   - Někdy nástroje mohou vyžadovat více času než se očekává dokončení jejich práce nebo mohou přestat odpovídat. Pro předejití pádům v mnoha situacích, v sekci **Safety configuration**, vyberte po kolika hodinách Security Server by měl automaticky ukončit proces nástroje.
   - Klikněte na tlačítko **Save**. Nástroj bude přidán do tabulky.

Podle dříve popsaných kroků můžete přidat kolik nástrojů, kolik potřebujete.

7.2.3. Antimalware

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery
- Linux
- macOS

Modul Antimalware chrání systém před všemi druhy malwarových hrozeb (viry, trojskými koni, spywarem, rootkity, adwarem, a tak dále). Ochrana je rozdělena do tří kategorií:

- Skenování při přístupu - brání vstupu nových malwarových hrozeb do systému.
- Testování při spuštění: Aktivně chrání proti hrozbam a automaticky detekuje a blokuje bezsouborové útoky ve fázi pre-execution.
- Manuální skenování - umožňuje detekci a odstranění malwaru, který se již nachází v systému.

Když bezpečnostní agent Bitdefender nalezne virus nebo jiný malware, automaticky se pokusí odstranit škodlivý kód z infikovaného souboru a rekonstruovat původní soubor. Tato operace se označuje jako dezinfekce. Soubory, které nelze dezinfikovat, budou přesunuty do karantény, která bude infekci zadržovat. Virus v karanténě nemůže způsobit žádnou škodu, protože ho nelze spustit ani přečíst.

Pokročilí uživatelé mohou nakonfigurovat výjimky ze skenování, pokud nechtějí skenovat konkrétní soubory nebo typy souborů.

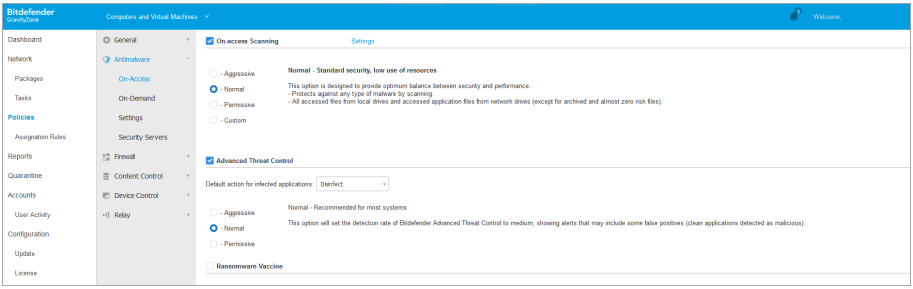
Nastavení jsou uspořádána do následujících sekcí:

- Při přístupu
- Spuštění
- Manuální
- HyperDetect
- Pokročilý Anti-Exploit
- Nastavení
- Bezpečnostní servery

Při přístupu

V této části můžete nakonfigurovat části, které poskytují ochranu při přístupu k souborům nebo aplikacím:

- Skenování při přístupu
- Ransomware vakcína



Práva - Nastavení při přístupu

Skenování při přístupu

Skenování Při přístupu brání novým malwarovým hrozbám v přístupu k systému tím, že skenuje místní a síťové soubory při přístupu (když jsou otevřeny, přemisťovány, kopírovány nebo spouštěny), spouštěcí sektory a potenciálně nežádoucí aplikace (PUA).

Poznámka
V systémech na bázi Linux je tato funkce je částečně limitována. Více podrobností naleznete v kapitole o požadavcích v Instalační příručce GravityZone.

Pro nastavení skenování při přístupu:

1. Použijte zaškrtávací pole pro vypnutí nebo zapnutí skenování při přístupu.

   Varování
   Pokud vypnete skenování při přístupu, koncové body se stanou zranitelnými pro malware.

2. Pro rychlou konfiguraci klikněte na úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (agresivní, normální nebo tolerantní). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

3. Podrobné nastavení skenování můžete konfigurovat zvolením **Vlastní** úrovně ochrany a kliknutím na odkaz **Nastavení**. Zobrazí se okno **Nastavení skenování při přístupu**, obsahující několik možností uspořádaných pod dvěma kartami, **Obecné** a **Pokročilé**.

   Možnosti pod kartou **Obecné** jsou popsány níže:

   - **Umístění souboru**. Pomocí těchto možností upřesněte, které typy souborů chcete skenovat. Předvolby skenování mohou být nastaveny zvlášť pro lokální soubory (uložené na lokálním koncovém bodě) nebo síťové soubory (uložené na síťových sdílených složkách). Pokud je antimalwarová ochrana nainstalovaná na všech počítačích v síti, můžete vypnout skenování síťových souborů a tím umožnit rychlejší přístup k síti.

     Můžete nastavit bezpečnostního agenta, aby skenoval všechny soubory (nehledě na příponu souboru), pouze soubory aplikací, nebo určité souborové přípony, které považujete za nebezpečné. Skenování všech souborů, ke kterým přistupujete, poskytuje nejlepší ochranu, zatímco pokud budete skenovat pouze aplikace, dosáhnete lepšího výkonu systému.

     > **Poznámka**
     > Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

     Pokud si přejete skenovat pouze určité souborové přípony, zvolte v nabídce **Uživatelem definované přípony**, přípony zadejte do pole úprav a po každé stiskněte `Enter`.

     > **Poznámka**
     > V systémech na bázi Linux jsou přípony souborů citlivé na velká a malá písmena, a soubory se stejným jménem, ale jinými příponami budou považovány za dva různé soubory. Například, `file.txt` je odlišný od `file.TXT`.

     Z důvodů výkonnosti systému můžete také ze skenování vynechat velké soubory. Označte pole **Maximální velikost (MB)** a určete hranici velikosti souborů, které mají být skenovány. Využívejte této možnosti s rozvahou, protože malware může infikovat i velké soubory.
   - **Sken.** Vyberte odpovídající políčka pro nastavení požadovaných možností skenování.

- **Pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Boot sektorů.** Skenovat zaváděcí sektor systému. Tento sektor pevného disku obsahuje počítačový kód nezbytný k zahájení spouštěcího procesu. Když virus infikuje spouštěcí sektor, jednotka se může stát nepřístupnou a nemusí být možné spustit systém a přistupovat k datům.
- **Pro keyloggery.** Keyloggery zaznamenávají, co píšete na klávesnici, a odesílají po Internetu zprávy osobě se zlými úmysly (hackerovi). Hacker může ze zcizených dat získat citlivé informace, jako čísla účtů a hesla, a použít je k vlastnímu prospěchu.
- **Potenciálně nežádoucí aplikace (PUA).** Potenciálně nežádoucí aplikace (PUA) je program, který může být na PC nežádoucí a někdy bývá součástí freewaru nebo softwaru. Takové programy mohou být nainstalovány bez vědomí uživatele (jsou známé také jako adware), nebo mohou být obsaženy v původní expresní instalační sadě (podporované reklamou). Možný dopad těchto programů zahrnuje zobrazování vyskakovacích oken, instalaci nechtěných nástrojových lišt ve výchozím prohlížeči nebo spuštění několika procesů na pozadí a zpomalení výkonu PC.
- **Archivy**. Zvolte tuto možnost, pokud chcete zapnout skenování při přístupu pro archivované soubory. Skenování uvnitř archivů je pomalý proces náročný na prostředky, který proto není doporučen pro ochranu v reálném čase. Archivy obsahující infikované soubory nepředstavují pro zabezpečení vašeho systému bezprostřední hrozbu. Malware může ovlivňovat váš systém, pouze pokud je infikovaný soubor z archivu extrahován a spuštěn bez zapnutého skenování při přístupu.

  Pokud se rozhodnete využít této možnosti, můžete konfigurovat následující optimalizační možnosti:
  - **Maximální velikost archivu (MB). .** Můžete nastavit maximální přijatelnou velikost archivů, které mají být skenovány při přístupu. Zaškrtněte příslušné políčko a zadejte maximální velikost archivů (v MB).
  - **Maximální hloubka archivu (úrovně).** Zaškrtněte příslušné políčko a z nabídky zvolte maximální hloubku archivu. Pro nejvyšší výkon zvolte nejnižší hodnotu, pro maximální ochranu zvolte nejvyšší hodnotu.
- **Odložené skenování.** Odložené skenování zvýší výkon systému při provádění přístupových operací k souborům. Například, při kopírovaní

velkých souborů zůstanou systémové zdroje nedotčeny. Tato možnost je ve výchozím stavu povolená.

- **Skenovací akce**. Podle typu rozpoznaných souboru, následující možnosti jsou provedeny automaticky:
  - **Výchozí akce pro infikované soubory.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanizmů, které zahrnují malwarové signatury, machine learnign a umělou inteligenci (AI). Bezpečnostní agent Bitdefender může za běžných okolností odstranit malwarový kód z infikovaného souboru a obnovit původní soubor. Této operaci se říká dezinfikace.

    Pokud je nalezen infikovaný soubor, bezpečnostní agent Bitdefender se ho ve výchozím nastavení automaticky pokusí dezinfikovat. Pokud se dezinfekce nezdaří, soubor je přesunut do karantény, která infekci zadrží. Tento doporučený postup můžete změnit dle svých potřeb.

    Důležité
    V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

  - **Výchozí akce pro podezřelé soubory.** Soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé). Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.

    Pro zabránění potenciální infekci bude případě nalezení podezřelého souboru k němu uživatelům zakázán přístup,

Přestože to nedoporučejeme, výchozí nastavení můžete změnit. Pro každý typ souboru můžete určit dvě akce. K dispozici jsou následující akce:

Odepřít přístup
Zakázat přístup k nalezeným souborům.

Důležité
Na koncových bodech MAC je místo akce **Zakázání přístupu** provedeno **Přesunutí do karantény**.

vyléčit
Odstranit malwarový kód z infikovaných souborů. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech.

Odstranit
Odstranit odhalené soubory z disku, bez jakéhokoli upozornění. Této akci se doporučujeme vyhýbat.

Přesunout soubory do karantény
Přesunout odhalené soubory z jejich současného umístění do karanténní složky. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Můžete spravovat soubory v karanténě ze záložky Karanténa v konzoli.

Nedělat nic
Hlášení pouze infikovaných souborů nalezených produktem Bitdefender.

Karta **Pokročilé** se týká skenování při přístupu pro stroje Linux. Použijte zaškrtávací pole pro jeho zapnutí nebo vypnutí.

V tabulce níže můžete konfigurovat adresáře Linux, které chcete skenovat. Ve výchozím nastavení tu je pět položek a každá z nich odpovídá určitému umístění na koncových bodech: `/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

Pro přidání dalších položek:

- Do vyhledávacího pole v horní části tabulky zadejte jakýkoli vlastní název umístění.
- Zvolte předem definovaná umístění ze seznamu, který se zobrazí kliknutím na šipku na pravé straně vyhledávacího pole.

Klikněte na tlačítko ⊕ **Přidat** pro uložení umístění do tabulky, a tlačítko ⊗ **Odstranit** pro jeho odstranění.

Ransomware vakcína

Ransomwarová vakcína imunizuje váš stroj proti **známému** ransomwaru blokujícímu šifrovací proces i v případě, že je počítač infikovaný. Použijte zaškrtávací pole pro zapnutí nebo vypnutí Ransomwarové vakcíny.

Funkce Ransomwarová vakcína je ve výchozím nastavení vypnutá. Laboratoře Bitdefender analyzují chování všeobecně rozšířeného ransomwaru a s každou

aktualizací signatur jsou doručeny nové signatury, aby reagovaly i na nejnovější hrozby.

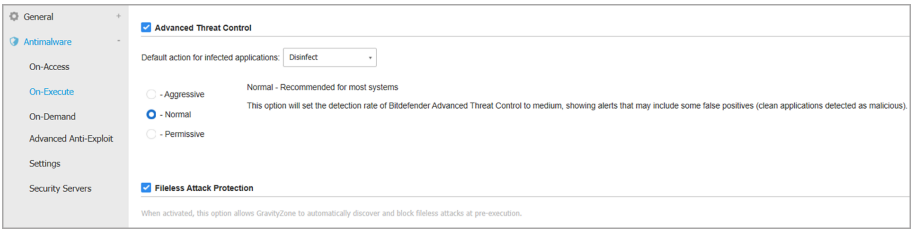
Varování
Pro zvýšení ochrany proti ransomwarovým hrozbám dávejte pozor na nevyžádané nebo podezřelé přiložené soubory a ujistěte se, že je databáze signatur aktuální.

Poznámka
Vakcína Ransomware je k dispozici pouze s Bitdefender Endpoint Security Tools pro Windows.

Spuštění

V této části můžete nakonfigurovat ochranu před škodlivými procesy, pokud jsou spuštěny. Pokrývá následující ochranné vrstvy:

- Cloudová detekce hrozeb
- Pokročilá ochrana před hrozbami (ATC)
- Ochrana proti Fileless útokům
- Zotavení po infekci Ransomware



Politiky - při nastavování

Pokročilá ochrana před hrozbami (ATC)

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery
- macOS

Bitdefender Advanced Threat Control je proaktivní detekční technologie, která využívá pokročilé heuristické metody k detekci nových potenciálních hrozeb v reálném čase.

Pokročilá ochrana před hrozbami neustále sleduje aplikace běžící na koncovém bodě a hledá akce s chováním podobným malwaru. Každá z těchto akcí je ohodnocena a pro každý proces je spočítáno celkové skóre. Když celkové skóre procesu dosáhne daného prahu, proces je považován za škodlivý.

Pokročilá ochrana před hrozbami se automaticky pokusí vydezinfikovat odhalený soubor. Pokud dezinfikační postup selže, Pokročilá ochrana před hrozbami soubor odstraní.

Poznámka
Před uplatněním dezinfikační akce je kopie souboru odeslána do karantény, abyste ho v případě, že se jednalo o falešný poplach, mohli obnovit později. Tuto akci můžete konfigurovat v možnosti **Kopírovat soubory do karantény před aplikováním dezinfikace**, dostupné na kartě **Antimalware > Nastavení** v nastavení pravidel. V šablonách pravidel je tato možnost automaticky povolena.

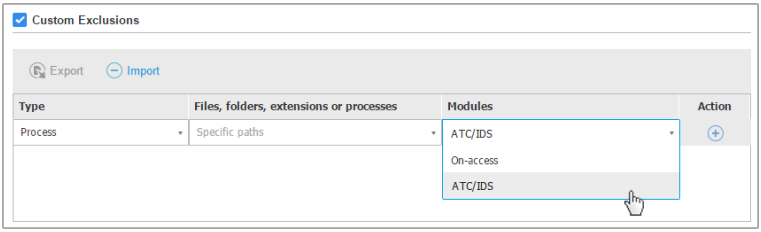
Pro konfiguraci Pokročilé ochrany před hrozbami:

1. Použijte zaškrtávací pole pro zapnutí nebo vypnutí Pokročilé ochrany před hrozbami.

   Varování
   Pokud vypnete Pokročilou ochranu před hrozbami, počítače budou zranitelné vůči neznámému malwaru.

2. Výchozí akce pro infikované aplikace odhalené Pokročilou kontrolou před hrozbami je dezinfikace. Můžete zvolit jinou výchozí akci pomocí dostupné nabídky:
   - **Blokovat (Block)**, pro zablokování přístupu k infikované aplikaci.
   - **Nedělat nic**, a hlásit pouze infikované aplikace odhalené produktem Bitdefender.
3. Klikněte na úroveň zabezpečení, která nejlépe vyhovuje vašim potřebám (**Aggressive, Normal or Permissive**). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

Poznámka
Při nastavením vyšší úrovně ochrany bude Pokročilá ochrana před hrozbami pro nahlášení procesu vyžadovat méně známek chování podobného malwaru. To povede k hlášení většího počtu aplikací a současně zvýšené pravděpodobnosti falešných detekcí (čistých aplikací rozpoznaných jako škodlivé).
Důrazně doporučujeme vytvoření pravidel s výjimkami pro běžně používané nebo známé aplikace pro zamezení falešnému poplachu (chybná detekce legitimních aplikací). Přejděte na kartu Antimalware > Nastavení a nastavte pravidla výjimek procesu ATC/IDS pro důvěryhodné aplikace.



Politiky Počítačů a Virtuálních Strojů - Vyloučení procesu ATC/IDS

Ochrana proti Fileless útokům

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery

Fileless Attack Protection detekuje a blokuje fileless malware ve fázi před spuštěním, včetně ukončení PowerShell spuštěním škodlivého příkazového řádku, blokování škodlivého přenosu, analýzu vyrovnávací paměti před vložením kódu a blokování procesu vniknutí kódu.

Zotavení po infekci Ransomware

Ransomware Mitigation využívá detekční a nápravné technologie k ochraně vašich dat před útoky ransomware. Bez ohledu na to, zda je ransomware známý nebo nový, GravityZone detekuje abnormální pokusy o šifrování a blokuje proces. Poté obnoví soubory ze záložních kopií do jejich původního umístění.

Důležité
Zmírnění ransomwaru vyžaduje aktivní kontrolu hrozeb.

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery

Konfigurace zmírnění ransomwaru:

1. Chcete-li tuto funkci povolit, zaškrtněte políčko **Zmírnění ransomwaru** v části zásad **Antimalware a při spuštění** .
2. Vyberte režimy monitorování, které chcete použít:
   - Lokálně. GravityZone sleduje procesy a detekuje útoky ransomwaru zahájené lokálně v koncovém bodě. Doporučuje se pro pracovní stanice. Používejte opatrně na serverech kvůli dopadu na výkon.
   - Vzdálený. GravityZone sleduje přístup ke sdíleným cestám v síti a detekuje útoky ransomwaru, které jsou iniciovány z jiného počítače. Tuto možnost použijte, pokud je koncovým bodem souborový server nebo pokud jsou povoleny sdílené síťové položky.
3. Vyberte metodu obnovení:
   - Manuální. Ručně vyberete útoky, ze kterých chcete soubory obnovit. Na stránce **Reporty a aktivity ransomwaru** to můžete provést kdykoli, kdykoli to budete chtít, nejpozději však do 30 dnů od útoku. Po této době již nebude možné obnovení.
   - Automaticky. GravityZone automaticky obnoví soubory hned po detekci ransomwaru.

   Aby bylo zotavení úspěšné, musí být k dispozici koncové body.

Po povolení máte několik možností, jak zkontrolovat, zda je vaše síť napadena ransomwarem:

- Zkontrolujte oznámení a vyhledejte **Detekce ransomwaru** .

  Další informace o tomto oznámení najdete na stránce „Typy oznámení“ (str. 534).
- Zkontrolujte report **Bezpečnostní audit** .

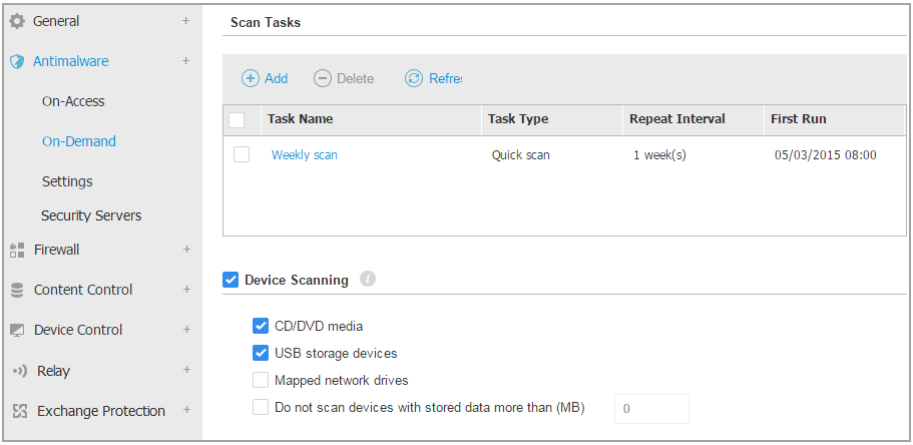
- Zkontrolujte stránku **Aktivita ransomwaru** .

  Dále na této stránce můžete v případě potřeby spustit úlohy obnovy. Další informace viz ???.

V případě, že si všimnete detekce, která je legitimním procesem šifrování, máte určité cesty, kde povolíte šifrování souborů nebo povolíte vzdálený přístup z určitých počítačů, přidejte výjimky do **Nastavení a Antimalware a Vlastní výjimky** sekce zásad. Ransomware Mitigation umožňuje vyloučení složek, procesů a IP/masek. Další informace viz „Výjimky“ (str. 280).

Manuální

V této sekci si můžete přidávat a konfigurovat antimalwarové skenovací úlohy, které budou pravidelně probíhat na cílových počítačích v závislosti na definovaném plánu.



Politiky Počítačů a Virtuálních Strojů - Úlohy On Demand Scan

Skenování probíhá tiše na pozadí nehledě na to, zda je uživatel přihlášený v systému, nebo ne.

Přestože to není povinné, doporučujeme naplánovat kompletní systémový sken, který proběhne každý týden na všech koncových bodech. Pravidelné skenování koncových bodů je aktivní bezpečnostní opatření, které pomáhá v odhalení a blokování malwaru, který by mohl uniknout funkcím ochrany v reálném čase.

Kromě pravidelného skenování můžete nastavit také automatickou detekci a skenování externích paměťových médií.

Správa skenovacích úloh

Tabulka Skenovací úlohy vás informuje o existujících skenovacích úlohách a poskytuje o každé z nich důležité informace:

- Název a typ úlohy.
- Plán, podle kterého úloha pravidelně probíhá (opakování).
- Čas, kdy úloha proběhla poprvé.

Můžete přidat a konfigurovat následující typy skenovacích úloh:

- **Rychlý sken** používá k nalezení malwaru ve vašem systému cloudovou detekci. Provedení rychlého skenu obvykle trvá méně než minutu a využije jen zlomek systémových prostředků, které potřebuje běžný sken.

  Pokud je nalezen malware nebo rootkity, Bitdefender automaticky provede dezinfekci. Pokud je soubor z jakéhokoli důvodu nemožné dezinfikovat, je přesunut do karantény. Tento typ skenování ignoruje podezřelé soubory.

  Rychlý sken je výchozí skenovací úloha s přednastavenými možnostmi, které nelze upravovat. V rámci jednoho pravidla můžete přidat pouze jeden rychlý sken.

- **Kompletní sken** otestuje celý koncový bod na přítomnost malwaru ohrožujícího jeho bezpečnost, jako viry, spyware, adware, rootkity a další.

  Bitdefender se automaticky pokusí vyčistit soubory, které byli identifikované jako malware. Pokud malware nemůže být odstraněn, je přesunut do karantény, kde nemůže napáchat žádné škody. Podezřelé soubory jsou ignorovány. Chcete-li také podniknout kroky proti podezřelým souborům nebo podniknout další běžné akce s infikovanými soubory, poté vybrat a spustit Vlastní Skenování.

  Kompletní sken je výchozí skenovací úloha s přednastavenými možnostmi, které nelze upravovat. V rámci jednoho pravidla můžete přidat pouze jeden kompletní sken.

- **Vlastní sken** vám umožňuje zvolit specifická umístění, která chcete skenovat, a nastavit možnosti skenování.

- **Síťový sken** je typ vlastního skenování, které umožňuje přiřazení jediného spravovaného koncového bodu pro skenování síťových jednotek, a nastavení možností skenování a určitých umístění, která mají být skenována. Pro úlohy

skenování sítě musíte zadat pověření uživatelského účtu s oprávněními pro čtení/psaní na cílové síťové jednotky, aby bezpečnostní agent mohl přistupovat a provádět na nich opatření.

Opakování úlohy síťového skenování bude zasíláno pouze na koncový bod zvolený jako skener. Pokud je zvolený koncový bod nedostupný, budou použita místní nastavení skenování.

Poznámka
Úlohy síťového skenování můžete tvořit pouze v rámci pravidla, které je již přiřazeno ke koncovému bodu, který má sloužit jako skener.

Kromě výchozích skenovacích úloh (které nemůžete mazat nebo duplikovat) můžete vytvořit tolik vlastních a síťových skenovacích úloh, kolik chcete.

Pro vytvoření a nastavení nové vlastní nebo síťové skenovací úlohy klikněte na tlačítko ⊕ **Přidat** na pravé straně tabulky. Pro změnu nastavení existující skenovací úlohy klikněte na její jméno. V následujícím tématu naleznete pokyny, jak se naučit konfiguraci nastavení úloh.

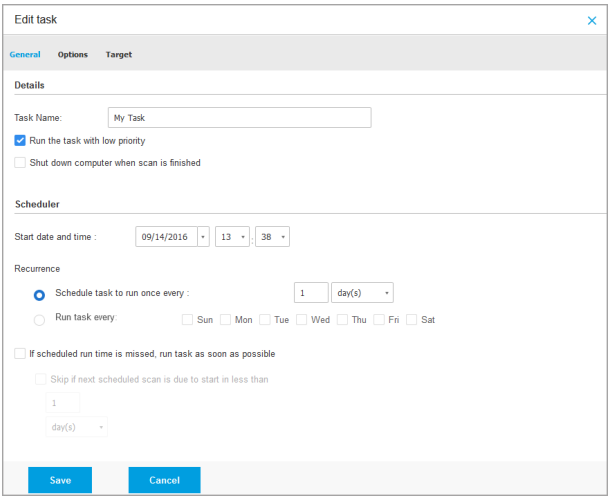
Pro odstranění úlohy ze seznamu ji vyberte a klikněte na tlačítko ⊖ **Odstranit** na pravé straně tabulky.

Konfigurace Skenovacích úloh

Nastavení skenovacích úloh jsou uspořádána pod třemi kartami:

- **Obecné**: nastavte jméno a plán spuštění úlohy.
- **Možnosti**: zvolte profil skenování pro rychlou konfiguraci parametrů skenu a určete skenovací nastavení vlastního skenu.
- **Cíl**: zvolte soubory a složky, které mají být skenovány, a definujte výjimky ze skenování.

Možnosti od první po poslední kartu jsou popsány níže:



Politiky Počítačů a Virtuálních Strojů - Konfigurace Hlavního Nastavení Úloh On Demand Scan

- **Podrobnosti.** Zvolte pro úlohu definující jméno pro usnadnění identifikace, o jakou úlohu se jedná. Při volbě jména vezměte v úvahu cíl skenování a případně nastavení skenu.

  Ve výchozím nastavení probíhají skenovací úlohy se sníženou prioritou. Tímto způsobem umožňuje Bitdefender ostatním programům rychlejší práci, ale prodlouží se tím doba skenovacího procesu. Použijte zaškrtávací pole **Spustit úlohu s nízkou prioritou** pro obnovení této funkce.

  Poznámka
  Tato možnost platí pouze pro Bitdefender Endpoint Security Tools a Endpoint Security (agent pro starší verze).

  Označte pole **Vypnout počítač po dokončení skenování** pro vypnutí vašeho stroje, pokud ho plánujete nějakou chvíli nepoužívat.

  Poznámka
  Tato možnost se vztahuje na Bitdefender Endpoint Security Tools, Endpoint Security (agent pro starší verze) a Endpoint Security for Mac.

- **Plánovač.** Použijte možnosti plánování pro nastavení skenovacího plánu. Můžete nastavit skenování tak, aby se spouštělo každých pár hodin, dnů nebo týdnů, počínaje od určeného data a času.

  Koncový bod musí být zapnutý v době kdy se má spustit naplánovaná úloha. Naplánovaný sken se nespustí pokud je stroj vypnutý, hibernuje a nebo pokud je ve spánkovém módu. V takových případech bude skenování odloženo na příště.

  > **Poznámka**
  > Naplánovaný sken se spustí na cílovém koncovém bodě v místním čase. Například, pokud je naplánovaný sken nastavený na zahájení v 18:00 a koncový bod je v jiné časové zóně než Control Center, skenování začne v 18:00 (času na koncovém bodě).

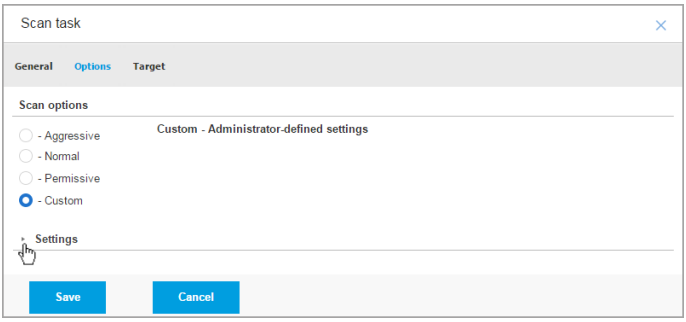
  Volitelně si můžete vyspecifikovat co se má stát, když se skenovací úloha nemohla spustit v naplánovaném čase (Koncový bod byl offline nebo vypnutý). Použijte tuto volbu **Pokud neproběhne skenovací úloha v naplánovaném času, tak spustit skenovací úlohu co nejdříve jakmile to půjde** podle vašich potřeb:

  – Pokud ponecháte tuto volbu neoznačenou, tak se skenovací úloha zkusí spustit znova v dalším naplánovaném čase.

  – Když si vyberete tuto volbu, tak tím vynutíte aby byl sken spuštěn ihned jakmile to bude možné. Pro jemné nastavení nejlepšího načqasovánískenovací rutinu a abyste zabránili rušení uživatele během pracovní doby, si vyberte **Přeskočit pokud následující sken je naplánován aby se spustil za méně než**, pak vyspecifikujte interval jaký chcete.

- **Parametry skenu.** Zvolte úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (agresivní, normální nebo tolerantní). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

  Na základě zvoleného profilu budou parametry skenování v sekci **Nastavení** nastaveny automaticky. Ale pokud si přejete, můžete je nastavit podrobněji. To provedete tak, že označíte políčko **Vlastní** a poté rozbalíte sekci **Nastavení**.



Úloha skenování počítače - konfigurace Vlastního skenování

- **Soubory.** Pomocí těchto možností upřesněte, které typy souborů chcete skenovat. Můžete nastavit bezpečnostního agenta, aby skenoval všechny soubory (nehledě na příponu souboru), pouze soubory aplikací, nebo určité souborové přípony, které považujete za nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

  Poznámka

  Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

  Pokud si přejete skenovat pouze určité souborové přípony, zvolte v nabídce **Uživatelem definované přípony**, přípony zadejte do pole úprav a po každé stiskněte `Enter`.

- **Archivy.** Archivy obsahující infikované soubory nepředstavují pro zabezpečení vašeho systému bezprostřední hrozbu. Malware může ovlivňovat váš systém, pouze pokud je infikovaný soubor z archivu extrahován a spuštěn bez zapnuté ochrany v reálném čase. Doporučujeme však tuto možnost použít, aby byly detekovány a odstraněny všechny potenciální hrozby, i když nejsou bezprostřední.

  Poznámka

  Skenování archivovaných souborů zvyšuje celkovou dobu skenu a vyžaduje více systémových prostředků.

- **Skenovat uvnitř archivů.** Zvolte tuto možnost, pokud si přejete kontrolovat archivované soubory na malware. Pokud se rozhodnete využít této možnosti, můžete konfigurovat následující optimalizační možnosti:
  - **Omezit velikost archivu na (MB).** Můžete nastavit maximální přijatelnou velikost archivů, které mají být skenovány. Zaškrtněte příslušné políčko a zadejte maximální velikost archivů (v MB).
  - **Maximální hloubka archivu (úrovně).** Zaškrtněte příslušné políčko a z nabídky zvolte maximální hloubku archivu. Pro nejvyšší výkon zvolte nejnižší hodnotu, pro maximální ochranu zvolte nejvyšší hodnotu.
- **Skenovat emailové archivy.** Vyberte tuto možnost, pokud chcete povolit skenování souborů emailových zpráv a emailových databází včetně souborů s formáty jako .eml, .msg, .pst, .dbx, .mbx, .tbb a další.

  Poznámka
  Skenování emailových archivů je zdrojově náročné a může ovlivnit výkon systému.

- **Různé.** Vyberte odpovídající políčka pro nastavení požadovaných možností skenování.
  - **Skenovat spouštěcí sektory.** Skenovat zaváděcí sektor systému. Tento sektor pevného disku obsahuje počítačový kód nezbytný k zahájení spouštěcího procesu. Když virus infikuje spouštěcí sektor, jednotka se může stát nepřístupnou a nemusí být možné spustit systém a přistupovat k datům.
  - **Skenovat registr.** Tuto možnost použijte ke skenování klíčů registru. Registr systému Windows je databáze, která uchovává nastavení konfigurací a možností pro součásti operačního systému Windows i pro nainstalované aplikace.
  - **Hledat rootkity.** Tuto možnost zvolte pro skenování rootkitů a objektů skrytých pomocí tohoto softwaru.
  - **Hledat keyloggery.** Zvolte tuto možnost pro skenování keylogger softwaru.
  - **Skenovat síťové složky.** Tato možnost skenuje mountované síťové jednotky.

    Pro rychlé skenování je tato možnost ve výchozím nastavení vypnutá. Úplný sken je aktivován už v základní konfiguraci. Vlastní skenování, pokud jste nastavily stupeň zabezpečení na možnost**Agresivní/Normální**, **Skenovat síť**

je automaticky povolené Pokud jste nastavily stupeň zabezpečení na možnost **Přípustné**, **Skenovat Síť** je automaticky zakázané.

- **Skenovat paměť.** Tuto možnost použijte ke skenování programů běžících v paměti systému.
- **Skenovat cookies.** Tuto možnost zvolte pro skenování souborů cookie, které jsou ukládány prohlížeči na koncových bodech.
- **Skenovat pouze nové a změněné soubory.** Skenováním pouze nových a změněných souborů výrazně zlepšíte celkovou reakci systému s minimálními ústupky v oblasti zabezpečení.
- **Skenovat pro potenciálně nežádoucí aplikace (PUA).** Potenciálně nežádoucí aplikace (PUA) je program, který může být na PC nežádoucí a někdy bývá součástí freewaru nebo softwaru. Takové programy mohou být nainstalovány bez vědomí uživatele (jsou známé také jako adware), nebo mohou být obsaženy v původní expresní instalační sadě (podporované reklamou). Možný dopad těchto programů zahrnuje zobrazování vyskakovacích oken, instalaci nechtěných nástrojových lišt ve výchozím prohlížeči nebo spuštění několika procesů na pozadí a zpomalení výkonu PC.

- **Akce.** Podle typu rozpoznaných souboru, následující možnosti jsou provedeny automaticky:
  - **Výchozí akce pro infikované soubory.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanizmů, které zahrnují malwarové signatury, machine learnign a umělou inteligenci (AI). Bezpečnostní agent může za běžných okolností odstranit malwarový kód z infikovaného souboru a obnovit původní soubor. Této operaci se říká dezinfikace.

    Pokud je nalezen infikovaný soubor, bezpečnostní agent se ho automaticky pokusí dezinfikovat. Pokud se dezinfekce nezdaří, soubor je přesunut do karantény, která infekci zadrží.

    Důležité
    V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. V takových případech bude infikovaný soubor z disku odstraněn.

  - **Výchozí akce pro podezřelé soubory.** Soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují

vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé). Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.

Skenování je ve výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení. Soubory v karanténě jsou pravidelně posílány na analýzu do laboratoří Bitdefender. Pokud je přítomnost malwaru potvrzena, je vydána signatura umožňující odstranění malwaru.

– **Výchozí akce pro rootkity.** Rootkity představují specializovaný software, používaný pro ukrytí souborů před operačním systémem. Přestože ve své podstatě nejsou škodlivé, rootkity jsou často využívány pro ukrytí malwaru nebo pro zamaskování přítomnosti narušitele v systému.

  Nalezené rootkity a skryté soubory jsou ve výchozím nastavení ignorovány.

Přestože to nedoporučejeme, výchozí nastavení můžete změnit. Můžete určit druhou akci, která bude provedena v případě selhání té první, a různé akce pro každou kategorii. Z odpovídajících nabídek zvolte první a druhou akci, které budou provedeny na každém typu rozpoznaného souboru. K dispozici jsou následující akce:

Nedělat nic
S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu.

vyléčit
Odstranit malwarový kód z infikovaných souborů. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech.

Odstranit
Odstranit odhalené soubory z disku, bez jakéhokoli upozornění. Této akci se doporučujeme vyhýbat.

Přesunout soubory do karantény
Přesunout odhalené soubory z jejich současného umístění do karanténní složky. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Můžete spravovat soubory v karanténě ze záložky Karanténa v konzoli.

- **Cíle testu.** Do seznamu přidejte všechna umístění, která chcete skenovat na cílových počítačích.

  Pro přidání nového souboru nebo složky ke skenování:

  1. Z rozbalovacího menu zvolte přednastavené umístění, nebo zadejte **Určité cesty**, které si přejete skenovat.
  2. Určete cestu k objektu, který chcete skenovat, v poli úprav.
     - V případě, že jste zvolili přednastavené umístění, doplňte cestu dle potřeby. Například, pro skenování celé složky `Program Files`, stačí vybrat příslušné přednastavené umístění z rozbalovací nabídky. Pro skenování konkrétní složky v `Program Files`, musíte doplnit cestu přidáním lomítka (\) a názvu složky.
     - Pokud jste vybrali **Určité cesty**, zadejte celou cestu k objektu, který má být oskenován. Pro jistotu, že je cesta platná na všech cílových počítačích, doporučujeme používat systémové proměnné (tam, kde je to vhodné).
  3. Klikněte na odpovídající tlačítko ⊕ **Přidat**.

  Klikněte na něj pro úpravu existujícího umístění. Pro vymazání umístění ze seznamu na něj ukažte kurzorem a klikněte na odpovídající tlačítko ⊖ **Odstranit**.

- Pro úlohy skenování sítě musíte zadat pověření uživatelského účtu s oprávněními pro čtení/psaní na cílové síťové jednotky, aby bezpečnostní agent mohl přistupovat a provádět na nich opatření.
- **Výjimky.** Můžete buď použít výjimky určené v sekci **Antimalware > Výjimky** v současném pravidle, nebo můžete nastavit vlastní výjimky pro současnou skenovací úlohu. Pro více detailů ohledně výjimek, se prosím odkažte na „Výjimky“ (str. 280).

Skenování zařízení

Můžete nastavit bezpečnostního agenta tak, aby automaticky rozpoznal a skenoval externí paměťová zařízení, když jsou připojena ke koncovému bodu. Detekovaná zařízení spadají do jedné z následujících kategorií:

- Disky CD/DVD
- Paměťová zařízení USB, jako flashdisky a externí pevné disky
- Jednotky s více než je určené množství uložených dat.

Skeny zařízení se automaticky snaží o dezinfikaci souborů zjištěných jako infikované, nebo o jejich přesunutí do karantény v případě, že dezinfikace není možná. Upozorňujeme, že některá zařízení, jako jsou CD/DVD, jsou určena pouze ke čtení. U infikovaných souborů obsažených na takové podpoře úložiště nelze provádět žádnou akci.

Poznámka
Během skenování zařízení má uživatel přístup ke všem datům na zařízení.

Pokud jsou v sekci **Obecné > Oznámení** povoleny výstražná vyskakovací okna, uživatel je vybídnut ke schválení nebo odmítnutí skenování nalezeného zařízení místo toho, aby se skenování spustilo automaticky.

Když je zahájeno skenování zařízení:

- Oznamovací vyskakovací okno upozorní uživatele na sken zařízení, pokud jsou v sekci **Obecné > Oznámení** oznamovací vyskakovací okna povolena.

Jakmile je skenování dokončeno, uživatel musí zkontrolovat zjištěné hrozby, pokud nějaké jsou.

Zvolte možnost **Skenování zařízení** pro zapnutí automatické detekce a skenování paměťových zařízení. Pro nastavení skenování jednotlivě pro každý typ zařízení použijte následující možnosti:

- **CD/DVD média**
- **Paměťová zařízení USB**
- **Neskenovat zařízení, na kterých jsou uložená data větší než (MB)**. Použijte tuto možnost pro automatické přeskočení skenování zjištěného zařízení v případě, že množství uložených dat přesahuje určenou velikost. Zadejte velikostní limit (v megabajtech) do odpovídajícího pole. Nula znamená, že žádný velikostní limit není zaveden.

HyperDetect

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery
- Linux

HyperDetect přidá vrstvu ochrany navíc k existujícím skenovacím technologiím (Při přístupu, Na vyžádání a Sken síťového provozu) a bojuje tak proti kyberútokům nové generace, včetně pokročilých přetrvávajících hrozeb. HyperDetect posiluje ochranné moduly Antimalware a Kontrolu obsahu pomocí silné heuristiky založené na bázi umělé inteligence a strojového učení.

Se svou schopností předvídat cílené útoky a rozpoznat i ten nejsofistikovanější malware ve fázi před spuštěním, HyperDetect odhaluje hrozby mnohem rychleji než skenovací technologie založené na bázi signatur nebo chování.

Pro nastavení HyperDetectu:

1. Použijte zaškrtávací pole **HyperDetect** pro zapnutí nebo vypnutí modulu.
2. Zvolte, před jakým typem hrozeb chcete chránit svou síť. Ve výchozím nastavení je zapnutá ochrana proti všem typům hrozeb: cíleným útokům, podezřelým souborům a síťovému přenosu, exploitům, ransomwaru nebo graywaru.

   Poznámka
   Heuristika pro síťový přenos vyžaduje povolení **Kontroly obsahu > Skenování síťového provozu**.

3. Upravte úroveň zabezpečení proti hrozbám určeného typu.

   Použijte hlavní spínač navrchu seznamu hrozeb a zvolte jedinečnou úroveň ochrany pro všechny typy hrozeb, nebo zvolte individuální úrovně pro doladění zabezpečení.

   Nastavení modulu na určitou úroveň bude mít za výsledek akce, které budou dotaženy na danou úroveň. Například, pokud je nastaven na **Normální**, modul rozpoznává a uzavírá hrozby, které aktivují prahy **Tolerantní** a **Normální**, ale ne **Agresivní**.

   Ochrana se zvýší z **Tolerantní** na **Agresivní**.

   Mějte na paměti, že agresivní detekce může mít za následek plané poplachy, zatímco tolerantní může vaši síť vystavit některým hrozbám. Doporučujeme nejprve nastavit stupeň ochrany na nejvyšší, a poté ho snížit v případě výskytu mnoha planých poplachů, dokud nedocílíte optimální rovnováhy.

   Poznámka
   Kdykoli zapnete ochranu pro druh hrozeb, detekce je automaticky nastavena na výchozí hodnotu (**Normální** úroveň).

4. V sekci **Akce** nastavte, jak má HyperDetect reagovat na detekce. Zvolte možnosti z rozbalovacího menu pro nastavení akce, která má být aplikována na hrozby:
   - Pro soubory: odepřít přístup, dezinfikovat, odstranit, karanténa, nebo jen nahlásit soubor.
   - Pro síťový provoz: blokovat, nebo jen nahlásit podezřelý přenos.
5. Označte pole **Rozšířit hlášení na vyšší úrovně** vedle rozbalovacího menu, pokud chcete prohlížet hrozby zjištěné na vyšších úrovních ochrany, než je nastavená úroveň.

Pokud si nejste jistí současným nastavením, můžete snadno obnovit původní nastavení tak, že kliknete na tlačítko **Obnovit výchozí** ve spodní části stránky.

Pokročilý Anti-Exploit

Poznámka
Tento modul je k dispozici pro:
- Windows pro pracovní stanice

Advanced Anti-Exploit je proaktivní technologie, která detekuje exploity v reálném čase. Na základě strojového učení chrání před řadou známých a neznámých exploitů, včetně bezsouborových útoků v paměti.

Chcete-li povolit ochranu před exploity, zaškrtněte políčko **Advanced Anti-Exploit**.

Funkce Advanced Anti-Exploit je nastavena na spuštění s doporučenými nastaveními. Ochranu můžete nastavit dle svých potřeb. Chcete-li obnovit výchozí nastavení, klikněte na odkaz **Obnovit výchozí** v pravé horní části sekce.

GravityZone má funkci anti-exploit uspořádanou do tří částí:

- **Detekce v celém systému**

  Techniky anti-exploit v této sekci sledují systémové procesy, které jsou cíli zneužití.

  Další informace o dostupných technikách a konfiguraci jejich nastavení naleznete v části „Konfigurace zmírnění celého systému“ (str. 274).

- **Předdefinované aplikace**

  Pokročilý modul Anti-Exploit je předkonfigurován seznamem častých aplikací, jako např. Microsoft Office, Adobe Reader nebo Flash Player, které jsou nejčastěji vystavovány útokům.

Další informace o dostupných technikách a konfiguraci jejich nastavení naleznete v části „Nakonfigurovat techniky specifické pro aplikace“ (str. 275).

- **Další aplikace**

  V této sekci můžete přidat a konfigurovat ochranu pro další aplikace dle potřeby.

  Další informace o dostupných technikách a konfiguraci jejich nastavení naleznete v části „Nakonfigurovat techniky specifické pro aplikace“ (str. 275).

Každou sekci můžete rozbalit nebo sbalit klepnutím na její záhlaví. Tímto způsobem se rychle dostanete k nastavení, které chcete konfigurovat.

Konfigurace zmírnění celého systému

V této sekci si můžete vybrat jednu z následujících možností:

Technika	Popis
Stupňování oprávnění	Zabraňuje získávání neoprávněnému přístupu ke zdrojům. Výchozí akce: Zablokovat proces
Ochrana procesu LSASS	Chrání proces LSASS před únikem informací, jako hashování hesel a nastavení zabezpečení. Výchozí akce: Zablokovat proces

Techniky anti-exploitu jsou standardně zapnuty. Chcete-li některou z nich vypnout, zrušte zaškrtnutí políčka.

Volitelně můžete změnit akci provedenou automaticky po detekci. Vyberte akci, která je k dispozici v nabídce:

- **Zatavit proces**: okamžitě ukončí využívaný proces.
- **Blokovat proces**: zabraňuje přístupu škodlivého procesu k neoprávněným zdrojům.
- **Pouze reportovat**: GravityZone ohlásí událost bez provedení zmírňující akce. Podrobnosti události můžete zobrazit v **Pokročilá ochrana proti exploitům** a v reportech Blokovaných aplikací a Bezpečnostním auditu.

Nakonfigurovat techniky specifické pro aplikace

Ať už předdefinované, nebo dodatečné aplikace, všechny sdílí stejnou sadu anti-exploit technik. Můžete je najít popsané zde:

Technika	Popis
ROP emulace	Detekuje pokusy o zneužití spustitelných stránek paměti pro data pomocí techniky ROP (Return-Oriented Programming). Výchozí akce: Zablokovat proces
Přetečení zásobníku ROP	Zjišťuje pokusy o únos plovoucího kódu pomocí techniky ROP, ověřením umístění zásobníku. Výchozí akce: Zablokovat proces
ROP Nelegální volání	Detekuje pokusy o únos plovoucího kódu pomocí techniky ROP, ověřením volaní citlivých systémových funkcí. Výchozí akce: Zablokovat proces
ROP Nezarovnaný zásobník	Detekuje pokusy o poškození zásobníku za použití ROP techniky, kdy validuje zarovnání adres zásobníku. Výchozí akce: Zablokovat proces
ROP Návrat do zásobníku	Detekuje pokusy o spuštění kódu přímo na zásobníku pomocí ROP techniky, kdy validuje rozsah návratové adresy. Výchozí akce: Zablokovat proces
ROP zásobník připraven	Zjistí pokusy o poškození zásobníku pomocí techniky ROP ověřením zásobníku ochrany stránky. Výchozí akce: Zablokovat proces
Flash Generic	Detekuje pokusy o zneužití Flash přehrávače. Výchozí akce: Zablokovat proces
Užitečné zatížení Flash	Detekuje pokusy o spuštění škodlivého kódu uvnitř Flash přehrávače tím, že skenuje Flash objekty v paměti. Výchozí akce: Zablokovat proces
VBScript Generic	Detekuje pokusy o zneužití VBScript.

Technika	Popis
	Výchozí akce: Zablokovat proces
Provedení kódu Shell	Detekuje pokusy o vytvoření nových procesů nebo stažení souborů, pomocí shellcode. Výchozí akce: Zablokovat proces
Shellcode LoadLibrary	Detekuje pokusy o spuštění kódu přes síťové cesty, pomocí shellcode. Výchozí akce: Zablokovat proces
Anti-Detour	Detekuje pokusy obejít bezpečnostní kontroly při vytváření nových procesů. Výchozí akce: Zablokovat proces
Shellcode EAF (Export Address Filtering)	Detekuje pokusy o přistupování škodlivého kódu k citlivým systémovým funkcím z DLL exportů. Výchozí akce: Zablokovat proces
Hrozba Shellcode	Detekuje pokusy o injektování škodlivého kódu, pomocí validace nově vytvořených hrozeb. Výchozí akce: Zablokovat proces
Anti-Meterpreter	Detekuje pokusy o vytvoření skriptu reverse shell, pomocí skenování spustitelných stránek paměti. Výchozí akce: Zablokovat proces
Vytváření zastaralých procesů	Detekuje pokusy o vytvoření nových procesů pomocí zastaralých technik. Výchozí akce: Zablokovat proces
Vytvoření podřízeného procesu	Blokuje vytvoření jakéhokoli podřízeného procesu. Výchozí akce: Zablokovat proces
Vynutit Windows DEP	Vynucuje Data Execution Prevention (DEP), která blokuje provádění kódu z datových stránek. Výchozí: Zakázáno
Vynutit přemístění modulu (ASLR)	Zabrání načtení kódu na předvídatelných místech přemístěním paměťových modulů. Výchozí: Povoleno

Technika	Popis
Vznikající exploity	Chrání před vznikajícími hrozbami nebo využíváním. Pro tuto kategorii se používají rychlé aktualizace, než je možné provést komplexnější změny. Výchozí: Povoleno

Chcete-li sledovat další aplikace kromě předdefinovaných, klikněte na tlačítko **Add Application** v horní a dolní části stránky.

Konfigurace nastavení ochrany před zneužitím pro aplikaci:

1. U stávajících aplikací klikněte na název aplikace. U nových aplikací klikněte na tlačítko **Přidat**

   Nová stránka zobrazuje všechny techniky a jejich nastavení pro vybranou aplikaci.

   Důležité
   Při přidávání nových sledovaných aplikací buďte opatrní. Bitdefender nemůže zaručit kompatibilitu s jakoukoli aplikací. Proto se doporučuje tuto funkci nejprve otestovat na několika nekritických koncových bodech a poté ji nasadit do sítě.

2. Pokud přidáváte novou aplikaci, zadejte její název a názvy procesů do vyhrazených polí. Pro oddělení procesů použijte středník (;)
3. Pokud potřebujete rychle zkontrolovat popis techniky, klikněte na šipku vedle jejího názvu.
4. Podle potřeby zaškrtněte nebo zrušte zaškrtnutí políček technik využití.

   Pokud chcete označit všechny techniky najednou, použijte možnost **Vše**.
5. V případě potřeby změňte automatickou akci po detekci. Vyberte akci, která je k dispozici v nabídce:
   - **Zatavit proces**: okamžitě ukončí využívaný proces.
   - **Pouze reportovat**: GravityZone ohlásí událost bez provedení zmírňující akce. Podrobnosti o události si můžete prohlédnout v oznámení **Advanced Anti-Exploit** a ve zprávách.

   Ve výchozím nastavení jsou všechny techniky pro předdefinované aplikace nastaveny tak, aby problém zmírnily, zatímco pro další aplikace jsou nastaveny pouze hlášení o událostech.

Chcete-li rychle změnit akci provedenou pro všechny techniky najednou, vyberte akci z nabídky spojené s možností **Vše**.

Klepnutím na tlačítko **Back** v horní části stránky se vraťte do obecného nastavení Anti-Exploit.

Nastavení

V této sekci můžete konfigurovat nastavení karantény a pravidla výjimek ze skenování.

- Konfigurace nastavení karantény
- Konfigurace výjimek skenování

Karanténa

Pro soubory v karanténě na cílových koncových bodech můžete nastavit následující možnosti:

- **Odstranit soubory starší než (dní).** Ve výchozím nastavení jsou soubory v karanténě, které jsou starší než 30 dní, automaticky mazány. Pokud chcete tento interval změnit, zvolte jinou možnost z nabídky.
- **Podávat soubory z karantény do Laboratoří společnosti Bitdefender každých (hodin).** Ve výchozím nastavení jsou soubory do Laboratoří společnosti Bitdefender automaticky odesílány každou hodinu. Můžete upravit časovými interval mezi odesíláním souborů z karantény (ve výchozím nastavení je to hodina). Vzorky souborů budou analyzovány pracovníky výzkumu malwaru společnosti Bitdefender. Pokud je přítomnost malwaru potvrzena, je vydána signatura umožňující odstranění malwaru.
- **Rescan quarantine after security content updates.** Ponechte tuto možnost vybranou pro automatické skenování souborů v karanténě po každé aktualizaci obsahu zabezpečení. Vyčištěné soubory budou automaticky vráceny do původního umístění.
- **Před dezinfikací zkopírovat soubory do karantény.** Zvolte tuto možnost pro zabránění ztráty dat v případě falešného poplachu a pro zkopírování každého souboru rozpoznaného jako infikovaný do karantény před aplikací dezinfikační činnosti. Legitimní soubory můžete později obnovit na stránce **Karanténa**.
- **Povolit uživatelům provádět akce v lokální karanténě.** Tato možnost kontroluje akce, které mohou uživatelé koncových bodů provádět na místních souborech v karanténě prostřednictvím uživatelského rozhraní Bitdefender Endpoint

Security Tools. Ve výchozím nastavení mohou místní uživatelé obnovit nebo odstranit soubory v karanténě z jejich počítače pomocí možností dostupných v Bitdefender Endpoint Security Tools. Když tuto možnost vypnete, uživatelé ztratí přístup k tlačítkům pro provádění akce na souborech v karanténě v rozhraní Bitdefender Endpoint Security Tools.

Centralizovaná karanténa

Pokud chcete soubory v karanténě na vašich spravovaných koncových bodech zachovat pro další analýzu, použijte možnost **Centralizovaná karanténa**, která odešle archivovanou kopii každého lokálního karanténovaného souboru do sdílené sítě.

Po povolení této možnosti bude každý karanténovaný soubor ze spravovaných koncových bodů zkopírován a zabalen do heslem chráněného archivu ZIP do určeného síťového umístění. Jméno archivu je hash souboru v karanténě.

Důležité
Hranice velikosti archivu je 100 MB. Pokud archiv přesáhne 100 MB, nebude uložen do umístění ve sdílené síti.

Pro konfiguraci parametrů centralizované karantény vyplňte následující pole:

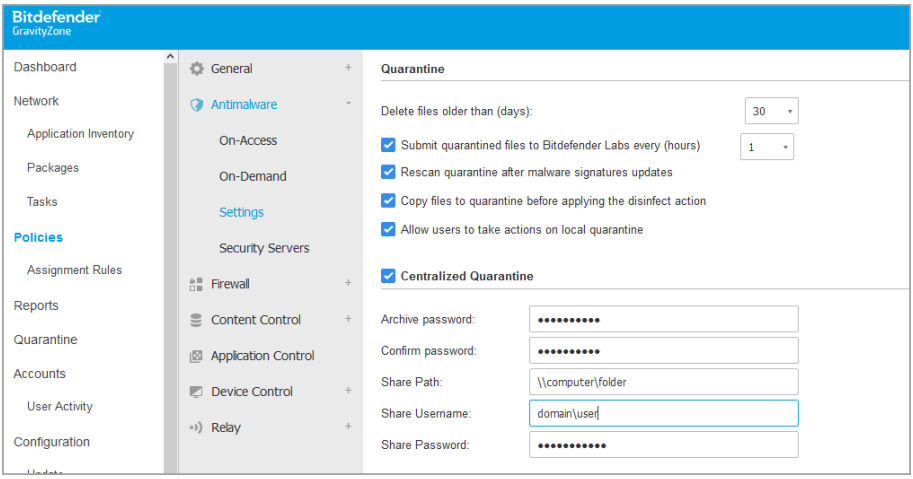
- **Heslo archivu**: zadejte heslo potřebné k archivu souborů v karanténě. Heslo musí obsahovat alespoň jedno velké písmeno, malé písmeno a alespoň jednu číslici nebo zvláštní znak. V dalším poli heslo potvrďte.
- **Sdílení cesty**: zadejte síťovou cestu, kam chcete uložit archiv (například `\\computer\folder`).
- Uživatelské jméno a heslo požadované k připojení se k síťovému sdílení. Podporované formáty uživatelského jména jsou následující:
  - `username@domain`
  - `domain\username`
  - `uživatelské jméno`.

Pro správné fungování centralizované karantény se ujistěte, že jsou naplněny následující podmínky:

- Sdílené umístění je přístupné v síti.
- Koncové body mají připojení ke sdílení v síti.

- Přihlašovací údaje jsou platné a umožňují přístup pro zápis do sdílené síťové položky.
- Síťové sdílení má dostatek místa na disku.

Poznámka
Centralizovaná karanténa se nevztahuje na karanténu poštovních serverů.



Centralizovaná karanténa

Pokud máte místní Sandbox Analyzer instanci nakonfigurovanou v sekci **Sandbox Analyzer > Endpoint Sensor** můžete zaškrtnout políčko **Automaticky odesílat položky z karantény do Sandbox Analyzer**. Upozorňujeme, že odeslané položky musí mít maximální velikost 50 MB.

Výjimky

Bezpečnostní agent Bitdefender může ze skenování vyloučit určité typy položek. Výjimky ze skenování by měly být používány za zvláštních okolností nebo na základě doporučení Microsoftu nebo Bitdefender. Pro nejnovější seznam výjimek doporučených Microsoftem se prosím podívejte na tento článek.

V této sekci můžete konfigurovat použití různých typů výjimek dostupných s bezpečnostním agentem Bitdefender.

- **Vestavěné výjimky** jsou ve výchozím nastavení povoleny a zahrnuty v bezpečnostním agentu Bitdefender.

  Pro skenování všech typů položek můžete vestavěné výjimky vypnout, tato možnost ale významně ovlivní výkon stroje a prodlouží dobu skenování.

- Také si můžete nadefinovat **Vlastní výjimky** pro vlastní vyvinuté aplikace nebo přizpůsobené nástroje, dle vašich specifických potřeb.

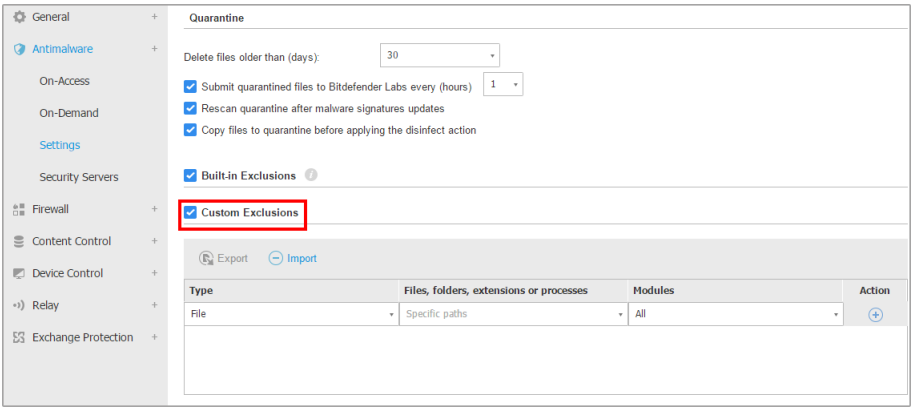
  Vlastní antimalware výjimky se aplikují pro jednu nebo více z těchto metod skenování:

  – Skenování při přístupu
  – Manuální skenování
  – Pokročilá ochrana před hrozbami (ATC)
  – Ochrana proti Fileless útokům
  – Zotavení po infekci Ransomware

  Důležité

  – Pokud máte testovací soubor EICAR, který pravidelně používáte pro testování antimalwarové ochrany, měli byste ho vyloučit ze skenování při přístupu.
  – Pokud používáte VMware Horizon View 7 a App Volumes AppStacks, odkažte se na Dokument VMware.

  Chcete-li vyloučit konkrétní položky z kontroly, vyberte možnost **Vlastní výjimky** a poté přidejte pravidla do tabulky pod.



Pravidla pro počítače a virtuální stroje - Vlastní výjimky

Pro přidání vlastního pravidla výjimky:

1. Z nabídky zvolte typ výjimky:
   - **Soubor**: pouze určený soubor
   - **Složka**: všechny soubory a procesy uvnitř vybrané složky a ze všech jejích podsložek
   - **Přípona**: všechny položky, které mají uvedenou zadanou příponu
   - **Proces**: jakýkoli objekt přístupný vyloučeným procesem
   - **Souborový hash** : soubor se specifikovaným hashem
   - **Hash certifikátu**: všechny aplikace ve specifickém hashi certifikátu (otisk prstu - thumbprint)
   - **Threat Name**: jakákoli položka s názvem detekce (není k dispozici pro operační systémy Linux)
   - **Command Line**: zadaný příkazový řádek (k dispozici pouze pro operační systémy Windows)

Varování
V prostředích VMware bez agenta integrovaných s vShieldem můžete vyloučit pouze složky a přípony. Nainstalováním Bitdefender Tools na virtuální stroje můžete vyloučit také soubory a procesy.

Při konfiguraci balíčku během instalačního procesu musíte označit pole **Zavést vShield na koncový bod, když je zjištěno prostředí VMware integrované s vShieldem**. Pro více informací se odkažte na sekci **Tvorba instalačních balíčků** v Instalačním průvodci.

2. Uveďte podrobnosti specifické pro vybraný typ vyloučení:

   Soubor, složka nebo proces

   Zadejte cestu k položce, která má být ze skenování vyloučena. Cestu můžete zadat několika možnostmi:

   – Deklarujte cestu explicitně.

     Například: `C: emp`

     Chcete-li přidat vyloučení pro cesty UNC, použijte některou z následujících syntaxí:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   – Použijte systémové proměnné dostupné v rozbalovacím menu.

     Pro výjimky procesů musíte zadat také jméno spustitelného souboru aplikace.

     Například:

     `%ProgramFiles%` - vyloučí složku Program Files

     `% WINDIR%\system32` - vyloučí složku system32 ve složce Windows

     Poznámka
     Pro jistotu, že je cesta platná na všech cílových počítačích, doporučujeme používat systémové proměnné (tam, kde je to vhodné).

   – Použít zástupné znaky.

     Hvězdička (*) zastupuje nula nebo více znaků. Otazník (?) Nahrazuje přesně jeden znak. Můžete použít několik otazníků pro určení jakékoli kombinace konkrétního počtu znaků. Například, ??? nahrazuje jakoukoli kombinaci přesně tří znaků.

     Například:

     Vyloučení souborů:

`C:\Test\*` – vyloučí všechny soubory ze složky Test

`C:\Test\*.png` - vyloučí všechny soubory PNG ze složky Test

Vyloučení složky:

`C:\Test\*` - vyloučí všechny složky ze složky Test

Vyloučení procesu:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` - vylučuje procesy Microsoft Notes.

Poznámka
Proces výjimek nepodporuje zástupné znaky v operačních systémech Linux.

Přípona

Určete jednu nebo více souborových přípon, které chcete vyloučit ze skenování, a oddělte je středníkem ";". Přípony můžete zadat s i bez předcházející tečky. Například, pro vyloučení textových souborů zadejte txt.

Poznámka
V systémech na bázi Linux jsou přípony souborů citlivé na velká a malá písmena, a soubory se stejným jménem, ale jinými příponami budou považovány za dva různé soubory. Například, `file.txt` je odlišný od `file.TXT`.

Soubor hash, hash certifikátu, název hrozby nebo příkazový řádek

Vložte soubor hashe, otisk certifikátu (hash) přesný název hrozby nebo příkazový řádek podle nastavených pravidel pro výjimky. Můžete použít jednu položku pro vyloučení.

3. Vyberte skenovací metody, pro které bude pravidlo platit. Některé výjimky se mohou týkat jen skenování při přístupu, skenování na vyžádání, nebo ATC/IDS, zatímco některé mohou být vyžadovány pro všechny tři moduly.
4. Volitelně můžete kliknout na tlačítko **Zobrazit připomínky** pro přidání poznámky do sloupce **Připomínky** o pravidle.
5. Klikněte na tlačítko ⊕ **Přidat**.

   Nové pravidlo bude přidáno do seznamu.

Pro odstranění pravidla ze seznamu klikněte na odpovídající tlačítko ⊗ **Odstranit**.

Důležité
Mějte prosím na paměti, že výjimky ze skenování na vyžádání NEPLATÍ pro kontextové skenování. Kontextové skenování zahájíte kliknutím pravým tlačítkem na soubor nebo složku a zvolením **Skenovat s Bitdefender Endpoint Security Tools**.

Importování a exportování výjimek

Pokud máte v úmyslu použít pravidla výjimek znovu v dalších zásadách, můžete je importovat a exportovat.

Pro exportování vlastních výjimek:

1. Klikněte na **Exportovat** v horní části tabulky výjimek.
2. Uložte soubor CSV na váš počítač. V závislosti na nastavení vašeho prohlížeče se soubor může stáhnout automaticky, nebo budete vyzváni k jeho uložení do nějakého umístění.

Každá řádka v souboru CSV odpovídá jednomu pravidlu, a má pole v následujícím pořadí:

```
<exclusion type>, <object to be excluded>, <modules>
```

Toto jsou dostupné hodnoty v polích CSV:

Typ výjimky:
- 1, pro výjimky souborů
- 2, pro výjimky složek
- 3, pro výjimky přípon
- 4, pro výjimky procesů
- 5, pro výjimky z hashe souboru
- 6, pro výjimky z hashů certifikátu
- 7, pro výjimky z názvu hrozby
- 8, pro vyloučení příkazového řádku

Objekt, který má být vyloučen:
Cesta nebo přípona souboru

Moduly:

1, pro skenování na vyžádání

2, pro skenování při přístupu

3, pro všechny moduly

4, pro ATC/IDS

Například, soubor CSV obsahující antimalwarové výjimky může vypadat takto:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Poznámka
Cesty ve Windows musí mít znak lomítka (\) dvojitý. Například, `%WinDir%\\System32\\LogFiles`.

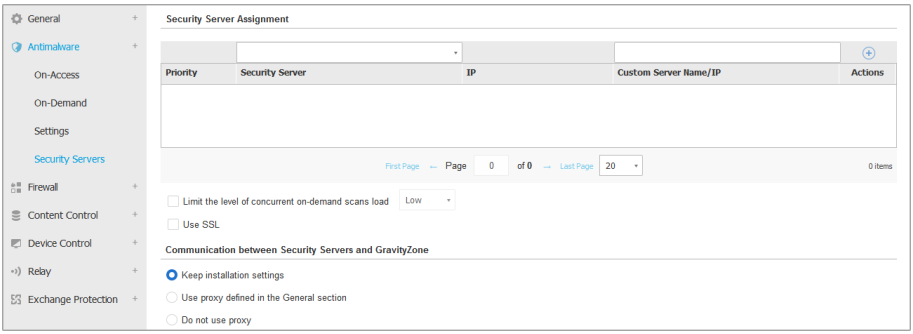
Pro imporotování vlastních výjimek:

1. Klikněte na **Importovat**. Zobrazí se okno **Importovat Výjimky pravidel**.
2. Klikněte na **Přidat** a poté vyberte soubor CSV.
3. Klikněte na tlačítko **Save**. V tabulce jsou zobrazena platná pravidla. Pokud soubor CSV obsahuje neplatná pravidla, budete upozorněni varováním na čísla příslušných řádků.

Security Servery

V této sekci můžete konfigurovat:

- Přiřazení Security Server
- Security Server specifická nastavení



Politika - počítače a virtuální stroje - Antimalware - bezpečnostní servery

Přiřazení Security Server

K cílovým koncovým bodům můžete přiřadit jeden nebo několik Security Serverů a nastavit prioritu, s jakou budou koncové body zvoleny Security Server pro odesílání požadavku na skenování.

Poznámka
Doporučuje se používat Security Servery pro skenování virtuálních strojů nebo počítačů s nízkými zdroji.

Chcete-li cílovým koncovým bodům přiřadit Security Server, přidejte Security Servery, které chcete použít, do tabulky **Přiřazení Security Server**, takto:

1. Klikněte na rozevírací seznam **Security Server** a poté vyberte Security Server.
2. Pokud je Security Server v DMZ nebo za serverem NAT, zadejte do pole **Název vlastního serveru/IP** FQDN nebo IP serveru NAT.

   Důležité
   Ujistěte se, že předávání portů je správně nakonfigurováno na serveru NAT, aby přenos z koncových bodů mohl dosáhnout k Security Server. Podrobnosti viz GravityZone Communication Ports KB article.

3. Klikněte na tlačítko ⊕ **Přidat** ve sloupci **Akce**.

   Security Server je přidán na seznam.
4. Opakujte předchozí kroky pro přidání dalšího Security Serveru, pokud jsou k dispozici nebo jsou-li potřeba.

Pro nastavení priority Security Serveru:

1. Pomocí šipek nahoru a dolů dostupných ve sloupci **Akce** můžete zvýšit nebo snížit prioritu každého Security Serveru.

   Při přiřazování více Security Serverů má ten nejvyšší v seznamu nejvyšší prioritu a bude vybrán jako první. Pokud tento Security Server není k dispozici nebo je přetížen, je vybrán další Security Server. Skenování provozu je přesměrováno na první Security Server, který je k dispozici a má vhodné zatížení.

2. Vyberte **První připojení k Security Server nainstalovanému na stejném fyzickém hostiteli, je-li k dispozici, bez ohledu na přiřazenou prioritu** pro rovnoměrné rozdělení koncových bodů a pro optimalizovanou latenci. Pokud tento Security Server není k dispozici, bude zvolen Security Server ze seznamu v pořadí podle priority.

   Důležité
   Tato možnost funguje pouze s Security Server a pouze pokud je GravityZone integrována do virtualizovaného prostředí.

Pro odstranění Security Server ze seznamu, klikněte na tlačítko ⊗ **Odstranit** ve sloupci **Akce**

Nastavení Security Server

Při přiřazování politik pro Security Servery lze nakonfigurovat následující nastavení:

- **Omezit počet souběžných skenování na vyžádání**.

  Spuštění několika skenování na vyžádání na virtuálních strojích se sdíleným datastorem může vyvolat antimalwarové bouře. Chcete-li tomu zabránit a povolit spuštění pouze určitého počtu skenovacích úloh:

  1. Vyberte možnost **Omezit počet souběžných skenů na vyžádání**.
  2. Z rozevírací nabídky vyberte úroveň povolených souběžných úloh skenu. Můžete si vybrat předdefinovanou úroveň nebo zadat vlastní hodnotu.

     Vzorec pro nalezení maximálního limitu skenovacích úloh pro každou předdefinovanou úroveň je: `N = a x MAX(b ; vCPUs - 1)`, kde:

     - `N` = maximální limit úloh skenování
     - `a` = multiplikační koeficient, který má následující hodnoty: `1` - pro nízký; `2` - pro střední; `4` - pro vysoký

- Funkce `MAX(a;b)` vrací maximální počet míst dostupných pro skenování na Security Server.
- `b` = výchozí počet slotů pro sken na vyžádání, který je nyní nastaven na čtyři.
- `vCPUs` = počet virtuálních procesorů přiřazených k Security Serveru.

Například:

Pro Security Server s 12 CPU a vysokým limitem pro souběžné skenování, je limit:

`N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` souběžných skenovacích úloh na vyžádání.

- **Povolit přiřazení pravidel pro multiplatformní Security Server**

  Vyberte, jak by se měl Security Server zachovat, když jeho hostitel vstoupí do režimu údržby:

  - Pokud je to povoleno, Security Server zůstává vázán na hostitele a GravityZone ho vypne. Po ukončení údržby GravityZone automaticky restartuje Security Server.

    Toto je výchozí chování

  - Pokud je to zakázáno, Security Server je přesunut na jiného hostitele a pokračuje ve spuštění. V tomto případě se název Security Server změní v Control Center tak, aby směřoval na předchozího hostitele. Změna názvu trvá, dokud se Security Server nepřesune zpět na svého nativního hostitele.

    Pokud jsou zdroje nedostatečné, Security Server by se mohl dostat na hostitele, kde už je jiný Security Server nainstalovaný.

    Důležité
    Tato volba nemá žádný účinek, pokud Security Server používá také HVI.

- **Použit SSL**

  Tuto možnost povolte, pokud chcete šifrovat spojení mezi cílovými koncovými body a určenými appliancemi Security Server.

  Ve výchozím nastavení GravityZone používá bezpečnostní certifikáty s vlastním podpisem. Můžete je změnit pomocí vlastních certifikátů na stránce **Konfigurace**

> Certifikáty v Control Center. Další informace naleznete v kapitole „Konfigurace nastavení Control Center“ v Instalační příručce.

- **Komunikace mezi Security Servery a GravityZone**

  V této sekci můžete definovat své preference pro proxy pro komunikaci mezi zvolenými stroji Security Server a GravityZone.

  - **Ponechat instalační nastavení** pro použití stejných nastavení proxy, která jsou definována v instalačním balíčku.
  - **Použít proxy definovanou v sekci Obecné** pro použití nastavení proxy definovaného v současném pravidle pod sekcí **Obecné > Nastavení**.
  - **Nepoužívat proxy**, pokud cílové koncové body nekomunikují s konkrétními komponentami Bitdefender přes proxy.

7.2.4. Sandbox Analyzer

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery

Sandbox Analyzer poskytuje silnou ochrannou vrstvu proti pokročilým hrozbám díky tomu, že provádí automatickou hloubkovou analýzu podezřelých souborů, které ještě nejsou v signaturách antimalwarové ochrany Bitdefender.

V této části můžete nakonfigurovat následující položky:

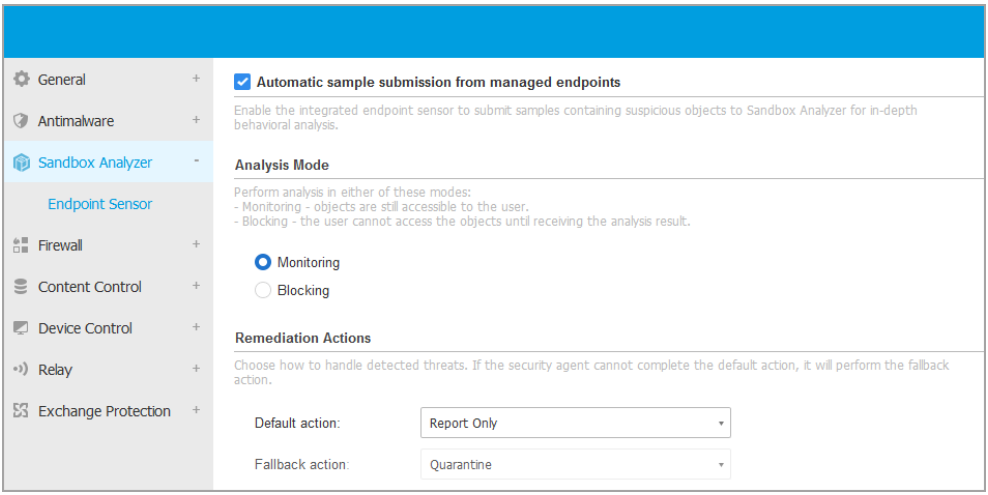
- Odeslání pomocí koncového senzoru
- Podání prostřednictvím síťového senzoru
- Podání prostřednictvím senzoru ICAP
- Nastavení správce karantény(Sandbox)

V nastavení zásad můžete také nakonfigurovat automatické odesílání z centralizované karantény. Více informací naleznete na „Centralizovaná karanténa“ (str. 279).

Podrobnosti o ručním odesílání naleznete v části „Ruční odeslání“ (str. 523). Podrobnosti o odesílání prostřednictvím rozhraní API naleznete v kapitolách **Sandbox** a **Sandbox Portal** v GravityZone Průvodce API (On-Premises) .

Senzor koncového bodu

Bitdefender Endpoint Security Tools může fungovat jako zdroj informací z koncových bodů Windows pro Sandbox Analyzer



Politiky > Sandbox Analyzer > Senzor koncových bodů

Chcete-li nakonfigurovat automatické odesílání pomocí senzoru koncového bodu:

1. V části **Nastavení připojení** vyberte jednu z možností:
   - **Use Cloud Sandbox Analyzer** - senzor koncového bodu odešle vzorky do Sandbox Analyzer hostovaného u společností Bitdefender, v závislosti na vaší oblasti.
   - **Použít místní instanci analyzátoru Sandbox** - snímač koncového bodu odešle vzorky do instance Sandbox Analyzer On-Premises. Z rozbalovací nabídky vyberte požadovanou instanci Sandbox Analyzer.

   Pokud máte síť za proxy serverem nebo bránou firewall, můžete nakonfigurovat proxy server pro připojení k Sandbox Analyzer zaškrtnutím políčka **Use proxy configuration** .

   Je nutné vyplnit následující pole:
   - **Server** - IP proxy serveru.
   - **Port** - port, který slouží k připojení k proxy serveru.

- **Username** - uživatelské jméno rozpoznávané proxy serverem.
- **Password** - platné heslo pro určeného uživatele.

2. Vyberte **Automatické předávání vzorků pro spravované koncové body (Automatic sample submission from managed endpoints)** označte tuto volbu v rámečku pro zapnutní automatického předávání podezdřelých vzorků souborů do Sandbox Analyzeru.

   Důležité

   - Sandbox Analyzer vyžaduje Skenování při zápisu (On-Access). Ujistěte se, že máte povolený modul **Antimalware > Skenování při přístupu**.
   - Sandbox Analyzer používá stejné cíle a výjimky jako jsou definovány v **Antimalware > Skenování při zápisu (On-Access)**. Při konfiguraci Sandbox Analyzer pečlivě prohlédněte nastavení Skenování při zápisu (On-Access).
   - Pro zabránění falešným poplachům (chybná detekce legitimních aplikací) můžete nastavit výjimky pomocí jména souboru, přípony, velikosti a cesty k souboru. Pro více informací o Skenování při přístupu se odkažte na „Antimalware“ (str. 251).
   - Limit velikosti pro nahrávání je pro každý soubor nebo archiv 50 MB.

3. Vyberte **Režim analýzy**. K dispozici jsou dvě možnosti:
   - **Monitorování**. Uživatel má během sandboxové analýzy přístup k souboru, ale je doporučeno ho nespouštět, dokud neobdrží výsledek analýzy.
   - **Blokování**. Uživatel nemůže spustit soubor, dokud se výsledek analýzy nevrátí na koncový bod z clusteru Sandbox Analyzer prostřednictvím Portálu Sandbox Analyzer.
4. Určete **Nápravná opatření**. Tyto jsou uplatněny, když Sandbox Analyzer rozpozná hrozbu. Pro každý režim analýzy máte k dispozici dvojité nastavení, skládající se z jedné výchozí akce a jedné záložní. Sandbox Analyzer nejprve provede výchozí akci, a následně záložní akci v případě, že tu první nebylo možné dokončit.

   Při prvním přístupu do této sekce jsou k dispozici následující nastavení:

   Poznámka
   Jako nejlepší postup doporučujeme používat nápravná opatření v tomto nastavení.

- V režimu **Monitorování** je výchozí akce **Pouze hlášení** a záložní akce je vypnuta.
- V režimu **Blokování** je výchozí akce **Karanténa**, zatímco záložní akce je **Odstranit**.

Sandbox Analyzer poskytuje následující nápravná opatření:

- **Dezinfikovat**. To odstraní malwarový kód z infikovaných souborů.
- **Odstranit**. To odstraní celý odhalený soubor z disku.
- **Karanténa**. To přesune odhalené soubory z jejich současného umístění do karanténní složky. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Soubory v karanténě můžete spravovat ze stránky **Karanténa** v Control Center.
- **Pouze hlášení**. Sandbox Analyzer nalezené hrozby pouze hlásí, aniž by na nich prováděl další akce.

Poznámka
V závislosti na výchozí akci může být záložní akce nedostupná.

5. Výchozí i záložní nápravné akce jsou nastaveny na režim **Pouze hlášení** .
6. V části **Content Prefiltering** upravte úroveň ochrany proti potenciálním hrozbám. Koncový bod má zabudovaný mechanismus filtrování obsahu, který určuje, zda je třeba podezřelý soubor spustit v Sandbox Analyzer.

   Podporované typy objektů jsou: aplikace, dokumenty, skripty, archivy, e-maily. Další podrobnosti o podporovaných typech objektů naleznete v části „Typy souborů podporované předfiltrováním obsahu při automatickém odesílání“ (str. 570).

   Pomocí hlavního přepínače v horní části seznamu hrozeb vyberte jedinečnou úroveň ochrany pro všechny typy objektů, nebo vyberte jednotlivé úrovně pro jemné doladění ochrany.

   Nastavení modulu na určitou úroveň povede k určitému počtu předložených vzorků:

   - **Permissive**. Senzor koncového bodu automaticky odesílá do Sandbox Analyzer pouze objekty s nejvyšší pravděpodobností škodlivého chování a ostatní objekty ignoruje.

- **Normal**. Senzor koncového bodu najde rovnováhu mezi odeslanými a ignorovanými objekty a odešle do Sandbox Analyzer oba objekty s vyšší a nižší pravděpodobností škodlivosti.
- **Aggressive**. Senzor koncového bodu odesílá do Sandbox Analyzer téměř všechny objekty, bez ohledu na jejich potenciální riziko.

Ve vyhrazeném poli můžete definovat výjimky pro typy objektů, které nechcete odeslat do Sandbox Analyzer

Můžete také definovat omezení velikost odeslaných objektů zaškrtnutím příslušného zaškrtávacího políčka a zadáním požadovaných hodnot mezi 1 KB a 50 MB.

7. V části **Detonační profil** můžete upravit úroveň složitosti analýzy chování a zároveň ovlivnit propustnost Sandbox Analyzer. Pokud je například nastaveno na **Vysoká**, Sandbox Analyzer provede přesnější analýzu na menším počtu vzorků ve stejném intervalu než na **Střední** nebo **Nízká**.

Sandbox Analyzer podporuje odesílání místních souborů prostřednictvím koncových bodů s rolí relay, které se mohou připojit k různým adresám Sandbox Analyzer portálu podle vašeho regionu. Více informací o konfiguraci relay nastavení naleznete v „Relay“ (str. 339).

Poznámka
Proxy nastavená v nastavení připojení Sandbox Analyzer obchází všechny koncové body s rolí relay.

Síťový Senzor

V této části můžete nakonfigurovat automatické odesílání vzorků síťového provozu do Sandbox Analyzer pomocí síťového senzoru. Tento modul vyžaduje nasazení a konfiguraci virtuálního zařízení pro zabezpečení sítě pomocí Sandbox Analyzer On-Premises.

Konfigurace automatického odesílání prostřednictvím síťového senzoru:

1. Zaškrtnutím políčka **Automatické odeslání vzorků ze síťového senzoru** povolíte automatické odesílání podezřelých souborů do Sandbox Analyzer.
2. V části **Content Prefiltering** upravte úroveň ochrany proti potenciálním hrozbám. Síťový senzor má zabudovaný mechanismus filtrování obsahu, který určuje, zda je třeba podezřelý soubor detonovat v Sandbox Analyzer.

Podporované typy objektů jsou: aplikace, dokumenty, skripty, archivy, e-maily. Další podrobnosti o podporovaných typech objektů naleznete v části „Typy souborů podporované předfiltrováním obsahu při automatickém odesílání“ (str. 570).

Použijte hlavní spínač navrchu seznamu hrozeb a zvolte jedinečnou úroveň ochrany pro všechny typy hrozeb, nebo zvolte individuální úrovně pro doladění zabezpečení.

Nastavení modulu na určitou úroveň povede k určitému počtu předložených vzorků:

- **Permissive**. Síťový senzor automaticky odesílá do Sandbox Analyzer pouze objekty s nejvyšší pravděpodobností škodlivého chování a ignoruje ostatní objekty.
- **Normal**. Síťový senzor najde rovnováhu mezi odeslanými a ignorovanými objekty a pošle Sandbox Analyzer oba objekty s vyšší a nižší pravděpodobností škodlivosti.
- **Aggressive**. Síťový senzor odesílá do Sandbox Analyzer téměř všechny objekty, bez ohledu na jejich potenciální riziko.

Ve vyhrazeném poli můžete definovat výjimky pro typy objektů, které nechcete odeslat do Sandbox Analyzer

Můžete také definovat omezení velikost odeslaných objektů zaškrtnutím příslušného zaškrtávacího políčka a zadáním požadovaných hodnot mezi 1 KB a 50 MB.

3. V části **Nastavení připojení** vyberte preferovanou instanci Sandbox Analyzer pro odesílání síťového obsahu.

   Pokud máte síť za proxy serverem nebo bránou firewall, můžete nakonfigurovat proxy server pro připojení k Sandbox Analyzer zaškrtnutím políčka **Use proxy configuration** .

   Je nutné vyplnit následující pole:

   - **Server** - IP proxy serveru.
   - **Port** - port, který slouží k připojení k proxy serveru.
   - **Username** - uživatelské jméno rozpoznávané proxy serverem.
   - **Password** - platné heslo pro určeného uživatele.

4. V části **Detonační profil** můžete upravit úroveň složitosti analýzy chování a zároveň ovlivnit propustnost Sandbox Analyzer. Pokud je například nastaveno na **Vysoká**, Sandbox Analyzer provede přesnější analýzu na menším počtu vzorků ve stejném intervalu než na **Střední** nebo **Nízká**.

ICAP Sensor

V této části můžete nakonfigurovat automatické odesílání do Sandbox Analyzer pomocí senzoru ICAP.

Poznámka
Sandbox Analyzer vyžaduje Security Server nakonfigurovaný pro skenování zařízení připojených k síti (NAS), která používají protokol ICAP. Podrobnosti viz„Ochrana Úložiště“ (str. 376)

1. Zaškrtnutím políčka **Automatické odeslání vzorků ze senzoru ICAP** povolíte automatické odesílání podezřelých souborů do Sandbox Analyzer.
2. V části **Content Prefiltering** upravte úroveň ochrany proti potenciálním hrozbám. Síťový senzor má zabudovaný mechanismus filtrování obsahu, který určuje, zda je třeba podezřelý soubor detonovat v Sandbox Analyzer.

   Podporované typy objektů jsou: aplikace, dokumenty, skripty, archivy, e-maily. Další podrobnosti o podporovaných typech objektů naleznete v části „Typy souborů podporované předfiltrováním obsahu při automatickém odesílání“ (str. 570).

   Použijte hlavní spínač navrchu seznamu hrozeb a zvolte jedinečnou úroveň ochrany pro všechny typy hrozeb, nebo zvolte individuální úrovně pro doladění zabezpečení.

   Nastavení modulu na určitou úroveň povede k určitému počtu předložených vzorků:

   - **Permissive**. Senzor ICAP automaticky odesílá do Sandbox Analyzer pouze objekty s nejvyšší pravděpodobností škodlivosti a zbytek objektů ignoruje.
   - **Normal**. Senzor ICAP najde rovnováhu mezi odeslanými a ignorovanými objekty a pošle do Sandbox Analyzer oba objekty s vyšší a nižší pravděpodobností škodlivosti.
   - **Aggressive**. Senzor ICAP odesílá do Sandbox Analyzer téměř všechny objekty, bez ohledu na jejich potenciální riziko.

Ve vyhrazeném poli můžete definovat výjimky pro typy objektů, které nechcete odeslat do Sandbox Analyzer

Můžete také definovat omezení velikost odeslaných objektů zaškrtnutím příslušného zaškrtávacího políčka a zadáním požadovaných hodnot mezi 1 KB a 50 MB.

3. V části **Nastavení připojení** vyberte preferovanou instanci Sandbox Analyzer pro odesílání síťového obsahu.

   Pokud máte síť za proxy serverem nebo bránou firewall, můžete nakonfigurovat proxy server pro připojení k Sandbox Analyzer zaškrtnutím políčka **Use proxy configuration** .

   Je nutné vyplnit následující pole:

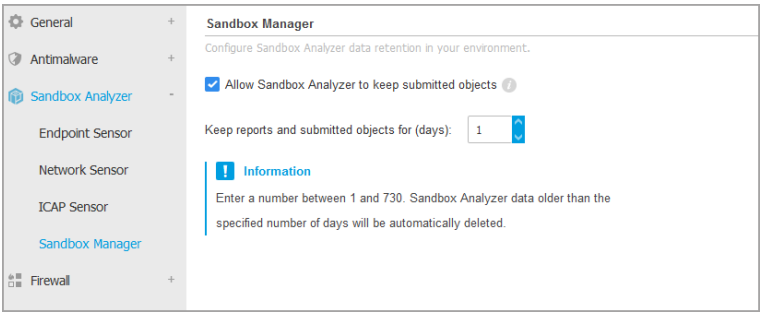
   - **Server** - IP proxy serveru.
   - **Port** - port, který slouží k připojení k proxy serveru.
   - **Username** - uživatelské jméno rozpoznávané proxy serverem.
   - **Password** - platné heslo pro určeného uživatele.

4. V části **Detonační profil** můžete upravit úroveň složitosti analýzy chování a zároveň ovlivnit propustnost Sandbox Analyzer. Pokud je například nastaveno na **Vysoká**, Sandbox Analyzer provede přesnější analýzu na menším počtu vzorků ve stejném intervalu než na **Střední** nebo **Nízká**.

Sandbox Manager

V této části nakonfigurujete uchovávání dat pro své instance Sandbox Analyzer:

- Zaškrtněte políčko **Povolit Sandbox Analyzer uchovat odeslané objekty** . Toto nastavení umožňuje použít možnost **Znovu odeslat k analýze** v oblasti odeslaných karet rozhraní pro hlášení Sandbox Analyzer.
- Určete počet dní, po které má aplikace Sandbox Analyzer uchovávat zprávy a odeslané objekty v datovém úložišti. Maximální hodnota, kterou můžete zadat, je 730. Po uplynutí definovaného období budou všechna data vymazána.



Politiky > Sandbox Analyzer > Sandbox Manager

7.2.5. Firewall

Poznámka
Tento modul je k dispozici pro Windows pro pracovní stanice.

Firewall chrání váš koncový bod před pokusy o neautorizované připojení zvenku i zevnitř.

Funkčnost Firewallu závisí na síťových profilech. Profily jsou založeny na úrovních důvěryhodnosti, které musí být určeny pro každou síť.

Firewall rozpozná každé nové připojení, porovná informace o adaptéru tohoto připojení s informacemi z existujících profilů, a aplikuje správný profil. Podrobné informace o aplikaci profilů naleznete na „Síťová nastavení“ (str. 301).

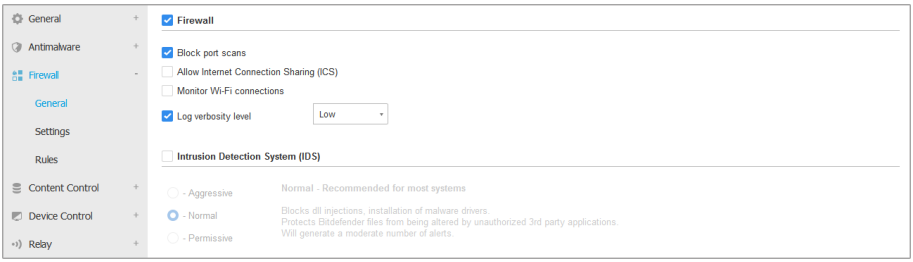
Důležité
Modul Firewall je dostupný pouze pro podporované pracovní stanice s Windows.

Nastavení jsou uspořádána do následujících sekcí:

- Hlavní
- Nastavení
- Pravidla

Hlavní

V této sekci můžete povolit nebo zakázat Bitdefender Firewall a konfigurovat obecná nastavení.



Politiky Počítačů a Virtuálních Strojů - Nastavení Firewallu

- **Firewall.** Použijte zaškrtávací pole pro zapnutí nebo vypnutí Firewallu.

  Varování
  Pokud vypnete firewallovou ochranu, počítače se stanou zranitelnými vůči síťovým a internetovým útokům.

- **Blokovat skenování portů.** Skenování portů často používají hackeři, aby zjistili, které porty jsou na vašem počítači otevřené. Pokud najdou hůře zabezpečený nebo zranitelný port, mohli by proniknout do vašeho počítače.
- **Povolit Sdílení internetového připojení (ICS).** Zvolte tuto možnost pro nastavení firewallu, aby povolil přenos Sdílení internetového připojení.

  Poznámka
  Touto možností není ICS automaticky povoleno v systému uživatele.

- **Sledovat WiFi připojení.** Bezpečnostní agent Bitdefender může informovat uživatele připojené k síti Wi-Fi, když se k ní připojí nový počítač. Pro zobrazení těchto oznámení na obrazovce uživatele, zvolte tuto možnost.
- **Úroveň výmluvnosti protokolu.** Bezpečnostní agent Bitdefender vede protokol událostí týkajících se používání modulu Firewall (povolení/zakázání firewallu, blokování provozu, úprava nastavení), nebo vygenerovaný na základě činností zjištěných tímto modulem (skenování portů, blokování pokusů o připojení nebo přenosu v souladu s pravidly. Zvolte možnost z **Úrovně výmluvnosti protokolu** pro určení, jaké informace by měl protokol zahrnovat.
- **Systém detekce průniků.** Systém detekce průniků monitoruje systém na podezřelé aktivity (například neoprávněné pokusy o změnu souborů Bitdefender, DLL injekce, keyloggerové pokusy atd.).

Poznámka
Nastavení politik Intrusion Detection Systemu (IDS) jsou pouze aplikovatelná na Endpoint Security (legacy security agentovi). Bitdefender Endpoint Security Tools agent má integrovanou funkci Host-Based Intrusion Detection Systemu zabudovanou přímo v modulu Advanced Threat Control (ATC).

Pro nastavení Systému detekce průniků:

1. Použijte zaškrtávací pole pro zapnutí nebo vypnutí Systému detekce průniků.
2. Zvolte úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (agresivní, normální nebo tolerantní). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

Pro zabránění tomu, aby byla legitimní aplikace odhalena Systémem detekce úniků, přidejte této aplikaci **Pravidlo výjimky procesu ATC/IDS** v sekci **Antimalware > Nastavení > Vlastní výjimky**.

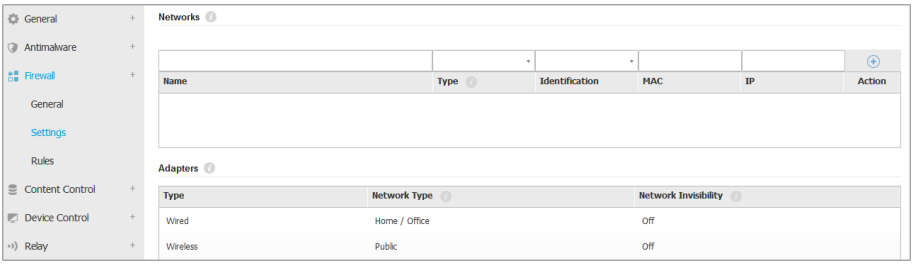
Důležité
Intrusion Detection System je pouze k dispozici pro Endpoint Security klienty.

Nastavení

Firewall automaticky aplikuje profil na základě úrovně důvěryhodnosti. Pro síťová připojení můžete mít různé úrovně důvěryhodnosti v závislosti na síťové architektuře, nebo na typu adaptéru používaného k navázání síťového připojení. Na příklad, pokud máte v síti vaší firmy podsítě, můžete pro každou z nich nastavit úroveň důvěryhodnosti.

Nastavení jsou uspořádána pod následujícími kartami:

- Sítě
- Adaptéry



Práva - Nastavení Firewallu

Síťová nastavení

Pokud chcete, aby Firewall aplikoval různé profily pro několik síťových úseků ve vaší firmě, musíte specifikovat spravované sítě v kartě **Sítě**. Vyplňte pole v tabulce **Sítě** podle popisu níže:

- **Název.** Zadejte jméno, podle kterého síť v seznamu poznáte.
- **Typ.** Zvolte z nabídky profil, který bude přiřazen k síti.

  Bezpečnostní agent Bitdefender automaticky aplikuje jeden ze čtyř profilů každému zjištěnému připojení k síti na koncovém bodě pro určení základních možností filtrování. Typy profilů jsou:

  - **Důvěryhodná** síť. Vypne bránu firewall pro příslušný adaptér.
  - Síť **Doma/V kanceláři**. Povolí všechen příchozí a odchozí provoz na počítačích v místní síti, zatímco ostatní provoz je filtrován.
  - **Veřejná** síť. Veškerý provoz je filtrovaný.
  - **Nedůvěryhodná** síť. Kompletně zablokuje síťový a internetový provoz skrze příslušné adaptéry.
- **Identifikace.** Z nabídky zvolte metodu, prostřednictvím které bude síť rozpoznána bezpečnostním agentem Bitdefender. Sítě mohou být rozpoznány pomocí tří metod: **DNS**, **Brána** a **Síť**.
  - **DNS**: identifikuje všechny koncové body pomocí určeného DNS.
  - **Brána**: identifikuje všechny koncové body komunikující prostřednictvím určené brány.
  - **Síť**: identifikuje všechny koncové body z určeného síťového úseku, definovaného svou síťovou adresou.

- **MAC**. Použijte toto pole pro určení MAC adresy DNS serveru nebo brány, která vymezuje síť, podle toho, jakou identifikační metodu jste zvolili.

  Adresu MAC musíte zadat ve formátu šestnáctkové soustavy, rozdělené pomlčkami (-) a dvojtečkami (:). Například, obě `00-50-56-84-32-2b` a `00:50:56:84:32:2b` jsou platné adresy.

- **IP.** Použijte toto pole pro určení specifických IP adres v síti. Formát IP závisí na identifikační metodě následovně:
  - **Síť.** Zadejte číslo sítě ve formátu CIDR. Například, `192.168.1.0/24`, kde `192.168.1.0` je adresa sítě a `/24` je maska sítě.
  - **Brána.** Zadejte IP adresu brány.
  - **DNS.** Zadejte IP adresu DNS serveru.

Po definování sítě klikněte na tlačítko **Přidat** na pravé straně tabulky a přidejte ji do seznamu.

Nastavení adaptérů

Pokud je zjištěna síť, která není určena v tabulce **Sítě**, bezpečnostní agent Bitdefender zjistí typ síťového adaptéru a přiřadí k připojení odpovídající profil.

Pole tabulky **Adaptéry** jsou popsány následovně:

- **Typ.** Zobrazuje typ síťových adaptérů. Bezpečnostní agent Bitdefender dokáže rozpoznat tři přednastavené typy adaptérů: **Kabelový**, **Bezdrátový** a **Virtuální** (Soukromá virtuální síť).
- **Typ sítě.** Popisuje síťový profil přiřazený k určitému typu adaptéru. Síťové profily jsou popsány v sekci síťových nastavení. Kliknutím na pole se síťovým typem můžete změnit nastavení.

  Pokud zvolíte **Nechat rozhodnout Windows**, bezpečnostní agent Bitdefender bude přiřazovat každé nové síti, rozpoznané po aplikování pravidla, profil pro firewall na základě klasifikace sítí ve Windows, a bude ignorovat nastavení z tabulky **Adaptéry**.

  Pokud detekce na základě Správce sítě Windows selže, bude proveden pokus o základní detekci. Je použit obecný profil, ve kterém je síťový profil nastaven jako **Veřejný** a nastavení stealth jsou **Zapnutá**.

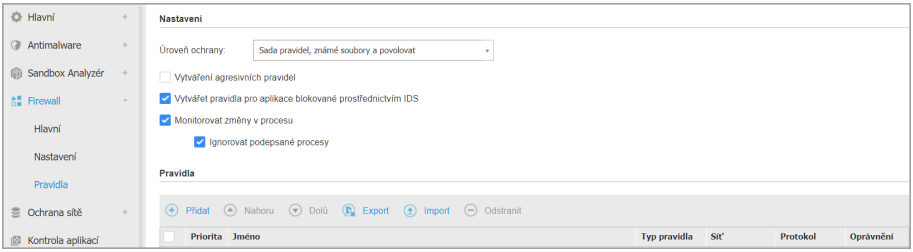
  Jakmile se koncový bod zapojený do Active Directory spojí s doménou, tak se nastaví jeho firewallový profil na **Home/Office** a skrytá (stealth) nastavení se

přepnou na **Vzdálená (Remote)**. Pokud se počítač nenachází v doméně, tato možnost není uplatnitelná.

- **Zjišťování sítě.** Skryje počítač před škodlivým softwarem a hackery v síti nebo na internetu. Nastavte viditelnost počítače v síti dle potřeby pro každý typ adaptéru tak, že zvolíte jednu z následujících možností:
  - **Ano.** Kdokoli z místní sítě nebo Internetu může použít na váš počítač příkaz ping a detekovat ho.
  - **Ne.** Váš počítač je neviditelný z místní sítě i Internetu.
  - **Vzdálený.** Počítač nemůže být objeven z internetu. Kdokoli z místní sítě nebo Internetu může použít na váš počítač příkaz ping a detekovat ho.

Pravidla

V této sekci můžete nastavit přístup aplikací k síti a pravidla datového přenosu vynucené firewallem. Mějte na paměti, že použitelná nastavení platí pouze pro **Doma/V kanceláři** a **Veřejné** profily.



Politiky Počítačů a Virtuálních Strojů - nastavení pravidel Firewallu

Nastavení

Můžete nastavit následující parametry:

- **Úroveň ochrany.** Zvolená úroveň zabezpečení definuje rozhodovací logiku firewallu používanou v případě, že aplikace žádají přístup k síti a internetovým službám. K dispozici jsou následující možnosti:

  Sada pravidel a povolit

  Aplikujte existující pravidla firewallu a automaticky povolte všechny ostatní pokusy o připojení. Pro každý nový pokus o připojení je vytvořeno pravidlo, které je přidáno do sady pravidel.

Sada pravidel a ptát se
Aplikujte existující pravidla firewallu a vybídněte uživatele k akci pro všechny ostatní pokusy o připojení. Na obrazovce uživatele se zobrazí okno s upozorněním obsahující podrobné informace o neznámém pokusu o připojení. Pro každý nový pokus o připojení je vytvořeno pravidlo, které je přidáno do sady pravidel.

Sada pravidel a zakazovat
Aplikujte existující pravidla firewallu a automaticky zakažte všechny ostatní pokusy o připojení. Pro každý nový pokus o připojení je vytvořeno pravidlo, které je přidáno do sady pravidel.

Sada pravidel, známé soubory a povolovat
Aplikujte existující pravidla pro firewall, automaticky povolte pokusy o připojení známých aplikací a automaticky povolte všechny ostatní neznámé pokusy o připojení. Pro každý nový pokus o připojení je vytvořeno pravidlo, které je přidáno do sady pravidel.

Sada pravidel, známé soubory a ptát se
Aplikujte existující pravidla pro firewall, automaticky povolte pokusy o připojení známých aplikací a vybídněte uživatele k reakci pro všechny ostatní neznámé pokusy o připojení. Na obrazovce uživatele se zobrazí okno s upozorněním obsahující podrobné informace o neznámém pokusu o připojení. Pro každý nový pokus o připojení je vytvořeno pravidlo, které je přidáno do sady pravidel.

Sada pravidel, známé soubory a zakazovat
Aplikujte existující pravidla pro firewall, automaticky povolte pokusy o připojení známých aplikací a automaticky zakažte všechny ostatní neznámé pokusy o připojení. Pro každý nový pokus o připojení je vytvořeno pravidlo, které je přidáno do sady pravidel.

Poznámka
Známé soubory představují rozsáhlou sbírku bezpečných, důvěryhodných aplikací, která je sestavena a pravidelně udržována společností Bitdefender.

- **Vytváření agresivních pravidel.** Zvolením této možnosti bude firewall vytvářet pravidla pro každý z různých procesů, který otevře aplikaci požadující přístup k síti nebo internetu.

- **Vytvářet pravidla pro aplikace blokované prostřednictvím IDS.** Zvolením této možnosti bude firewall automaticky tvořit pravidlo **Zakázat** pokaždé, když Systém detekce úniků zablokuje aplikaci.
- **Monitorovat změny v procesu.** Zvolte tuto možnost, pokud chcete kontrolovat pro každou aplikaci snažící se o přístup k internetu, jestli byla změněna od chvíle, kdy k ní bylo přiřazeno pravidlo kontrolující její přístup k internetu. Pokud aplikace byla změněna, bude vytvořeno nové pravidlo v souladu se stávající úrovní zabezpečení.

  Poznámka

  Aplikace jsou obvykle měněny aktualizacemi. Je tu však riziko, že mohou být změněny malwarovými aplikacemi za účelem infikování místního počítače a ostatních počítačů v síti.

  Podepsané aplikace by měly být důvěryhodné a mít vyšší úroveň zabezpečení. Můžete vybrat **Ignorovat podepsané procesy** pro automatické povolení připojení se k internetu pro změněné podepsané aplikace.

Pravidla

V tabulce Pravidla je uveden seznam existujících pravidel pro firewall, s důležitými informacemi o každém z nich:

- Název pravidla nebo aplikace, ke které odkazuje.
- Protokol, na který se pravidlo vztahuje.
- Akce pravidla (povolit nebo zakázat paket).
- Akce, které můžete na pravidle provádět.
- Priorita pravidla.

Poznámka

Jedná se o pravidla brány firewall explicitně vynucovaná zásadami. Další pravidla mohou být na počítačích nakonfigurována v důsledku použití nastavení brány firewall.

Řada výchozích pravidel firewallu vám pomůže snadno povolit nebo zamítnout oblíbené typy provozu. Vyberte požadovanou možnost z nabídky **Oprávnění** .

Příchozí ICMP/ICMPv6
Povolení nebo zakázání zpráv ICMP/ICMPv6. Zprávy ICMP často používají hackeři k provádění útoků proti počítačovým sítím. Ve výchozím stavu je tento typ přenosu povolen.

Příchozí připojení ke vzdálené ploše
Povolení nebo zakázání přístupu jiných počítačů pomocí připojení ke vzdálené ploše. Ve výchozím stavu je tento typ přenosu povolen.

Odesílání emailů
Povolit nebo zakázat posílání emailů přes SMTP. Ve výchozím stavu je tento typ přenosu povolen.

HTTP - procházení webu
Povolení nebo zakázání procházení webu pomocí protokolu HTTP. Ve výchozím stavu je tento typ přenosu povolen.

Síťový Tisk
Povolte nebo zakažte přístup k tiskárnám v jiné místní síti. Ve výchozím stavu je tento typ přenosu zakázán.

HTTP/FTP provoz Průzkumníka Windows
Povolení nebo zakázání HTTP a FTP provozu z Průzkumníka Windows. Ve výchozím stavu je tento typ přenosu zakázán.

Kromě výchozích pravidel můžete vytvořit přídavná firewallová pravidla pro ostatní aplikace nainstalované na koncových bodech. Toto nastavení je ale určeno pouze pro správce s pokročilými síťovými dovednostmi.

Pro vytvoření a nastavení nového pravidla klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Více podrobností naleznete v následujícím tématu.

Pro odstranění pravidla ze seznamu ho vyberte a klikněte na tlačítko ⊖ **Odstranit** v horní části tabulky.

Poznámka
Výchozí pravidla pro firewall nemůžete mazat ani upravovat.

Nastavení Vlastních pravidel

Můžete nastavit dva druhy firewallových pravidel:

- **Pravidla na bázi aplikací.** Tato pravidla platí pro specifický software, který se nachází na klientských počítačích.

- **Pravidla na bázi připojení.** Tato pravidla platí pro jakoukoli aplikaci nebo službu, která využívá určitého připojení.

Pro vytvoření a nastavení nového pravidla klikněte na tlačítko ⊕ **Přidat** v horní části tabulky a z nabídky zvolte požadovaný typ pravidla. Pro úpravu existujícího pravidla klikněte na jeho jméno.

Můžete konfigurovat následující nastavení:

- **Jméno pravidla.** Zadejte jméno, pod kterým bude pravidlo přidáno do seznamu v tabulce s pravidly (například jméno aplikace, pro kterou pravidlo platí).
- **Cesta k aplikaci** (pouze pro pravidla na bázi aplikace). Musíte určit cestu k spustitelnému souboru aplikace na cílových počítačích.
  - Z nabídky zvolte přednastavené umístění a doplňte cestu dle potřeby. Například, pro aplikaci nainstalovanou ve složce `Program Files`, zvolte `%Program Files%` a doplňte cestu přidáním lomítka (\) a jména složky s aplikací.
  - Do pole úprav zadejte kompletní cestu. Pro jistotu, že je cesta platná na všech cílových počítačích, doporučujeme používat systémové proměnné (tam, kde je to vhodné).
- **Příkazový řádek** (pouze pro pravidla na bázi aplikací). Pokud chcete, aby bylo pravidlo uplatněno pouze, když je určená aplikace spuštěna se specifickým příkazem v rozhraní příkazového řádku Windows, zadejte příslušný příkaz do pole úprav. V opačném případě ho nechte nevyplněné.
- **MD5 aplikace** (pouze pro pravidla na bázi aplikace). Pokud chcete, aby pravidlo kontrolovalo integritu dat souborů aplikace na základě jejího MD5 hash kódu, zadejte ho do pole úprav. V opačném případě nechte pole nevyplněné.
- **Lokální adresa.** Specifikujte místní IP adresu a port, na které se pravidlo vztahuje. Pokud máte více než jeden síťový adaptér, můžete zrušit označení pole **Jakýkoli** a zadat konkrétní IP adresu. Stejným způsobem, pro filtrování připojení pro specifický port nebo řadu portů, zrušte označení pole **Jakýkoli** a do příslušného pole zadejte port nebo řadu portů.
- **Vzdálená adresa.** Specifikujte vzdálenou IP adresu a port, na které se pravidlo vztahuje. Pro filtrování příchozího a odchozího přenosu z konkrétního počítače, zrušte označení pole **Jakýkoli** a zadejte jeho IP adresu.
- **Použít toto pravidlo jen pro přímo připojené počítače.** Můžete filtrovat přístup podle Mac adresy.

- **Protokol.** Vyberte protokol IP, na který se pravidlo vztahuje.
  - Pokud chcete pravidlo aplikovat na všechny protokoly, vyberte možnost **Vše**.
  - Pokud chcete pravidlo aplikovat na protokol TCP, vyberte možnost **TCP**.
  - Pokud chcete pravidlo aplikovat na protokol UDP, vyberte možnost **UDP**.
  - Pokud chcete, aby pravidlo platilo pro konkrétní protokol, zvolte ho z nabídky **Jiné**.

    Poznámka
    Čísla protokolům IP přiděluje organizace Internet Assigned Numbers Authority (IANA). Kompletní seznam přidělených čísel protokolů IP najdete na adrese http://www.iana.org/assignments/protocol-numbers.

- **Směr.** Vyberte v nabídce směr provozu, na který se pravidlo vztahuje.

Směr	Popis
Odchozí	Pravidlo se použije pouze pro odchozí provoz.
Příchozí	Pravidlo se použije pouze pro příchozí provoz.
Obojí	Pravidlo se použije pro oba směry komunikace.

- **Verze IP.** Vyberte verzi IP (IPv4, IPv6 nebo jakoukoli), pro kterou se pravidlo uplatní.
- **Síť.** Vyberte typ sítě, na nějž se pravidlo vztahuje.
- **Oprávnění.** Vyberte jedno z dostupných oprávnění:

Oprávnění	Popis
Povolit	Specifikované aplikaci bude povolen přístup k síti/Internetu za určitých okolností.
Zakázat	Specifikované aplikaci bude zakázán přístup k síti/Internetu za určitých okolností.

Pro přidání pravidla klikněte na **Uložit**.

Použijte šipky na pravé straně tabulky pro nastavení priority vámi vytvořených pravidel. Pravidlo s vyšší prioritou je blíže k vrcholu seznamu.

Pravidla pro import a export

Pravidla brány firewall můžete exportovat a importovat a použít je v jiných zásadách nebo společnostech. Pro export pravidel:

1. V horní části tabulky pravidel klikněte na **Export** .
2. Uložte soubor CSV na váš počítač. V závislosti na nastavení vašeho prohlížeče se soubor může stáhnout automaticky, nebo budete vyzváni k jeho uložení do nějakého umístění.

Důležité

- Každý řádek v souboru CSV odpovídá jednomu pravidlu a má více polí.
- Pozice pravidel brány firewall v souboru CSV určuje jejich prioritu. Prioritu pravidla můžete změnit přesunutím celého řádku.

U výchozí sady pravidel můžete upravovat pouze následující prvky:

- **Priority** : Nastavte prioritu pravidla v libovolném pořadí přesunutím řádku CSV.
- **Oprávnění** : Upravte nastavení pole . `Oprávnění` pomocí dostupných oprávnění:
  - 1 pro **Povolit**
  - 2 pro **Odepřít**

Veškeré další úpravy se při importu zahodí.

U vlastních pravidel brány firewall jsou všechny hodnoty pole konfigurovatelné takto:

Pole	Název a Hodnota
`Typ pravidla`	**Typ pravidla**: 1 pro **Pravidlo aplikace** 2 pro **Pravidlo připojení**
`typ`	Hodnota tohoto pole je volitelná.

Pole	Název a Hodnota
`details.name`	**Jméno pravidla**
`details.applictionPath`	**Cesta aplikace** (pouze pro pravidla založená na aplikaci)
`details.commandLine`	**Příkazový řádek** (pouze pro pravidla založená na aplikaci)
`details.applicationMd5`	**Aplikace MD5** (pouze pro pravidla založená na aplikaci)
`settings.protocol`	**Protokol** 1 pro **Jakýkoli** 2 pro **TCP** 3 pro **UDP** 4 pro **Ostatní**
`settings.customProtocol`	Vyžadováno, pouze pokud je **Protokol** nastaven na **Ostatní** . Pokud jde o konkrétní hodnoty, zvažte tuto stránku . Hodnoty 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141- 143 nejsou podporovány.
`settings.direction`	**Směr** : 1 pro **Oba** 2 pro **příchozí** 3 pro **odchozí**
`settings.ipVersion`	**verze IP**: 1 pro **Jakýkoli** 2 pro **IPv4** 3 pro **IPv6**
`settings.localAddress.any`	**Místní adresa** je nastavena na **Libovolná** :

Pole	Název a Hodnota
	1 pro Správně 0 nebo prázdné pro Špatně
`settings.localAddress.ipMask`	**Místní adresa** je nastavena na **IP nebo IP/Mask**
`settings.remoteAddress.portRange`	**Vzdálená adresa** je nastavena na **Port nebo rozsah portů**
`settings.directlyConnected.enable`	**Použít pravidlo pouze pro přímo připojené počítače** : 1 pro povoleno 0 pro prázdné nebo deaktivované
`settings.directlyConnected.remoteMac`	**Použít pravidlo pouze pro přímo připojené počítače** s filtrem **MAC adres** .
`permission.home`	**Síť** , na kterou se pravidlo vztahuje, je **Doma/Kancelář** : 1 pro Správně 0 pro prázdné nebo Falešné
`permission.public`	**Síť** , na kterou se pravidlo vztahuje, je **Veřejná** : 1 pro Správně 0 pro prázdné nebo Falešné
`permission.setPermission`	Dostupná oprávnění: 1 pro **Povolit** 2 pro **Odepřít**

Pro import pravidel:

1. V horní části tabulky pravidel klikněte na **Import** .
2. V novém okně klikněte na **Přidat** a vyberte soubor CSV.
3. Klikněte na tlačítko **Save**. V tabulce jsou zobrazena platná pravidla.

7.2.6. Ochrana sítě

V části Ochrana sítě můžete nakonfigurovat předvolby týkající se filtrování obsahu, ochrany dat pro činnosti uživatele včetně procházení webu, e-mailových a softwarových aplikací a detekce technik útoku na síť, které se snaží získat přístup na konkrétních koncových bodech. Můžete omezit nebo povolit přístup k webu a používání aplikací, nastavit skenování přenosu a pravidla pro antiphishing a ochranu dat.

Mějte prosím na paměti, že nakonfigurovaná nastavení síťové ochrany budou platit pro všechny uživatele přihlášené k cílovým počítačům.

Nastavení jsou uspořádána do následujících sekcí:

- Hlavní
- Kontrola obsahu
- Ochrana webu
- Síťové útoky

Poznámka

- Modul Content Control je k dispozici pro:
  - Windows pro pracovní stanice
  - macOS
- Modul Network Attack Defense je k dispozici pro:
  - Windows pro pracovní stanice

Důležité

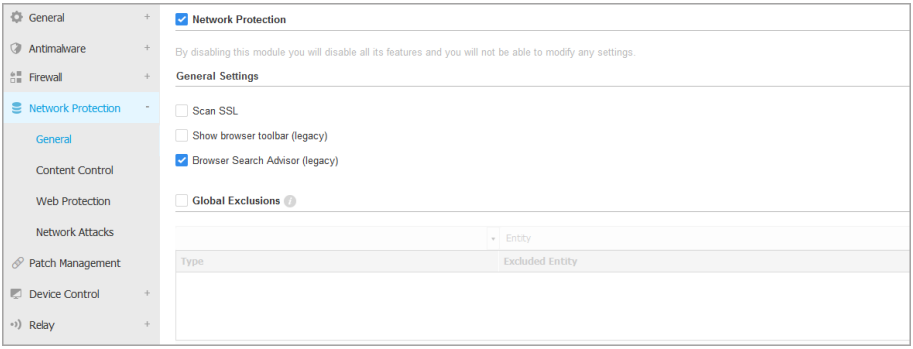
V případě macOS se Content Control opírá o rozšířené jádro (kernel extension). Instalace rozšíření jádra (kernel extensions) vyžaduje vaše schválení na macOS High Sierra (10.13) a novější. Systém upozorní uživatele o tom, že rozšíření systému od Bitdefender bylo zablokováno. uživatel může funkci povolit v předvolbách **Bezpečnost & Soukromí**. Dokud uživatel nepovolí rozšíření systému Bitdefender, tak nebudou moduly fungovat a uživatelské rozhraní (user interface)Endpoint Security for Mac bude ukazovat kritickou chybu a bude se dotazovat na schválení.
K eliminaci zásahu uživatele můžete předschválit rozšíření pro kernel Bitdefender pomocí Whitelistování s použitím nástroje správy mobilních zařízení. Pro detaily o rozšíření pro kernel Bitdefender, přejděte do článek KB.

Hlavní

Na této stránce můžete nakonfigurovat možnosti, jako je povolení nebo zakázání určitých funkcí a nastavení vyjímek.

Nastavení jsou uspořádána do následujících sekcí:

- Obecná nastavení
- Souhrnné výjimky



Zásady pro počítače a virtuální stroje - Ochrana sítě - Obecné

Obecná nastavení

- **Skenovat SSL**. Zvolte tuto možnost, pokud chcete vyšetřit síťový provoz Secure Sockets Layer (SSL) pomocí ochranných modulů bezpečnostního agenta společnosti Bitdefender.
- **Zobrazit panel nástrojů prohlížeče (starší)**. Panel nástrojů Bitdefender informuje uživatele o hodnocení internetových stránek, které navštěvují. Panel nástrojů Bitdefender není obyčejný panel nástrojů v prohlížeči. Jediná věc, kterou přidává do prohlížeče, je malý posuvník na vrchu každé webové stránky. Kliknutím na posuvník se otevře panel nástrojů.

  Podle toho, jak Bitdefender zařadí webovou stránku, se na levé straně panelu nástrojů zobrazí jedno z následujících hodnocení:

  – Na červeném pozadí se zobrazí zpráva "Tato stránka není bezpečná."

  – Na oranžovém pozadí se zobrazí zpráva "Doporučujeme opatrnost".

  – Na zeleném pozadí se zobrazí zpráva "Tato stránka je bezpečná".

  Poznámka

  – Tato volba není dostupná pro macOS.

– Tato volba je odebrána ze systému Windows, počínaje novou instalací Bitdefender Endpoint Security Tools verze 6.6.5.82.

- **Poradce pro vyhledávání v prohlížeči (starší).** Poradce pro vyhledávání hodnotí výsledky vyhledávání z Google, Bing a Yahoo!, stejně tak jako odkazy z Facebooku a Twitteru tak, že před každý výsledek umístí ikonu. Užité ikony a jejich význam:

  Tuto webovou stránku byste neměli navštěvovat.
  Tato webová stránka může obsahovat nebezpečný obsah. Pokud se rozhodnete ji navštívit, buďte opatrní.
  Návštěva této stránky je bezpečná.

  Poznámka
  – Tato volba není dostupná pro macOS.
  – Tato volba je odebrána ze systému Windows, počínaje novou instalací Bitdefender Endpoint Security Tools verze 6.6.5.82.

Souhrnné výjimky

Pokud jsou povoleny možnosti **Ochrana Sítě** , můžete se rozhodnout přeskočit určitý provoz skenovaný na malware.

Poznámka
Tyto výjimky platí pro **Skenování provozu** a **Antiphishing** , v části **Ochrana webu** , a **Network Attack Defense** , v části **Síťové útoky** . Vyloučení **ochrany dat** lze konfigurovat samostatně v sekci **Řízení obsahu** .

Definování výjimek:

1. Z nabídky zvolte typ výjimky.
2. Na základě typu výjimky definujte jednotku přenosu, která má být vyloučena ze skenování, následujícím způsobem:
   - **IP/mask** Zadejte adresu IP nebo masku IP, u které nechcete prověřovat příchozí a odchozí provoz, včetně technik útoku na síť.
   - **URL**. Vynechá ze skenování zadané webové adresy. Zohledněte to, že vyjímky pro skeny postavené na URL (URL-based scan exclusions) se aplikují jinak pro HTTP oproti HTTPS spojením, jak je vysvětleno dále.

Můžete definovat vyjímky postavené na URL adresách (URL-based scan exclusion) tímto způsobem:

– Zadejte konkrétní URL, jako je `www.example.com/example.html`
  - V případě HTTP spojení, pouze specifická URL adresa je vyjmuta ze skenování.
  - Pro připojení HTTPS přidáním určité adresy URL se vylučuje celá doména a její subdomény. Proto v tomto případě můžete přímo zadat doménu, která má být vyloučena ze skenování.
– Použijte zástupné znaky pro definování vzorů webových adres (pouze pro připojení HTTP).

  Důležité
  Výjimky s zástupnými znaky nefungují pro připojení HTTPS.

  Můžete použít následující zástupné:
  - Hvězdička (*) zastupuje nula nebo více znaků.
  - Otazník (?) zastupuje přesně jeden znak. Můžete použít několik otazníků pro určení jakékoli kombinace konkrétního počtu znaků. Například, `???` nahrazuje jakoukoli kombinaci přesně tří znaků.

  V následující tabulce můžete nalézt několik příkladových syntaxí pro specifikaci webových adres (URL).

Syntax	Aplikovatelnost výjimek
`www.example*`	Každá URL začínající `www.example` (nehledě na koncovku domény). Výjimka nebude platit pro subdomény specifikované webové stránky, jako je `subdomain.example.com`.
`*example.com`	Jakákoli URL končící na `example.com`, včetně jejich subdomén.
`*example.com*`	Jakákoli URL, která obsahuje zadaný řetězec.
`*.com`	Jakákoli webová stránka, která má doménovou koncovku `.com`, včetně subdomén. Použijte tuto

Syntax	Aplikovatelnost výjimek
	syntaxi pro vynechání všech domén na nejvyšší úrovni ze skenování.
`www.example?.com`	Jakákoli webová adresa začínající na `www.example?.com`, kde `?` může být nahrazeno libovolným samostatným znakem. Takové webové stránky mohou být: `www.example1.com` nebo `www.exampleA.com`.

Poznámka
Můžete používat URL relativní k protokolu.

- **Aplikace**. Vyjme ze skenování určený proces nebo aplikaci. Pro určení aplikace vyjmutou ze skenování:
  - Zadejte plnou cestu k aplikaci. Například, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Použijte proměnné prostředí pro určení cesty k aplikaci. Například `%programfiles%\Internet Explorer\iexplore.exe`
  - Použijte zástupné znaky pro určení libovolných aplikací odpovídajících určitému vzoru jmen. Například:
    - `c*.exe` odpovídá všem aplikacím začínajícím na "c" (chrome.exe).
    - `??????.exe` odpovídá všem aplikacím s názvem, který obsahuje šest znaků (chrome.exe, safari.exe, atd.).
    - `[^c]*.exe` odpovídá všem aplikacím kromě těch, které začínají na "c".
    - `[^ci]*.exe` odpovídá všem aplikacím kromě těch, které začínají na "c" nebo "i".

3. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.

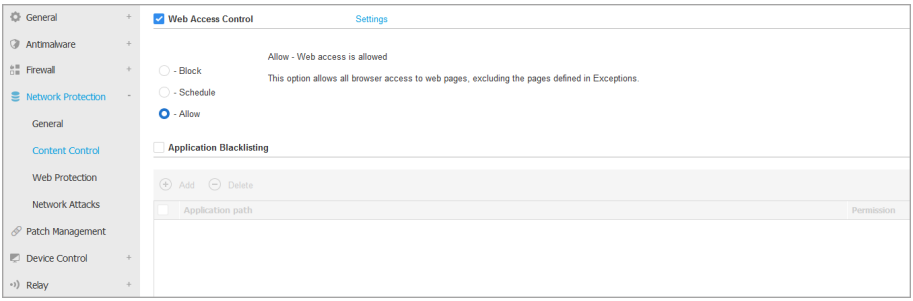
Pro odstranění položky ze seznamu klikněte na odpovídající tlačítko ⊗ **Odstranit**.

Kontrola obsahu

Nastavení Content Control jsou uspořádána do následujících sekcí:

- Kontrola přístupu k webu

- Blacklisting aplikací
- Ochrana dat



Kontrola přístupu k webu

Kontrola přístupu k webu vám umožňuje povolit nebo blokovat přístup k webu uživatelům nebo aplikacím v určitém časovém rozmezí.

Webové stránky blokované Kontrolou přístupu k webu se v prohlížeči nezobrazují. Místo nich se zobrazí výchozí webová stránka, která informuje uživatele, že požadovaná stránka byla zablokována Kontrolou přístupu k webu.

Použijte přepínač pro zapnutí nebo vypnutí **Kontroly přístupu k webu**.

Máte tři možnosti konfigurace:

- Vyberte **povolit** pro povolení přístupu k webu pokaždé.
- Vyberte **Blokovat** pro zakázání přístupu k webu pokaždé.
- Vyberte **Plánovač** pro povolení časových omezení při přístupu k webu podle podrobného časového rozvrhu.

Můžete si vybrat buď povolení nebo blokování přístupu k webu, můžete určit výjimky pro tyto akce, platící pro celé webové kategorie, nebo pouze pro určité webové adresy. Klikněte na **Nastavení** pro konfiguraci vašeho plánu přístupu k webu a výjimek následovně:

Plánovač

Pro omezení přístupu k internetu v určitých denních dobách nebo každý týden:

1. Z mřížky vyberte časové intervaly, během kterých má být přístup blokován.

Můžete kliknout na jednotlivé buňky nebo můžete kliknout a táhnout pro větší rozmezí. Pro navrácení výběru klikněte znovu do buňky.

Nový výběr začnete kliknutím na **Povolit vše** nebo **Blokovat vše** podle toho, který typ omezení chcete zavést.

2. Klikněte na tlačítko **Save**.

Poznámka
Bezpečnostní agent Bitdefender provádí aktualizace každou hodinu nehledě na to, jestli je přístup k internetu blokován.

Kategorie

Filtr webových kategorií dynamicky filtruje přístup k webovým stránkám na základě jejich obsahu. Filtr webových kategorií můžete použít pro určení výjimek ve zvolených akcích Kontroly přístupu k webu (Povolit nebo Blokovat) pro celé webové kategorie (jako jsou Hry, Mature Content nebo Online sítě).

Pro nastavení Filtru webových kategorií:

1. Zapněte **Filtr webových kategorií**.
2. Pro rychlou konfiguraci klikněte na úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (**Agresivní**, **Normální** nebo **Tolerantní**). Nastavte svůj výběr pomocí popisu na pravé straně stupnice. Přednastavené akce pro dostupné webové kategorie můžete prohlížet rozbalením sekce **Síťová pravidla** níže.
3. Pokud nejste spokojeni s výchozím nastavením, můžete nastavit vlastní filtr:
   a. Zvolte **Vlastní**.
   b. Klikněte na **Síťová pravidla** pro rozbalení příslušné sekce.
   c. Najděte kategorii, kterou chcete na seznamu, a z nabídky zvolte požadovanou akci. Pro více informací o dostupných kategoriích stránek, si přečtěte tento článek v znalostní databázi (KB article).
4. Pokud chcete ignorovat existující nastavení Přístupu k webu a aplikovat pouze Filtr kategorií webových stránek, zvolte možnost **Zacházet s Kategoriemi webových stránek jako s výjimkami pro Přístup k webu**.
5. Výchozí zpráva, která se zobrazí při přístupu k omezeným webovým stránkám, obsahuje také kategorii, se kterou se shoduje obsah stránky.

Odznačte volbu **Zobrazit detailní upozornění na klientovi (Show detailed alerts on client)** pokud chcete skrýt tuto informaci před uživatelem.

Poznámka
Tato volba není dostupná pro macOS.

6. Klikněte na tlačítko **Save**.

Poznámka

- Ohled je brán také na povolení **Povolit** pro konkrétní kategorie webových stránek během časových úseků, kdy je přístup k webu blokován Kontrolou přístupu k webu.
- Povolení **Povolit** fungují pouze, když je přístup k webu blokován Kontrolou přístupu k webu, zatímco povolení **Blokovat** fungují pouze, když Kontrola přístupu k webu přístup umožňuje.
- Můžete přepsat povolení kategorie pro jednotlivé webové stránky tak, že je přidáte s opačným povolením do **Kontrola přístupu k webu > Nastavení > Výjimky**. Například, pokud je webová adresa blokovaná Filtrem kategorií webových stránek, přidejte pro danou adresu síťové pravidlo s povolením nastaveným jako **Povolit**.

Výjimky

Můžete také definovat síťová pravidla pro výslovné blokování nebo povolení určitých webových adres, a přepsat tak existující nastavení Kontroly přístupu k webu. Například, uživatelé budou mít přístup k určité webové stránce i v případě, že je prohlížení internetu blokováno Kontrolou přístupu k webu.

Pro vytvoření síťového pravidla:

1. Povolte možnost **Použít výjimky**.
2. Zadejte požadovanou adresu, kterou chcete povolit nebo blokovat, do pole **Webová adresa**.
3. Z nabídky **Povolení** zvolte **Povolit** nebo **Blokovat**.
4. Klikněte na tlačítko ⊕ **Přidat** na pravé straně tabulky pro přidání adresy na seznam výjimek.
5. Klikněte na tlačítko **Save**.

Pro úpravu síťového pravidla:

1. Klikněte na webovou adresu, kterou chcete upravit.
2. Upravte stávající URL.
3. Klikněte na tlačítko **Save**.

Pro odstranění síťového pravidla klikněte na odpovídající tlačítko ⊗ **Odstranit**.

Blacklisting aplikací

V této sekci můžete konfigurovat Blacklisting aplikací, který vám umožňuje kompletně blokovat, nebo omezit přístup uživatelů k aplikacím na jejich počítačích. Tímto způsobem lze blokovat také hry, mediální software a aplikace pro zasílání zpráv a rovněž další kategorie softwaru a malwaru.

Pro nastavení Blacklistingu aplikací:

1. Povolte možnost **Blacklisting aplikací**.
2. Určete aplikace, ke kterým chcete omezit přístup. Pro omezení přístupu k aplikaci:
   a. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.
   b. Musíte určit cestu k spustitelnému souboru aplikace na cílových počítačích. Toto jde udělat dvěma způsoby:
      - Z nabídky zvolte přednastavené umístění a doplňte cestu dle potřeby do pole úprav. Například, pro aplikaci nainstalovanou ve složce `Program Files`, zvolte `%Program Files%` a doplňte cestu přidáním lomítka (\) a jména složky s aplikací.
      - Do pole úprav zadejte kompletní cestu. Pro jistotu, že je cesta platná na všech cílových počítačích, doporučujeme používat systémové proměnné (tam, kde je to vhodné).
   c. **Plánovač přístupu**. Naplánujte přístup k aplikacím v určitých denních hodinách, nebo týdně:
      - Z mřížky vyberte časové intervaly, během kterých má být přístup k aplikaci blokován. Můžete kliknout na jednotlivé buňky nebo můžete kliknout a táhnout pro větší rozmezí. Pro navrácení výběru klikněte znovu do buňky.
      - Nový výběr začnete kliknutím na **Povolit vše** nebo **Blokovat vše** podle toho, který typ omezení chcete zavést.
      - Klikněte na tlačítko **Save**. Nové pravidlo bude přidáno do seznamu.

Pro odstranění pravidla ze seznamu ho vyberte a klikněte na tlačítko ⊗ **Odstranit** v horní části tabulky. Pro úpravu existujícího pravidla na něj klikněte, a zobrazí se okno úprav.

Ochrana dat

Ochrana údajů zabraňuje neoprávněnému zveřejnění citlivých údajů v souladu s pravidly určenými správcem.

Poznámka
Tato volba není dostupná pro macOS.

Můžete vytvořit pravidla pro ochranu libovolných osobních nebo důvěrných informací, jako jsou:

- Osobní informace zákazníka
- Jména a klíčové detaily o vyvíjených produktech a technologiích
- Kontaktní informace vedení společnosti

Chráněné informace mohou zahrnovat jména, telefonní čísla, kreditní karty a informace o bankovních účtech, emailové adresy a tak dále.

Na základě vámi vytvořených bezpečnostních pravidel, Bitdefender Endpoint Security Tools skenuje síť a příchozí a odchozí emailový přenos pro určité řetězce znaků (například čísla kreditních karet). Pokud dojde ke shodě, daná webová stránka nebo emailová zpráva je zablokována, aby bylo zabráněno odeslání chráněných dat. Uživatel je okamžitě informován o opatřeních, která Bitdefender Endpoint Security Tools provedl, prostřednictvím varovné webové stránky nebo emailu.

Pro nastavení Ochrany dat:

1. Použijte zaškrtávací pole pro zapnutí Ochrany dat.
2. Vytvořte pravidla ochrany dat pro všechna citlivá data, která chcete chránit. Pro vytvoření pravidla:
   a. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.
   b. Zadejte jméno, pod kterým bude pravidlo přidáno do seznamu uvedeného v tabulce pravidel. Zadejte výmluvné jméno, abyste vy nebo jiný administrátor dokázali snadno rozpoznat, čeho se dané pravidlo týká.
   c. Zvolte typ dat, která chcete chránit.
   d. Zadejte data, která chcete chránit (například telefonní číslo vedoucího podniku nebo interní název produktu, na kterém firma pracuje). Povolena je jakákoli kombinace slov, číslic nebo řetězců skládajících se z alfanumerických a speciálních znaků (jako je @, # nebo $).

Ujistěte se, že zadáte alespoň pět znaků, abyste se vyhnuli mylnému zablokování emailových zpráv a webových stránek.

Důležité

Poskytnutá data jsou uložena v šifrované formě na chráněných koncových bodech, ale můžete je prohlížet ve vašem účtu v Control Center. Pro ještě vyšší bezpečnost nezadávejte všechna data, která chcete chránit. V tomto případě musíte zrušit možnost **Párovat celá slova**.

e. Nastavte možnosti skenování provozu dle potřeby.

- **Skenování webu (HTTP provoz)** - skenuje HTTP (webový) provoz a blokuje odchozí data odpovídající pravidlům.
- **Skenování emailu (SMTP provoz)** - skenuje SMTP (e-mailový) provoz a blokuje odchozí emailové zprávy obsahující data uvedená v pravidlech.

Uplatnění pravidla můžete zvolit pouze tehdy, když jeho data pravidla odpovídají celým slovům, nebo když data pravidla odpovídají zjištěnému řetězci.

f. Klikněte na tlačítko **Save**. Nové pravidlo bude přidáno do seznamu.

3. Nastavte výjimky pro pravidla ochrany dat, aby uživatelé mohli nadále odesílat chráněná data autorizovaným webovým stránkám a adresátům. Výjimky mohou být aplikovány globálně (pro všechna pravidla), nebo pouze na určitá pravidla. Pro přidání výjimky:
   a. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.
   b. Zadejte webovou stránku nebo emailovou adresu, pro kterou jsou uživatelé oprávněni odhalit chráněná data.
   c. Zvolte typ výjimky (webová stránka nebo emailová adresa).
   d. Za tabulky **Pravidla** vyberte pravidlo(a) ochrany dat, na které se má výjimka vztahovat.
   e. Klikněte na tlačítko **Save**. Nové pravidlo výjimky bude přidáno do seznamu.

Poznámka

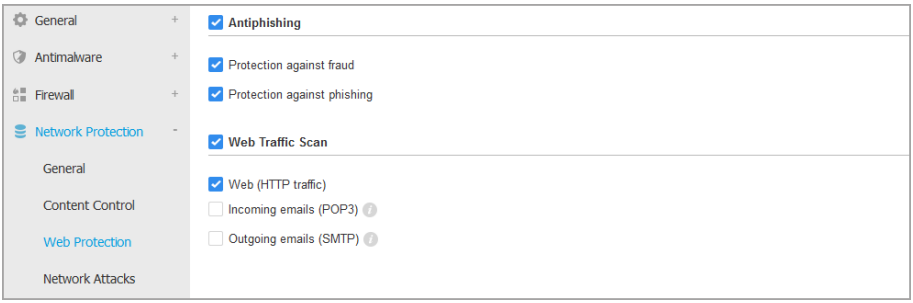
Pokud je email obsahující blokovaná data adresovaný několika příjemcům, obdrží ho ti, pro které byly definovány výjimky.

Pro odstranění pravidla nebo výjimky ze seznamu, klikněte na odpovídající tlačítko ⊗ **Odstranit** na pravé straně tabulky.

Ochrana webu

Na této stránce jsou nastavení uspořádána do následujících sekcí:

- Antiphishing
- Skenování webového provozu



Zásady pro počítače a virtuální stroje - Ochrana sítě - Ochrana webu

Antiphishing

Antiphishingová ochrana automaticky blokuje známé phishingové webové stránky, aby zabránil uživatelům v nechtěném odhalení svých osobních nebo důvěrných informací online podvodníkům. Místo phishingové webové stránky se v prohlížeči zobrazí zvláštní varovná stránka informující uživatele, že požadovaná webová stránka je nebezpečná.

Pro aktivaci antiphishingové ochrany vyberte **Antiphishing**. Antiphishing můžete dále vyladit nastavením následujících parametrů:

- **Ochrana proti podvodům**. Zvolte tuto možnost, pokud chcete rozšířit ochranu i na další typy podvodů kromě phishingu. Například webové stránky zastupující falešné firmy, které přímo nevyžadují osobní informace, ale místo toho se snaží vypadat jako oprávnění podnikatelé a vydělat peníze navedením lidí k tomu, aby s nimi obchodovali.
- **Ochrana proti phishingu**. Nechte tuto možnost povolenou pro ochranu uživatelů před pokusy o phishing.

Pokud je legitimní stránka chybně zjištěna jako phishingová a je zablokována, můžete ji přidat na whitelist a povolit uživatelům přístup. Seznam by měl obsahovat pouze webové stránky, kterým plně důvěřujete.

Pro správu antiphishingových výjimek:

1. Přejděte na **Obecná** nastavení a klikněte na **Globální výjimky** .
2. Zadejte webovou adresu a klikněte na tlačítko ⊕ **Přidat**.

   Pokud chcete vyloučit celou internetovou stránku, zadejte jméno domény, jako je `http://www.website.com`, a pokud chcete vynechat pouze webovou stránku, zadejte konkrétní webovou adresu dané stránky.

   Poznámka
   Při vytváření adres URL nejsou povoleny zvláštní znaky.

3. Pro odstranění výjimky ze seznamu klikněte na odpovídající tlačítko ⊗ **Odstranit**.
4. Klikněte na tlačítko **Save**.

Skenování webového provozu

Příchozí emaily (POP3) a webový provoz jsou skenovány v reálném čase, aby bylo zabráněno stažení malwaru na koncový bod. Odchozí emaily (SMTP) jsou skenovány pro zabránění malwaru v nakažení jiných koncových bodů. Skenování webového provozu může mírně zpomalit procházení webu, ale blokuje malware pocházející z Internetu, včetně stahovaných položek.

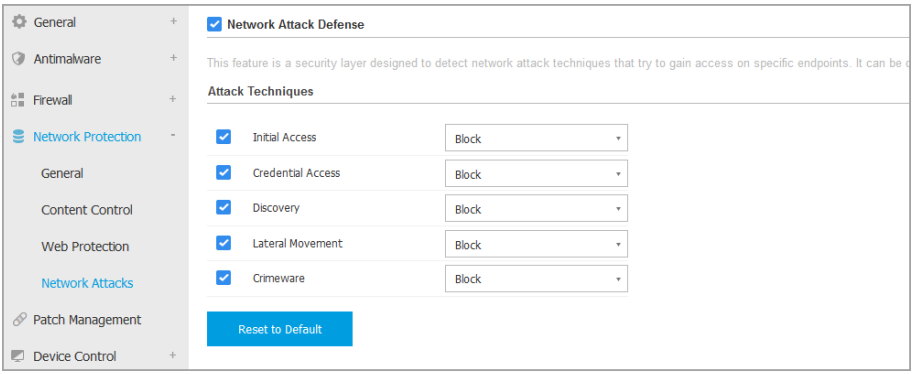
Když je nalezen nakažený email, je automaticky nahrazen standardním emailem, který informuje adresáta původního nakaženého emailu. Když webová stránka obsahuje nebo rozšiřuje malware, je automaticky blokována. Místo ní se zobrazí zvláštní stránka s varováním pro uživatele, že požadovaná webová stránka je nebezpečná.

Přestože to nedoporučujeme, můžete vypnout skenování emailů a síťového provozu pro zvýšení výkonu systému. Toto nepředstavuje zásadní hrozbu, pokud zůstane povoleno skenování místních souborů při přístupu.

Poznámka
Volby **Incoming emails** a **Outgoing emails** nejsou dostupné pro macOS.

Síťové útoky

Network Attack Defense poskytuje bezpečnostní vrstvu založenou na technologii Bitdefender, která detekuje a podniká kroky proti síťovým útokům zločinci , jejichž cílem je získat přístup na koncových bodech pomocí specifických technik, jako jsou: útoky brutální silou, zneužití sítě a hesel.



Zásady pro počítače a virtuální stroje - Ochrana sítě - Síťové útoky

Konfigurace Network Attack Defense:

1. Zaškrtnutím políčka **Network Attack Defense** modul aktivujete.
2. Zaškrtnutím příslušných políček aktivujete ochranu proti každé kategorii síťových útoků. Techniky síťového útoku jsou seskupeny podle znalostí MITRE's ATT&CK založených takto:
   - **Initial Access** - útočník získá přístup do sítě různými způsoby, včetně zranitelných webových serverů orientovaných na veřejnost. Například: zneužití informací, využití napíchnutého SQL , stažením napíchnutých vektorů
   - **Credential Access** - útočník ukradne přihlašovací údaje, jako jsou uživatelská jména a hesla, aby získal přístup do systémů. Například: útoky hrubou silou, zneužití neoprávněnou autentizací, krádeže hesel.
   - **Discovery** - útočník se po infiltrování pokusí získat informace o systémech a vnitřní síti, než se rozhodne, co dál. Například: procházením adresářů, zneužitím webového rozharní HTTP.
   - **Lateral Movement** - útočník prozkoumává síť, často tím že se pohybuje skrz více různých systémů, aby našel hlavní cíl Útočník může k dosažení cíle použít specifické nástroje. Na příklad: využití napíchnutých příkazů, využití Shellshock, využití dvojitého rozšíření.
   - **Crimeware** - tato kategorie zahrnuje techniky určené k automatizaci počítačové kriminality. Například, Crimeware techniky jsou: jaderné exploity, různý malware software, jako jsou trojské koně a roboty.

3. Vyberte akci, které chcete provést proti různým kategoriim technik síťového útoku, z následujících možností:
   a. **Block** - Network Attack Defense zastaví pokus o útok, jakmile bude detekován.
   b. **Report Only** - Network Attack Defense vás informuje o zjištěném pokusu o útok, ale nepokusí se jej zastavit.

Počáteční nastavení můžete snadno obnovit kliknutím na tlačítko **Reset to Default** na spodní straně stránky.

Podrobnosti o pokusech o síťové útoky jsou k dispozici ve zprávě Network Incident a v oznámení Network Incident.

7.2.7. Patch Management

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery

Modul Správa oprav vás zbaví zátěže při udržování koncových bodů aktuálních s nejnovějšími softwarovými balíčky díky tomu, že automaticky distribuuje a instaluje balíčky pro širokou škálu produktů.

Poznámka
Seznam podporovaných prodejců a produktů si můžete prohlédnout v tomto KB článku.

Tato sekce pravidel obsahuje nastavení pro automatické zavedení balíčků. Nejprve nastavíte, jak jsou balíčky stahovány na koncové body, a poté, které z nich instalovat a kdy.

Konfigurace Nastavení stahování balíčků

Proces šíření balíčků používá Servery pro načítání oprav do mezipaměti pro optimalizování síťového provozu. Koncové body se připojují k těmto serverům a stahují balíčky prostřednictvím místní sítě. Pro vysokou dostupnost balíčků doporučujeme používat více než jeden server.

Pro přiřazení Serverů pro načítání oprav do mezipaměti k cílovým koncovým bodům:

1. V sekci **Nastavení stahování balíčků** klikněte na pole v horní části tabulky. Zobrazí se seznam zjištěných Serverů pro načítání oprav do mezipaměti.

   Pokud je seznam prázdný, musíte nainstalovat funkci Serveru pro nahrávání oprav do mezipaměti na relaye ve vaší síti. Více informací naleznete v Instalační příručce.

2. Ze seznamu vyberte požadovaný server.
3. Klikněte na tlačítko ⊕ **Přidat**.
4. Pokud je potřeba, opakujte předchozí kroky pro přidání dalších serverů.
5. Použijte směrové šipky nahoru a dolů na pravé straně tabulky pro určení priority serverů. Priorita se snižuje směrem od vrchu ke spodu seznamu.

   Koncový bod žádá o balíček z přiřazených serverů v pořadí podle priority. Koncový bod stáhne balíček ze serveru, na kterém ho nalezne jako první. Server, na kterém požadovaný balíček chybí, ho automaticky stáhne od prodejce, aby byl k dispozici pro budoucí žádosti.

Pro odstranění již nepotřebných serverů ze seznamu, klikněte na odpovídající tlačítko ⊖ Odstranit na pravé straně tabulky.

Zvolte možnost **Použít internetové stránky prodejců jako záložní umístění pro stahování balíčků**, abyste se ujistili, že vaše koncové body obdrží softwarové opravy v případě, že jsou servery pro načítání oprav do mezipaměti nedostupné.

Nastavení Skenování balíčků a Instalace

GravityZone provádí zavedení balíčků ve dvou nezávislých fázích:

1. Hodnocení. Pokud je vyslán příkaz z konzole správy, tak koncové body jsou proskenovány za účelem odhalení chybějících balíčků a hlásí se jejich výskyt zpět.
2. Instalace. Konzole odesílá agentům seznam balíčků, které chcete nainstalovat. Koncový bod stahuje balíčky ze serveru pro načítání oprav do mezipaměti a poté je instaluje.

Pravidla poskytují nastavení pro automatizaci těchto procesů, částečnou nebo úplnou, takže jsou spouštěny pravidelně na základě zvoleného plánu.

Pro nastavení automatického skenování balíčků:

1. Označte pole **Automatické skenování balíčků**.

2. Použijte možnosti plánování pro nastavení opakování skenování. Můžete nastavit skenování, aby probíhalo denně, nebo v určité dny v týdnu v daný čas.
3. Vyberte **Inteligentní sken, když je nainstalována nová aplikace/program** , aby se zjistilo, kdykoli byla na koncový bod nainstalována nová aplikace a jaké záplaty jsou pro ni dostupné.

Pro nastavení automatické instalace balíčků:

1. Označte pole **Instalovat balíčky automaticky po skenování**.
2. Zvolte, jaké typy balíčků chcete instalovat: bezpečnostní, jiné, nebo oba.
3. Použijte možnosti plánování pro nastavení, kdy mají instalační úlohy probíhat. Můžete nastavit skenování, aby se spustilo okamžitě po dokončení skenování balíčků, denně, nebo v určité dny v týdnu v daný čas. Doporučujeme nainstalovat bezpečnostní záplaty ihned jakmile jsou odhaleny.
4. Ve výchozím nastavení jsou všechny produkty oprávněny k instalaci balíčků. Pokud chcete automaticky aktualizovat pouze některé produkty, které považujete za nezbytné pro vaše podnikání, postupujte podle následujících kroků:
   a. Označte pole **Konkrétní prodejce a produkt**.
   b. Klikněte na pole **Prodejce** v horní části tabulky. Zobrazí se seznam se všemi podporovanými prodejci.
   c. Projděte seznam a zvolte prodejce pro produkty, na které chcete aplikovat balíčky.
   d. Klikněte na pole **Produkty** v horní části tabulky. Zobrazí se seznam se všemi produkty zvoleného prodejce.
   e. Zvolte všechny produkty, pro které chcete instalovat balíčky.
   f. Klikněte na tlačítko ⊕ **Přidat**.
   g. Opakujte předchozí kroky pro zbývající prodejce a produkty.

      Pokud jste zapomněli přidat produkt, nebo chcete nějaký produkt odstranit, najděte v tabulce prodejce, poklepejte na pole **Produkty** a vyberte nebo zrušte výběr produktu ze seznamu.

   Pro odstranění prodejce se všemi jeho produkty, najděte ho v tabulce a klikněte na odpovídající tlačítko ⊖ **Odstranit** na pravé straně tabulky.

5. V době, kdy má proběhnout instalace balíčků, může být koncový bod z různých důvodů offline. Zvolte možnost **Pokud zmeškáno, spustit co nejdříve** pro instalaci balíčků okamžitě, jakmile je koncový bod znovu online.
6. Některé balíčky mohou vyžadovat restart systému pro dokončení instalace. Pokud toto chcete provést manuálně, zvolte možnost **Odložit restartování**.

Důležité
Aby zhodnocení a instalace na koncových bodech s Windows proběhlo úspěšně, musíte zajistit naplnění následujících podmínek:

- **Důvěryhodné autority pro certifikaci rootů** ukládá certifikát **DigiCert Assured ID Root CA**.
- **Zprostředkující certifikační autority** zahrnují **DigiCert SHA2 Assured ID Code Signing CA**.
- Koncové body nainstalovaly opravy pro systémy Windows 7 a Windows Server 2008 R2 uvedené v tomto článku společnosti Microsoft: Microsoft Security Advisory 3033929

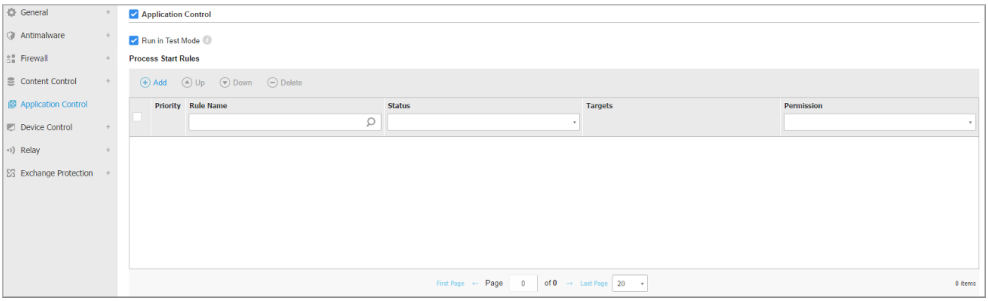
7.2.8. Kontrola aplikací

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery

Modul Kontrola aplikací přidá další vrstvu ochrany před všemi druhy malwarových hrozeb z aplikací třetích stran(ransomware, zero-day útoky, exploity, trojské koně, spyware, rootkity, adware a tak dále) tím, že blokuje spouštění neoprávněných aplikací a procesů. Kontrola aplikací snižuje dopadovou plochu útoku, které malwarové hrozby dokáží využívat na koncovém zařízení, a brání instalaci a spuštění všech nežádoucích, nedůvěryhodných nebo škodlivých aplikací.

Kontrola aplikací zavádí pružná pravidla, která vám umožňují whitelisting aplikací a správu oprávnění k aktualizaci.



Kontrola aplikací

Důležité

- Pro povolení **Kontroly aplikací** na vašich současně nainstalovaných klientech, spusťte úlohu **Přenastavit klienta**. Po nainstalování modulu můžete prohlížet jeho stav v okně **Informace**.
- Po aktualizaci aplikací Kontrola aplikací silně ovlivňuje režim Pokročilého uživatele. Například, když je aktualizována aplikace z whitelistu, koncové zařízení podá nové informace. GravityZone aktualizuje pravidlo s novými hodnotami a odešle ho zpět.

Musíte spustit úlohu **Vyhledání aplikací** pro zobrazení spuštěných aplikací a procesů ve vaší síti. Další informace viz „Vyhledání aplikací“ (str. 99). Poté můžete určit pravidla pro Kontrolu aplikací.

Kontrola aplikací pracuje ve dvou režimech:

- **Testovací režim**. Kontrola aplikací pouze detekuje a hlásí aplikace v Control Center, a nechává je pracovat jako obvykle. Můžete nastavit a testovat pravidla a zásady pro whitelisting, ale aplikace nebudou blokovány.
- **Produkční režim**. Kontrola aplikací blokuje všechny neznámé aplikace. Procesy operačního systému Microsoft a procesy Bitdefender jsou ve výchozím stavu na whitelistu. Vybraným aplikacím z whitelistu bude povolen provoz. Pro aktualizaci aplikací z whitelistu musíte definovat zdroj aktualizací. Toto jsou zvláštní procesy, které mohou měnit existující aplikace. Další informace viz „Inventář aplikací“ (str. 186).

Varování

- Abyste měli jistotu, že Kontrola aplikací neomezuje legitimní aplikace, musíte Kontrolu aplikací spustit nejprve v testovacím režimu. Díky tomu si můžete být jisti, že jsou pravidla a zásady pro whitelisting řádně definována.
- Procesy, které jsou ve chvíli nastavení Kontroly aplikací do **Produkčního režimu** již spuštěny, budou zablokovány po příštím restartování procesu.

Pro správu povolení aplikací ke spuštění:

1. Pro povolení tohoto modulu označte zaškrtávací políčko **Kontrola aplikací**.
2. Použijte zaškrtávací pole **Spustit v Testovacím režimu** pro zapnutí nebo vypnutí Testovacího režimu.

   Poznámka

   - V testovacím režimu jste upozorněni, když by Kontrola aplikací zablokovala konkrétní aplikaci. Další informace viz „Typy oznámení“ (str. 534).
   - Upozornění na **Blokované aplikace** se zobrazí v Oznamovací oblasti, když budou zjištěny nové aplikace, a když budou zablokovány aplikace z blacklistu.

3. Určete pravidla zahájení procesu.

Pravidla zahájení procesu

Kontrola aplikací vám umožňuje ruční oprávnění konkrétních aplikací a procesů na základě hashe spustitelného souboru, podepsání certifikátu otisku palce a cesty k aplikaci. Můžete určit také výjimky z pravidla.

Poznámka

Pro získání vlastních hodnot pro hash spustitelného souboru a otisku palce certifikátu použijte„Nástroje Kontroly aplikací“ (str. 569)

Tabulka **Pravidla zahájení procesu** vám poskytuje informace o existujících pravidlech a dodává důležité informace:

- Priorita pravidla. Pravidlo s vyšší prioritou je blíže k vrcholu seznamu.
- Název a stav pravidla.

- Cílové aplikace a jejich povolení ke spuštění. Cíl představuje počet podmínek, které musí být naplněny, aby pravidlo mohlo být uplatněno, nebo počet aplikací či skupin, pro které pravidlo platí.

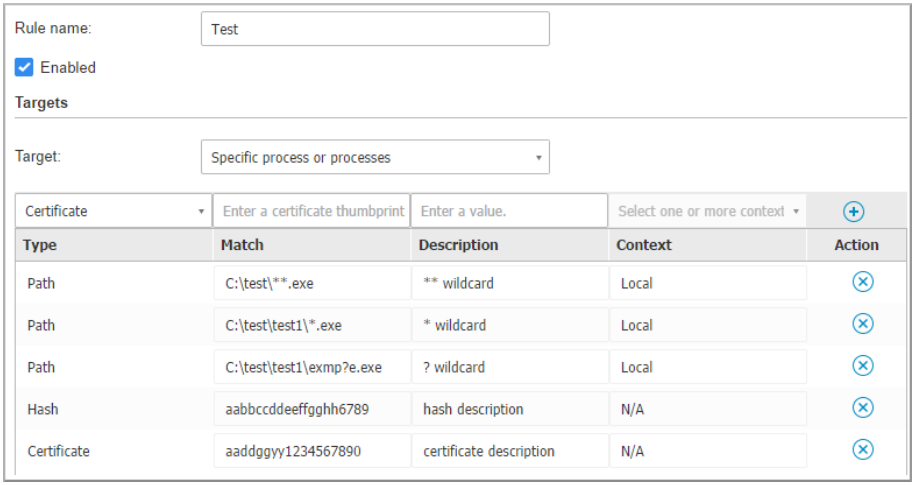
Pro vytvoření pravidla zahájení procesu:

1. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky pro otevření konfiguračního okna.
2. V sekci **Obecné** zadejte **Název pravidla**.
3. Označte zaškrtávací políčko **Povoleno** pro aktivaci pravidla.
4. V sekci **Cíle** určete cílové umístění pravidla:
   - **Konkrétní proces nebo procesy**, pro určení procesu, kterému je povoleno nebo zakázáno spuštění. Můžete autorizovat pomocí cesty, hashe nebo certifikátu. Podmínky uvnitř pravidel jsou spojovány pomocí logických AND.
     - Pro autorizování aplikace z určité cesty:
       a. Vyberte **Path** ve sloupci **Type**. Specifikujte cestu k objektu. Můžete poskytnout absolutní nebo relativní cestu a používat speciální znaky. Symbol hvězdičky (*) spojí všechny soubory v rámci adresáře. Dvě hvězdičky (**) spojí všechny soubory a adresáře v definovaném adresáři. Otazník (?) zastupuje přesně jeden znak. Můžete také přidat vysvětlení pro zjednodušení identifikování procesu.
       b. Z rozbalovací nabídky **Vybrat jeden nebo více kontextů** můžete vybrat mezi lokálním, CD-ROM, odpojitelné nebo síť. Můžete zablokovat spuštění aplikace z odnímatelných zařízení nebo je povolit pokud je aplikace lokálně spuštěna.
     - Pro autorizování aplikace na základě hashe, vyberte **Hash** ve sloupci **Type** a zadejte hashovou hodnotu. Můžete také přidat vysvětlení pro zjednodušení identifikování procesu.

       Důležité
       Pro vygenerování hashové hodnoty, stáhněte nástroj Fingerprint. Další informace viz „Nástroje Kontroly aplikací“ (str. 569)

     - Pro autorizování na základě certifikátu, vyberte **Certificate** ze sloupce **Type** a zadejte thumbprint certifikátu. Můžete také přidat vysvětlení pro zjednodušení identifikování procesu.

Důležité
Pro získání thumbprint certifikátu, stáhněte nástroj Thumbprint. Další informace viz „Nástroje Kontroly aplikací“ (str. 569)



Pravidla aplikací

Klikněte na ⊕ **Add** pro přidání pravidla.

- **Inventory applications or groups**, pro přidání skupiny nebo nějaké aplikace objevené v síti. Můžete zobrazit aplikace běžící ve vaší síti v záložce **Network > Application Invertory**. Další informace viz „Inventář aplikací“ (str. 186).

  Vloze aplikace nebo názvy skupin do pole, odděleně pomocí čárky. Funkce automatické vyplnění zobrazuje návrhy podle toho jak píšete.

5. Vyberte zaškrtávací pole **Include subprocesses** pro aplikování pravidla pro spuštěné podprocesy.

   Varování
   Při nastavování pravidel pro aplikace prohlížečů, doporučujeme tuto možnost vypnout, pro předejití bezpečnostních rizik.

6. Optimálně, můžete také definovat výjimky z pravidla procesu start. Operace přidání je podobná jako jedné, která byla vysvětlena již předtím.

7. V sekci **Permissions**, vyberte zda bude povolená nebo zamezená pro spuštění.
8. Kliknutím na tlačítko **Uložit** aplikujete změny.

Pro úpravu existujícího pravidla:

1. Klikněte na jméno pravidla pro otevření konfiguračního okna.
2. Zadejte nové hodnoty pro možnosti, které chcete změnit.
3. Kliknutím na tlačítko **Uložit** aplikujete změny.

Pro nastavení priority pravidel:

1. Označte pole požadovaného pravidla.
2. Použijte prioritní tlačítka na pravé straně tabulky:
   - Klikněte na tlačítko **Nahoru** pro povýšení zvoleného pravidla.
   - Kliknutím na tlačítko **Dolů** ji posunete dolů.

Můžete mazat jedno nebo více pravidel najednou. Vše, co musíte udělat, je:

1. Vyberte pravidla, která chcete smazat.
2. Klikněte na tlačítko **Smazat** v horní části tabulky. Jakmile je pravidlo smazáno, nelze ho obnovit.

7.2.9. Kontrola zařízení

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery
- macOS

Modul Kontrola zařízení umožňuje prevenci úniku citlivých dat a malwarových infekcí skrze externí zařízení připojená ke koncovým bodům pomocí aplikace pravidel pro blokování a výjimky prostřednictvím pravidel pro širokou škálu typů zařízení.

Důležité
V případě macOS se opírá modul správy přístupu zařízení (Device Control) o rozšířené jádro (kernel extension). Instalace rozšíření jádra (kernel extensions) vyžaduje vaše schválení na macOS High Sierra (10.13) a novější. Systém upozorní uživatele o tom,

že rozšíření systému od Bitdefender bylo zablokováno. uživatel může funkci povolit v předvolbách **Bezpečnost & Soukromí**. Dokud uživatel nepovolí rozšíření systému Bitdefender, tak nebudou moduly fungovat a uživatelské rozhraní (user interface)Endpoint Security for Mac bude ukazovat kritickou chybu a bude se dotazovat na schválení.
K eliminaci zásahu uživatele můžete předschválit rozšíření pro kernel Bitdefender pomocí Whitelistování s použitím nástroje správy mobilních zařízení. Pro detaily o rozšíření pro kernel Bitdefender, přejděte do článek KB.

Pro využití modulu Kontrola zařízení ho musíte nejprve zahrnout do bezpečnostního agenta nainstalovaném na cílových koncových bodech, a poté povolit možnost **Kontrola zařízení** v pravidlech zavedených na těchto koncových bodech. Poté, pokaždé, když je zařízení připojeno ke spravovanému koncovému bodu, bezpečnostní agent zašle informace o této události do Control Center, včetně jména zařízení, třídy, ID a data a času připojení.

V následující tabulce, naleznete které druhy zařízení jsou podporovány modulem pro správu zařízení (Device Control) na systémech Windows a macOS:

Typ zařízení	Windows	macOS
Bluetooth adaptéry	x	x
CD-ROM zařízení	x	x
Disketové jednotky	x	N/A
IEEE 1284.4	x	
IEEE 1394	x	
Záznamová zařízení	x	x
Modemy	x	Spravovaná pod síťovými adaptéry (kartami)
Páskové disky	x	N/A
Windows Portable	x	x
COM/LPT porty	x	LPT na sériové porty jsou podporovány
SCSI Raid	x	
Tiskárny	x	Podpora pouze pro lokálně připojené tiskárny

Typ zařízení	Windows	macOS
Síťový adaptér	x	x (včetně Wi-Fi donglů)
Adaptéry bezdrátového připojení	x	x
Vnitřní Úložiště	x	
Vnější Úložiště	x	x

Poznámka

- U macOS, pokud je **Vlastní (Custom)** vyjímka vybraná pro specifickou kategorii zařízení, tak bude pouze aplikována vyjímka konfigurovaná pro **Jiné (Other)** podkategorie.
- Na Windows a macOS, Správa Zařízení (Device Control) umožňuje přístup do celého Bluetooth adaptéru na sytémové úrovni, podle danné politiky. Neexistuje zde možnost granulárního nastavení vyjímek podle spárovaných zařízení.

Kontrola zařízení umožňuje správu oprávnění pro zařízení následovně:

- Definovat pravidla oprávnění
- Definovat výjimky oprávnění

Pravidla

Sekce **Pravidla** umožňuje definici oprávnění pro zařízení připojená k cílovým koncovým bodům.

Pro nastavení oprávnění pro požadovaný typ zařízení:

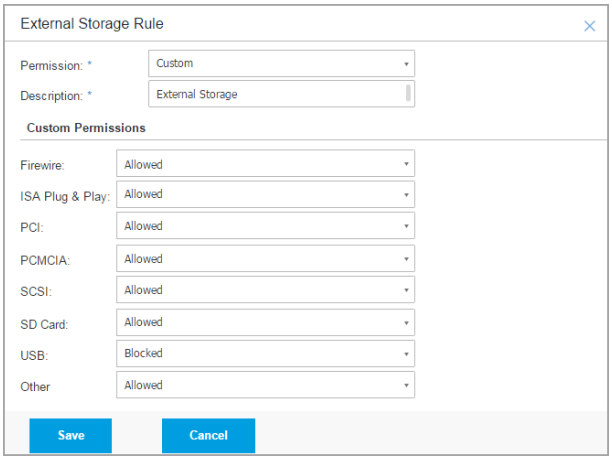
1. Přejděte na **Kontrola zařízení > Pravidla**.
2. V tabulce klikněte na název zařízení.
3. Z dostupných možností vyberte jeden typ oprávnění. Mějte prosím na paměti, že dostupná sada oprávnění se může lišit podle typu zařízení:
   - **Povolené**: zařízení může být používáno na cílovém koncovém bodě.
   - **Blokované**: zařízení nemůže být používáno na cílovém koncovém bodě. V tomto případě, při každém připojení zařízení ke koncovému bodu, bezpečnostní agent zobrazí upozornění, že zařízení bylo zablokováno.

Důležité

Dříve zablokovaná připojená zařízení nejsou automaticky odblokována změnou práv na **Povolit**. Uživatel musí restartovat systém nebo opětovně připojit zařízení aby byl schopen jej užívat.

- **Pouze pro čtení**: na zařízení lze používat pouze funkce pro čtení.
- **Vlastní**: určete různá povolení pro každý typ portu na tom samém zařízení, jako je Firewire, ISA Plug & Play, PCI, PCMCIA, USB, atd. V tomto případě se zobrazí seznam komponentů dostupných pro zvolené zařízení, a pro každý komponent můžete nastavit požadovaná povolení.

  Například, pro Externí úložiště můžete blokovat pouze USB, a povolit využití všech ostatních portů.



Politiky Počítačů a Virtuálních Strojů - Řízení Zařízení - Pravidla

Výjimky

Po nastavení pravidel oprávnění pro různé typy zařízení možná budete chtít z těchto pravidel určité typy zařízení nebo produktů vynechat.

Můžete určit výjimky zařízení:

- Určením jednotlivých zařízení, která chcete vynechat, pomocí ID zařízení (nebo ID hardwaru).
- Pomocí produktového ID (nebo PID) pro určení škály zařízení vydaných stejným výrobcem.

Pro určení pravidel výjimek pro zařízení:

1. Přejděte na **Kontrola zařízení > Pravidla**.

2. Povolte možnost **Výjimky**.
3. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky.
4. Zvolte způsob, který chcete použít pro přidávání výjimek:
   - **Manuálně**. V tomto případě je nutné zadat každé ID zařízení nebo produktové ID, které chcete vynechat, s předpokladem, že máte po ruce seznam s příslušnými ID:
     a. Zvolte typ výjimky (podle ID produktu nebo zařízení).
     b. Do pole **Výjimky** zadejte ID, která chcete vynechat.
     c. Do pole **Popis** zadejte jméno, které vám pomůže rozpoznat zařízení nebo řadu zařízení.
     d. Zvolte typ povolení pro určená zařízení (**Povolené** nebo **Blokované**).
     e. Klikněte na tlačítko **Save**.

     Poznámka
     Wildcard výjimky můžete konfigurovat ručně podle Device ID s použitím syntaxe `wildcards:deviceID`. Použijte question mark (?) k nahrazení jednoho znaku, a asterisk (*) k nahrazení jakéhokoliv čísla nebo znaku v `deviceID`. Příklad: pro `wildcards:PCI\VEN_8086*` platí že všechna zařízení obsahující řetězec `PCI\VEN_8086` ve svém ID budou vyloučena z pravidel politiky.

   - **Ze zjištěných zařízení**. V tomto případě můžete zvolit ID zařízení nebo ID produktů a vyloučit ho ze seznamu všech zjištěných zařízení ve vaší síti (týká se pouze spravovaných koncových bodů):
     a. Zvolte typ výjimky (podle ID produktu nebo zařízení).
     b. V tabulce **Výjimky** zvolte ID, která chcete vynechat:
        – Pro ID zařízení zvolte ze seznamu každé zařízení, které chcete vynechat.
        – Pro ID produktů tím, že vyberete jedno zařízení, vynecháte všechna zařízení s tím samým produktovým ID.
     c. Do pole **Popis** zadejte jméno, které vám pomůže rozpoznat zařízení nebo řadu zařízení.
     d. Zvolte typ povolení pro určená zařízení (**Povolené** nebo **Blokované**).
     e. Klikněte na tlačítko **Save**.

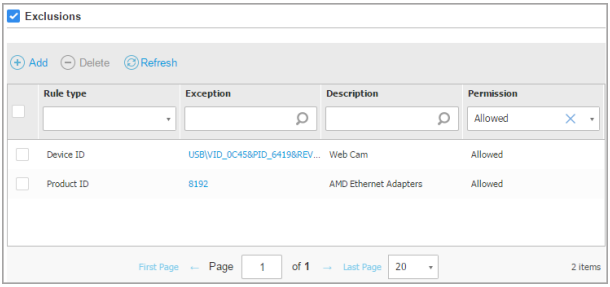
Důležité

- Zařízení, která byla ke koncovým bodům připojena již během instalace Bitdefender Endpoint Security Tools, budou rozpoznána až po restartování příslušných koncových bodů.
- Dříve zablokovaná připojená zařízení nejsou automaticky odblokována nastavením výjimky s právy **Povolit**. Uživatel musí restartovat systém nebo opětovně připojit zařízení aby byl schopen jej užívat.

Všechny výjimky zařízení se zobrazí v tabulce **Výjimky**.

Pro odstranění výjimky:

1. Vyberte ji v tabulce.
2. Klikněte na tlačítko ⊕ **Smazat** v horní části tabulky.



Politiky Počítačů a Virtuálních Strojů - Řízení Zařízení - Výjimky

7.2.10. Relay

Poznámka

Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery
- Linux

V této sekci můžete definovat nastavení komunikace a aktualizací pro cílové koncové body s přiřazenou funkcí relay.

Nastavení jsou uspořádána do následujících sekcí:

- Komunikace

- Aktualizace

Komunikace

Na kartě **Komunikace** naleznete volby proxy pro komunikaci mezi koncovými body s relay a komponenty GravityZone.

Je-li potřeba, můžete nezávisle nastavit komunikaci mezi cílovými koncovými body s relay a cloudovými službami Bitdefender / GravityZone, pomocí následujících nastavení:

- **Ponechat instalační nastavení** pro použití stejných nastavení proxy, která jsou definována v instalačním balíčku.
- **Použít proxy definovanou v sekci Obecné** pro použití nastavení proxy definovaného v současném pravidle pod sekcí **Obecné > Nastavení**.
- **Nepoužívat**, když cílové koncové body nekomunikují s určitými komponenty Bitdefender přes proxy.

Aktualizace

V této sekci můžete definovat nastavení aktualizací pro koncové body s funkcí relay:

- V sekci **Aktualizace** můžete konfigurovat následující parametry:
  - Časový úsek, během kterého koncové body s relay kontrolují dostupnost aktualizací.
  - Složka umístěná na koncovém bodě s relay, do které se stahují a zrcadlí aktualizace produktu a signatur. Pokud chcete určit konkrétní složku pro stažené soubory, zadejte její plnou cestu do odpovídajícího pole.

    Důležité
    Doporučujeme určit vlastní složku pro aktualizace produktu a signatur. Při výběru se vyhněte složkám obsahujícím systémové nebo osobní soubory.

- **Definovat vlastní umístění pro aktualizace**. Výchozí umístění aktualizací pro relay agenty je místní aktualizační server GravityZone. Další umístění aktualizací můžete určit zadáním IP nebo názvu místního hosta jednoho nebo více aktualizačních serverů ve vaší síti, a poté nastavit jejich prioritu pomocí směrových tlačítek, které se zobrazí při podržení ukazatele myši nad položkou.

Pokud je první umístění aktualizací nedostupné, bude použito to další, a tak dále.

Pro určení vlastního umístění pro aktualizace:

1. Povolte možnost **Určit vlastní umístění pro aktualizace**.
2. Zadejte adresu nového aktualizačního serveru do pole **Přidat umístění**. Použijte jednu z těchto syntaxí:
   - `update_server_ip:port`
   - `update_server_name:port`

   Výchozí port je 7074.
3. Pokud koncový bod s relay komunikuje s místním aktualizačním serverem skrze proxy server, zvolte **Použít proxy**. Bude brán ohled na nastavení proxy definované v **Obecné > Nastavení**.
4. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky.
5. Použijte šipky ⌃ Nahoru / ⌄ Dolů ve sloupci **Akce** pro nastavení priority definovaných aktualizačních umístění. V případě, že je první aktualizační umístění nedostupné, v potaz bude bráno to následující, a tak dále.

Klikněte na odpovídající tlačítko ⊗ **Odstranit** pro odstranění umístění ze seznamu. Přestože výchozí aktualizační umístění můžete odebrat, nedoporučujeme to.

7.2.11. Exchange Ochrana

Poznámka
Tento modul je k dispozici pro Windows pro servery.

Security for Exchange přináší vysoce nastavitelné parametry, čímž chrání Microsoft Exchange Servery proti hrozbám jako je malware, spam a phishing. S Exchange Protection nainstalovanou na vašem mailovém serveru můžete také filtrovat emaily obsahující přílohy nebo obsah považovaný za nebezpečný podle bezpečnostních zásad vaší firmy.

Pro udržení výkonu serveru na normálních úrovních, emailový přenos je zpracováván filtry Security for Exchange v následujícím pořadí:

1. Antispamové filtrování
2. filtrování Kontroly obsahu > Obsahu
3. filtrování Kontroly obsahu > Příloh

4. Antimalwarové filtrování

Nastavení Security for Exchange jsou uspořádána v následujících sekcích:

- Hlavní
- Antimalware
- Antispam
- Kontrola obsahu

Hlavní

V této sekci můžete vytvářet a spravovat skupiny emailových účtů, určit věk položek v karanténě a blokovat určité odesílatele.

Uživatelské skupiny

Control Center umožňuje tvorbu uživatelských skupin pro uplatnění různých zásad pro skenování a filtrování pro různé kategorie uživatelů. Například můžete vytvořit vhodná pravidla pro IT oddělení, pro obchodní tým, nebo nebo pro manažery vaší společnosti.

Skupiny uživatelů jsou dostupné globálně, i přes politiku nebo uživatele který je vytvořil.

Pro jednoduší správu skupin, Control Center automaticky importuje uživatelské skupiny ze Windows Active Directory.

Pro vytvoření uživatelské skupiny:

1. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se okno s podrobnostmi.
2. Zadejte jméno skupiny, popis a emailové adresy uživatelů.

> **Poznámka**
> - V případě dlouhého seznamu emailových adres je můžete zkopírovat a vložit z textového souboru.
> - Přijímaný způsob oddělení položek v seznamu: mezera, čárka, středník a enter.

3. Klikněte na tlačítko **Save**.

Vlastní skupiny je možné upravovat. Klikněte na jméno skupiny pro otevření konfiguračního okna, kde můžete změnit detaily skupiny nebo upravit seznam uživatelů.

Pro odstranění vlastní skupiny ze seznamu ji vyberte a klikněte na tlačítko ⊖ **Odstranit** v horní části tabulky.

Poznámka
Skupiny Active Directory nemůžete upravovat ani mazat.

Nastavení

- **Delete quarantined files older than (days).** Ve výchozím nastavení soubory v karanténě starší než 30 dní jsou automaticky smazány. Pokud chcete tento interval změnit, zadejte novou hodnotu do příslušného pole.
- **Blacklist připojení.** Pokud je tato možnost povolena, Exchange Server odmítá všechny emaily od odesílatelů zapsaných na blacklistu.

  Pro vytvoření blacklistu:
  1. Klikněte na odkaz **Upravit položky v blacklistu**.
  2. Zadejte emailové adresy, které chcete blokovat. Při upravování seznamu můžete použít také následující zástupné znaky pro určení celé emailové domény nebo vzoru emailových adres:
     - Hvězdičku (*), zastupující nula, jeden nebo více znaků.
     - Otazník, (?), zastupující jakýkoli jeden znak.

     Například, pokud zadáte `*@boohouse.com`, všechny emailové adresy z `boohouse.com` budou blokovány.
  3. Klikněte na tlačítko **Save**.

Kontrola IP domény (Antispoofing)

Použijte tento filtr, abyste zabránili spammerům ve spoofingu emailové adresy uživatele a v upravení emailu tak, aby vypadal jako odeslaný od někoho důvěryhodného. Můžete určit IP adresy oprávněné k odesílání emailů na vaše emailové domény a, pokud je třeba, na ostatní známé emailové domény. Pokud email vypadá, že je z domény zapsané na seznamu, ale IP adresa uživatele se neshoduje se zadanými IP adresami, email je odmítnut.

Varování
Nepoužívejte tento filtr, pokud používáte inteligentního hostitele, hostovanou službu filtrování emailů nebo řešení filtrování emailové brány před vašimi Exchange servery.

Důležité

- Filtr kontroluje pouze neověřená emailová připojení.
- Doporučený postup:
  - Tento filtr je doporučené používat pouze na Exchange serverech, které přímo čelí internetu. Například, pokud máte jak Edge Transport, tak Hub Transport servery, nastavte tento filtr pouze na Edge serverech.
  - Přidejte na váš seznam domén všechny interní IP adresy, které mají povolené odesílat emaily přes neověřená SMTP připojení. Tyto mohou zahrnovat automatizované notifikační systémy, síťová vybavení, jako jsou tiskárny, atd.
  - V nastavení Exchange pomocí Skupin dostupnosti databáze přidejte k vašim seznamům domén také IP adresy všech vašich Hub Transport a Mailbox serverů.
  - Buďte opatrní, pokud chcete nastavit autorizované IP adresy pro určité externí emailové domény, které nejsou pod vaší správou. Pokud neudržíte seznam IP adres aktuální, emailové zprávy z těchto domén budou odmítnuty. Pokud používáte MX backup, musíte ke všem externím emailovým doménám přidat nastavené IP adresy, ze kterých MX backup přeposílá emailové zprávy na váš primární mailový server.

Pro nastavení filtrování antispoofingu postupujte podle následujících kroků:

1. Označte pole **Kontrola IP domény (Antispoofing)** pro zapnutí filtru.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.
3. Zadejte emailovou doménu do příslušného pole.
4. Zadejte škálu autorizovaných IP adres, které budou použity s předtím určenou doménou, s použitím formátu CIDR (Maska IP/Sítě).
5. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky. IP adresy jsou přidány do tabulky.
6. Pro odstranění IP škály ze seznamu, klikněte na odpovídající tlačítko ⊗ **Odstranit** na pravé straně tabulky.
7. Klikněte na tlačítko **Save**. Doména je přidána do filtru.

Pro odstranění emailové domény z filtru ji vyberte v tabulce Antispoofing a klikněte na tlačítko ⊖ **Odstranit** v horní části tabulky.

Antimalware

Modul Antimalware chrání Exchange mailové servery před všemi druhy malwarových hrozeb (viry, trojskými koni, spywarem, rootkity, adwarem atd.) tak, že rozpozná nakažené nebo podezřelé soubory a pokusí se je vydezinfikovat, nebo infekci izolovat, v závislosti na určených akcích.

Antimalwarové skenování probíhá a dvou úrovních:

- Úroveň přepravy
- Exchange Store

Skenování na úrovni přepravy

Bitdefender Endpoint Security Tools je integrovaný s agenty mailové přepravy pro skenování veškerého mailového provozu.

Ve výchozím nastavení je skenování na úrovni přepravy zapnuto. Bitdefender Endpoint Security Tools filtruje emailový provoz a, pokud je třeba, informuje uživatele o provedených akcích přidáním textu do těla emailu.

Označte pole **Antimalwarové filtrování** pro vypnutí nebo opětovné zapnutí této funkce.

Pro nastavení notifikačního textu klikněte na odkaz **Nastavení**. K dispozici jsou následující možnosti:

- **Přidat zápatí ke skenovaným emailům.** Označte toto pole pro přidání věty na konec skenovaných emailů. Pro změnu výchozího textu zadejte svou zprávu do textového pole níže.
- **Náhradní text.** K emailům, jejichž přílohy byly smazány nebo vloženy do karantény, může být připojen notifikační soubor. Pro úpravu výchozích notifikačních textů zadejte vaši zprávu do příslušných textových polí.

Antimalwarové skenování je závislé na pravidlech. Každý email, který dorazí na mailový server, je porovnán s pravidly antimalwarového filtrování, v pořadí podle priority, dokud se s některým z pravidel neshodne. Email je poté zpracován na základě možností určených v daném pravidle.

Správa pravidel filtrování

Můžete prohlížet všechna existující pravidla zaznamenaná v tabulce, společně s informacemi ohledně jejich priority, stavu a rozsahu. Pravidla jsou řazena podle priority, přičemž první pravidlo má nejvyšší prioritu.

Jakékoli antimalwarové pravidlo má výchozí pravidlo, které se aktivuje, jakmile je antimalwarové filtrování zapnuto. Co je nutné vědět o výchozím pravidle:

- Toto pravidlo nemůžete kopírovat, vypnout, ani odstranit.
- Můžete upravovat pouze nastavení skenování a akce.
- Výchozí priorita pravidla je vždy nejnižší.

Vytváření pravidel

Při vytváření pravidel pro filtrování máte dvě možnosti:

- Začněte z výchozího nastavení podle následujících kroků:
  1. Klikněte na tlačítko **Přidat** v horní části tabulky pro otevření konfiguračního okna.
  2. Konfigurujte nastavení pravidel. Pro více podrobností o možnostech se odkažte na Možnosti pravidel.
  3. Klikněte na tlačítko **Save**. Pravidlo je v tabulce uvedeno jako první.
- Použijte klon vlastního pravidla jako šablonu podle následujících kroků:
  1. Zvolte požadované pravidlo z tabulky.
  2. Klikněte na tlačítko **Klonovat** v horní části tabulky pro otevření konfiguračního okna.
  3. Vylaďte parametry pravidla podle vašich potřeb.
  4. Klikněte na tlačítko **Save**. Pravidlo je v tabulce uvedeno jako první.

Upravování pravidel

Pro úpravu existujícího pravidla:

1. Klikněte na jméno pravidla pro otevření konfiguračního okna.
2. Zadejte nové hodnoty pro možnosti, které chcete změnit.
3. Klikněte na tlačítko **Save**. Změny vejdou v platnost po uložení pravidla.

Nastavení priority pravidel

Pro změnu priority pravidla:

1. Vyberte pravidlo pro přesunutí.
2. Použijte tlačítka **Nahoru** nebo **Dolů** v horní části tabulky pro zvýšení nebo snížení priority pravidla.

Mazání pravidel

Můžete mazat jedno nebo více vlastních pravidel najednou. Vše, co musíte udělat, je:

1. Označte pole pravidel, která chcete odstranit.
2. Klikněte na tlačítko **Smazat** v horní části tabulky. Jakmile je pravidlo smazáno, nelze ho obnovit.

Možnosti pravidel

K dispozici jsou následující možnosti:

- **Obecné.** V této sekci musíte nastavit jméno pravidla, nebo ho nemůžete uložit. Označte pole **Aktivní**, pokud chcete, aby se pravidlo aktivovalo po uložení.
- **Rozsah pravidla.** Můžete omezit pravidlo, aby platilo jen pro podmnožinu emailů tak, že nastavíte následující hromadné možnosti rozsahu:
  - **Aplikovat na (směr).** Vyberte směr emailového provozu, pro který pravidlo platí.
  - **Odesílatelé.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny odesílatele, nebo pro určité odesílatele. Pro zúžení škály odesílatelů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.
  - **Adresáti.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny adresáty, nebo pouze pro určité adresáty. Pro zúžení škály adresátů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.

    Pravidlo bude uplatněno, pokud se kterýkoli z adresátů shoduje s vaším výběrem. Pokud chcete uplatnit pravidlo pouze v případě, že jsou ve zvolených skupinách všichni adresáti, zvolte **Přiřadit všechny adresáty**.

    Poznámka
    Adresy v polích **Cc** a **Bcc** se také počítají jako příjemci.

    Důležité
    Pravidla založená na uživatelských skupinách platí pouze pro role Hub Transport a Mailbox.

- **Možnosti.** Konfigurujte možnosti skenování pro emaily odpovídající pravidlu:
  - **Skanované typy souborů.** Tuto možnost použijte pro specifikování, které typy souborů chcete aby byli skenovány. Můžete si vybrat aby skenoval všechny soubory (nehledě na jejich příponu), pouze soubory aplikací nebo specifické přípony, které si myslíte, že by mohly být nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

    Poznámka
    Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

Pokud chcete skenovat pouze soubory s určitou příponou, máte dvě možnosti:

- **Uživatelem definované přípony**, zde musíte jen poskytnout přípony které mají být skenované.
- **Všechny soubory, kromě určitých přípon**, kde musíte zadat pouze přípony, které mají být ze skenování vyloučeny.

– **Maximální velikost příloh / statí emailů (MB).** Označte toto zaškrtávací pole a zadejte hodnotu do příslušného pole, čímž nastavíte maximální přijatelnou velikost připojeného souboru nebo statě emailu, který má být skenován.
– **Archivujte maximum struktury (úrovní).** Vyberte zaškrtávací pole a vyberte maximální strukturu v příslušném poli. Čím nižší úroveň hloubky, tím je vyšší výkon a nižší třída ochrany.
– **Skenovat potenciálně nechtěné aplikace (PUA).** Vyberte toto zaškrtávací pole pro skenování možných škodlivých nebo nechtěných aplikací jako je adware, který se nainstaloval do systému bez vědomí uživatele, mění chování vybraných softwarových produktů a snižuje výkon systému.

- **Akce.** Můžete určit akce, které má bezpečností agent automaticky provádět na souborech podle jejich typu.

  Podle typu detekce jsou soubory rozděleny do tří kategorií:

  – **Infikované soubory.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanismů, které zahrnují malwarové signatury, a technologie na bázi machine learning a umělé inteligence (AI).
  – **Podezřelé soubory.** Tyto soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé).
  – **Neskenovatelné soubory.** Tyto soubory nelze skenovat. Neskenovatelné soubory zahrnují, ale ne výlučně, soubory chráněné heslem, šifrované nebo překomprimované soubory.

  Každý typ detekce má jednu hlavní akci a jednu alternativní pro případ, že ta hlavní selže. Přestože to nedoporučujeme, tyto akce je možné změnit v odpovídajících nabídkách. Zvolte akci, kterou si přejete provést:

  – **Dezinfikovat.** Odstraní malwarový kód z nakažených souborů a obnoví původní soubor. V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech. Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.

- **Odmítnout / Odstranit email.** Na serverech s rolí Edge Transport je rozpoznaný email odmítnut s chybovým kódem 550 SMTP. Ve všech ostatních případech je email odstraněn bez varování. Této akci se doporučujeme vyhýbat.
- **Odstranit soubor.** Odstraní problémové přílohy bez varování. Této akci se doporučujeme vyhýbat.
- **Nahradit soubor.** Odstraní problémové soubory a přiloží textový soubor, který upozorní uživatele na přijatá opatření.
- **Přesunout sobuor do karantény.** Přesune rozpoznané soubory do složky s karanténou a přiloží textový soubor informující uživatele o přijatých opatřeních. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Soubory v karanténě můžete spravovat ze stránky **Karanténa**.

  Poznámka
  Mějte prosím na paměti, že karanténa pro Exchange servery vyžaduje na oddílu, na kterém je nainstalovaný bezpečnostní agent, místo na pevném disku navíc. Velikost karantény závisí na počtu uložených položek a jejich velikosti.

- **Nedělat nic.** S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu. Skenování je ve výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení.
- Ve výchozím nastavení, pokud se email shoduje s rámcem pravidel, je s ním speciálně nakládáno v souladu s daným pravidlem, aniž by byl porovnán s jakýmkoli z dalších zbylých pravidel. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel.**

Výjimky

Pokud chcete, aby byl určitý emailový provoz ignorován kterýmkoli filtrovacím pravidlem, můžete určit výjimky ze skenování. Pro vytvoření výjimky:

1. Rozbalte sekci **Výjimky pro Antimalwarová pravidla**.
2. Klikněte na tlačítko ⊖ **Přidat** z panelu nástrojů této sekce, čímž otevřete konfigurační okno.
3. Konfigurujte nastavení výjimek. Pro více podrobností o možnostech se odkažte na Možnosti pravidel.
4. Klikněte na tlačítko **Save**.

Skenování Exchange Store

Exchange Protection používá Exchange Web Services (EWS) od Microsoftu pro umožnění skenování mailové schránky Exchange a databází veřejných složek. Antimalwarový modul můžete nastavit tak, aby spouštěl skenování na vyžádání na cílových databázích pravidelně podle plánu, který určíte.

Poznámka

- Skenování na vyžádání je dostupné pouze pro Exchange Servery s nainstalovanou rolí Mailbox.
- Mějte prosím na paměti, že skenování na vyžádání zvyšuje spotřebu zdrojů a podle parametrů skenování a počtu objektů ke skenování může jeho dokončení trvat značnou dobu.

Skenování na vyžádání vyžaduje účet Exchange administrátora (služební účet) pro zosobnění uživatelů Exchange a pro načtení cílových položek, které mají být skenovány, z emailových schránek uživatelů a veřejných složek. Pro tento účel doporučujeme vytvořit zvláštní účet.

Účet Exchange administrátora musí splňovat následující podmínky:

- Je členem Skupiny pro správu organizace (Exchange 2016, 2013 a 2010)
- Je členem Exchange Skupiny pro správu organizace (Exchange 2007)
- Má přiřazenou mailovou schránku.

Povolení skenování na vyžádání

1. V sekci **Skenovací úlohy** klikněte na odkaz **Přidat pověření**.
2. Zadejte uživatelské jméno a heslo služebního účtu.
3. Pokud se email liší od uživatelského jména, musíte uvést také emailovou adresu služebního účtu.
4. Zadejte URL služeb Exchange Web Services (EWS), nezbytné pro případ, že Exchange Autodiscovery nefunguje.

Poznámka

- Uživatelské jméno musí obsahovat jméno domény, jako v `user@domain` nebo `domain\user`.
- Kdykoli se změní, nezapomeňte pověření upravit v Control Center.

Správa skenovacích úloh

Tabulka skenovacích úloh zobrazuje všechny plánované úlohy a poskytuje informace o jejich cílech a opakování.

Pro vytvoření úloh pro skenování Exchange Store:

1. V sekci **Skenovací úlohy** klikněte na tlačítko ⊕ **Přidat** v horní části tabulky pro otevření konfiguračního okna.
2. Nastavte parametry úloh dle popisu v následující sekci.
3. Klikněte na tlačítko **Save**. Úloha je přidána do seznamu a začne platit po uložení pravidla.

Úlohu můžete kdykoli upravit tak, že kliknete na její jméno.

Pro odstranění úloh ze seznamu je vyberte a klikněte na tlačítko ⊖ **Odstranit** v horní části tabulky.

Nastavení skenovacích úloh

Úlohy mají řadu nastavení, jejichž popis můžete najít níže:

- **Obecné.** Zvolte pro úlohu definující jméno.

  Poznámka
  Název úlohy můžete vidět na časové ose Bitdefender Endpoint Security Tools.

- **Plánovač.** Použijte možnosti plánování pro nastavení skenovacího plánu. Můžete nastavit skenování tak, aby se spouštělo každých pár hodin, dnů nebo týdnů, počínaje od určeného data a času. Pro rozsáhlé databáze může skenování trvat velmi dlouho a může ovlivnit výkon serveru. V takových případech můžete nastavit úlohu tak, aby se po uplynutí určité doby zastavila.
- **Cíl.** Zvolte kontejnery a objekty, které mají být skenovány. Můžete si zvolit skenování mailových schránek, veřejných složek, nebo obou. Kromě emailů, můžete vybrat ke skenování objekty jako jsou **Kontakty**, **Úlohy**, **Schůzky** a **Položky pošty**. Navíc můžete pro skenovaný obsah nastavit následující omezení:
  - Pouze nepřečtené zprávy
  - Pouze položky s přílohami
  - Pouze nové objekty, přijaté za určitý časový interval

  Například, můžete vybrat skenovat emaily z uživatelských mailboxů, přijatých v posledních 7 dnech.

  Označte zaškrtávací pole **Výjimky**, pokud si přejete definovat výjimky ve skenování. Pro vytvoření výjimky, použijte pole z hlavičky tabulky jako například:
  1. Z nabídky zvolte typ úložiště.
  2. Na základě typu úložiště, zadejte objekt, který má být vyloučen:

Typ úložiště	Formát objektu
Mailbox	Emailová adresa
Veřejná Složka	Cesta složky od kořenové složky
Databáze	Identita databáze

Poznámka
Pro získání identity databáze použijte Exchange shell příkaz:
`Get-MailboxDatabase | fl name,identity`

Můžete zadat pouze jednu položku v danou chvíli. Pokud máte několik objektů stejného typu, musíte definovat tolik pravidel jako je počet objektů.

3. Kliknutím na tlačítko ⊕ **Přidat** v horní části tabulky výjimku uložíte a přidáte do seznamu.

Pro odstranění pravidla výjimky ze seznamu klikněte na odpovídající tlačítko ⊖ **Odstranit**.

- **Možnosti.** Konfigurujte možnosti skenování pro emaily odpovídající pravidlu:
  - **Skanované typy souborů.** Tuto možnost použijte pro specifikování, které typy souborů chcete aby byli skenovány. Můžete si vybrat aby skenoval všechny soubory (nehledě na jejich příponu), pouze soubory aplikací nebo specifické přípony, které si myslíte, že by mohly být nebezpečné. Skenování všech souborů poskytuje nejlepší ochranu, zatímco skenování aplikací lze použít k provedení rychlejšího skenu.

    Poznámka
    Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů. Další informace viz „Typy souborů aplikací“ (str. 566).

    Pokud chcete skenovat pouze soubory s určitou příponou, máte dvě možnosti:
    - **Uživatelem definované přípony**, zde musíte jen poskytnout přípony které mají být skenované.
    - **Všechny soubory, kromě určitých přípon**, kde musíte zadat pouze přípony, které mají být ze skenování vyloučeny.
  - **Maximální velikost příloh / statí emailů (MB).** Označte toto zaškrtávací pole a zadejte hodnotu do příslušného pole, čímž nastavíte maximální přijatelnou velikost připojeného souboru nebo statě emailu, který má být skenován.

- **Archivujte maximum struktury (úrovní).** Vyberte zaškrtávací pole a vyberte maximální strukturu v příslušném poli. Čím nižší úroveň hloubky, tím je vyšší výkon a nižší třída ochrany.
- **Skenovat potenciálně nechtěné aplikace (PUA).** Vyberte toto zaškrtávací pole pro skenování možných škodlivých nebo nechtěných aplikací jako je adware, který se nainstaloval do systému bez vědomí uživatele, mění chování vybraných softwarových produktů a snižuje výkon systému.

- **Akce.** Můžete určit akce, které má bezpečností agent automaticky provádět na souborech podle jejich typu.

  Podle typu detekce jsou soubory rozděleny do tří kategorií:
  - **Infikované soubory.** Bitdefender rozpoznává soubory jako infikované pomocí různých pokročilých mechanismů, které zahrnují malwarové signatury, a technologie na bázi machine learning a umělé inteligence (AI).
  - **Podezřelé soubory.** Tyto soubory jsou rozpoznány jako podezřelé pomocí heuristické analýzy a dalších technologií Bitdefender. Tyto poskytují vysokou míru detekce, ale uživatelé musí mít na vědomí, že v určitých případech se jedná o falešná pozitiva (čisté soubory rozpoznané jako podezřelé).
  - **Neskenovatelné soubory.** Tyto soubory nelze skenovat. Neskenovatelné soubory zahrnují, ale ne výlučně, soubory chráněné heslem, šifrované nebo překomprimované soubory.

  Každý typ detekce má jednu hlavní akci a jednu alternativní pro případ, že ta hlavní selže. Přestože to nedoporučejeme, tyto akce je možné změnit v odpovídajících nabídkách. Zvolte akci, kterou si přejete provést:
  - **Dezinfikovat.** Odstraní malwarový kód z nakažených souborů a obnoví původní soubor. V případě některých druhů malwaru není dezinfekce možná, protože detekovaný soubor je celý škodlivý. Toto doporučujeme v každém případě ponechat jako první akci, která bude provedena na infikovaných souborech. Podezřelé soubory nelze dezinfikovat, protože není k dispozici žádný dezinfekční postup.
  - **Odmítnout / Smazat email.** Email je smazán bez jakéhokoli varování. Této akci se doporučujeme vyhýbat.
  - **Odstranit soubor.** Odstraní problémové přílohy bez varování. Této akci se doporučujeme vyhýbat.
  - **Nahradit soubor.** Odstraní problémové soubory a přiloží textový soubor, který upozorní uživatele na přijatá opatření.
  - **Přesunout sobuor do karantény.** Přesune rozpoznané soubory do složky s karanténou a přiloží textový soubor informující uživatele o přijatých

opatřeních. Soubory v karanténě nelze spustit ani otevřít. Proto neexistuje riziko infekce. Soubory v karanténě můžete spravovat ze stránky **Karanténa**.

> **Poznámka**
> Mějte prosím na paměti, že karanténa pro Exchange servery vyžaduje na oddílu, na kterém je nainstalovaný bezpečnostní agent, místo na pevném disku navíc. Velikost karantény závisí na počtu uložených emailů a jejich velikosti.

- **Nedělat nic.** S nalezenými soubory nebude provedena žádná akce. Tyto soubory se pouze zobrazí ve skenovacím protokolu. Skenování je ve výchozím nastavení přednastaveno k ignorování podezřelých souborů. Pokud si přejete přesunout podezřelé soubory do karantény, můžete přenastavit výchozí nastavení.
- Ve výchozím nastavení, pokud se email shoduje s rámcem pravidel, je s ním speciálně nakládáno v souladu s daným pravidlem, aniž by byl porovnán s jakýmkoli z dalších zbylých pravidel. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel.**

Antispam

Modul Antispam nabízí vícevrstevnou ochranu proti spamu a phishingu díky tomu, že využívá kombinaci různých filtrů a strojů pro určení, jestli emaily jsou nebo nejsou spam.

> **Poznámka**
> - Antispamové filtrování je dostupné pro:
>   - Exchange Server 2016/2013 s rolí Edge Transport nebo Mailbox.
>   - Exchange Server 2010/2007 s rolí Edge Transport nebo Hub Transport
> - Pokud máte jak roli Edge, tak Hub ve vaší organizaci Exchange, doporučujeme zapnout antispamové filtrování na serveru s rolí Edge Transport.

Filtrování spamu je automaticky zapnuté pro příchozí emaily. Označte pole **Antispamové filtrování** pro vypnutí nebo opětovné zapnutí této funkce.

Antispamové filtry

Email je porovnán s pravidly antispamového filtrování na základě skupin odesílatelů a adresátů, v pořadí podle priority, dokud se neshodne s některým z pravidel. Email

je poté zpracován podle možností pravidla, a na zjištěném spamu jsou provedena opatření.

Určité antispamové filtry jsou nastavitelné a můžete ovládat, jestli je budete používat, nebo ne. Toto je seznam volitelných filtrů:

- **Filtr znakových sad.** Mnoho spamových emailů je napsáno v cyrilických nebo asijských znakových sadách. Filtr znakových sad takové zprávy detekuje a označí je jako spam.
- **Obsah označený jako sexuálně explicitní.** Spam, který obsahuje sexuálně orientovaný materiál musí obsahovat varování SEXUALLY-EXPLICIT: v předmětu. Tento filtr rozpoznává emaily označené jako SEXUALLY-EXPLICIT: v předmětu a označí je jako spam.
- **URL Filtr.** Téměř všechny spamové emaily obsahují odkazy k různým webovým lokalitám. Tyto lokality obvykle obsahují další reklamy a nabízí možnost něco koupit. Někdy mohou být také použity pro phishing.

  Bitdefender vede databázi takových lokalit. URL filtr porovnává každý URL odkaz v emailu se svou databází. Pokud dojde ke shodě, email je označen jako spam.
- **Seznam Blackhole v reálném čase (RBL).** Toto je filtr, který umožňuje porovnání mailového serveru odesílatele s RBL servery třetích stran. Filtr používá protokol DNSBL a RBL servery pro filtrování spamu na základě reputace mailových serverů jakožto odesílatelů spamu.

  Adresa mailového serveru je extrahována z hlavičky emailu a je kontrolována její platnost. Pokud adresa patří do soukromé třídy (`10.0.0.0`, `172.16.0.0` do `172.31.0.0` nebo `192.168.0.0` do `192.168.255.0`), je ignorována.

  Na doméně `d.c.b.a.rbl.example.com`, kde `d.c.b.a` je otočená IP adresa serveru a `rbl.example.com` je RBL server, je provedena kontrola DNS. Pokud DNS potvrdí platnost domény, znamená to, že IP je zapsáno na RBL serveru, a je poskytnuto určité skóre serveru. Toto skóre má rozsah mezi 0 a 100, podle úrovně důvěry, kterou jste serveru povolili.

  Vyšetření je provedeno pro každý RBL server ze seznamu a skóre, které se vrátí z každého z nich, je přidáno do meziskóre. Jakmile skóre dosáhne 100, nejsou prováděna žádná další vyšetřování.

  Pokud je skóre RBL filtru 100 nebo vyšší, email je považován za spam a je provedeno zadané opatření. V opačném případě je skóre vypočítáno ze skóre RBL filtru a přidáno k celkovému spamovému skóre daného emailu.

- **Heuristický filtr.** Vyvinut společností Bitdefender, Heuristický filtr detekuje nový a neznámý spam. Filtr je automaticky trénován na obrovském objemu spamových emailů v Antispamové laboratoři společnosti Bitdefender. Během výcviku se naučí rozlišovat mezi spamem a legitimními emaily a rozpoznávat nový spam díky zaznamenání jeho podobností, často nenápadných, s emaily, které již prohlédl. Tento filtr je navržen pro zdokonalení detekce na bázi signatur, zatímco udržuje počet falešných poplachů na velmi nízké úrovni.
- **Bitdefender Cloud Query.** Bitdefender vede neustále se vyvíjející databází "otisku prstů" spamových emailů v cloudu. Dotaz ohledně otisku prstů emailu je odeslán na cloudové servery pro rychlé ověření, jestli je email spam. I když otisk prstů není nalezen v databázi, je porovnán s ostatními nedávnými případy a, pokud jsou naplněny určité podmínky, email je označen jako spam.

Správa Antispamových pravidel

Můžete prohlížet všechna existující pravidla zaznamenaná v tabulce, společně s informacemi ohledně jejich priority, stavu a rozsahu. Pravidla jsou řazena podle priority, přičemž první pravidlo má nejvyšší prioritu.

Antispamové zásady obsahují výchozí pravidlo, které se aktivuje po zapnutí modulu. Co je nutné vědět o výchozím pravidle:

- Toto pravidlo nemůžete kopírovat, vypnout, ani odstranit.
- Můžete upravovat pouze nastavení skenování a akce.
- Výchozí priorita pravidla je vždy nejnižší.

Vytváření pravidel

Pro vytvoření pravidla:

1. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky pro otevření konfiguračního okna.
2. Konfigurujte nastavení pravidel. Pro více detailů ohledně možností se prosím odkažte na „Možnosti pravidel“ (str. 357).
3. Klikněte na tlačítko **Save**. Pravidlo je v tabulce uvedeno jako první.

Upravování pravidel

Pro úpravu existujícího pravidla:

1. Klikněte na jméno pravidla pro otevření konfiguračního okna.
2. Zadejte nové hodnoty pro možnosti, které chcete změnit.
3. Klikněte na tlačítko **Save**. Pokud je pravidlo aktivní, změny vejdou v platnost po uložení pravidla.

Nastavení priority pravidel

Pro změnu priority pravidla ho vyberte a použijte směrové šipky **Nahoru** and **Dolů**, umístěné v horní části tabulky. Můžete přesouvat vždy pouze jedno pravidlo.

Mazání pravidel

Pokud pravidlo již nechcete používat, vyberte ho a klikněte na tlačítko **Odstranit** v horní části tabulky.

Možnosti pravidel

K dispozici jsou následující možnosti:

- **Obecné.** V této sekci musíte nastavit jméno pravidla, nebo ho nemůžete uložit. Označte pole **Aktivní**, pokud chcete, aby se pravidlo aktivovalo po uložení.
- **Rozsah pravidla.** Můžete omezit pravidlo, aby platilo jen pro podmnožinu emailů tak, že nastavíte následující hromadné možnosti rozsahu:
  - **Aplikovat na (směr).** Vyberte směr emailového provozu, pro který pravidlo platí.
  - **Odesílatelé.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny odesílatele, nebo pro určité odesílatele. Pro zúžení škály odesílatelů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.
  - **Adresáti.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny adresáty, nebo pouze pro určité adresáty. Pro zúžení škály adresátů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.

    Pravidlo bude uplatněno, pokud se kterýkoli z adresátů shoduje s vaším výběrem. Pokud chcete uplatnit pravidlo pouze v případě, že jsou ve zvolených skupinách všichni adresáti, zvolte **Přiřadit všechny adresáty**.

    Poznámka
    Adresy v polích **Cc** a **Bcc** se také počítají jako příjemci.

    Důležité
    Pravidla založená na uživatelských skupinách platí pouze pro role Hub Transport a Mailbox.

- **Nastavení.** Klikněte na úroveň bezpečnosti, která nejlépe vyhovuje vašim potřebám (**Agresivní**, **Normální** nebo **Tolerantní**). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.

Navíc můžete povolit také různé filtry. Pro podrobné informace ohledně těchto filtrů se podívejte na „Antispamové filtry“ (str. 354).

Důležité
RBL filtr vyžaduje přídatnou konfiguraci. Filtr můžete nastavit poté, co jste vytvořili nebo upravili pravidlo. Další informace viz „Konfigurace RBL filtru“ (str. 359)

Pro oprávněná připojení můžete zvolit, jestli chcete provádět antispamové skenování, nebo ne.

- **Akce.** Je několik akcí, které můžete provádět na zjištěných emailech. Každá akce má, jakmile přijde na řadu, několik proveditelných možností nebo sekundárních akcí. Jejich popis naleznete níže:

  Hlavní akce:
  - **Doručit email.** Spam dorazí do emailových schránek adresátů.
  - **Vložit email do karantény.** Email je šifrován a uložen do složky karantény na Exchange serveru, aniž by byl doručen adresátům. Emaily v karanténě můžete spravovat ze stránky **Karanténa**.
  - **Přesměrovat email na.** Email není doručen původním adresátům, ale do emailové schránky, kterou určíte v příslušném poli.
  - **Odmítnout / Odstranit email.** Na serverech s rolí Edge Transport je rozpoznaný email odmítnut s chybovým kódem 550 SMTP. Ve všech ostatních případech je email odstraněn bez varování. Této akci se doporučujeme vyhýbat.

  Sekundární akce:
  - **Integrovat s Exchange SCL.** Přidá hlavičku spamovému emailu, čímž umožní Exchange Serveru nebo Microsoft Outlooku provést akci v souladu s mechanismem Spam Confidence Level (SCL).
  - **Označit předmět emailu jako.** Můžete přidat štítek k předmětu emailu, a pomoci tak uživatelům ve filtrování odhalených emailů v jejich emailovém klientovi.
  - **Přidat hlavičku emailu.** Emailům rozpoznaným jako spam je přidána hlavička. Můžete upravovat jméno a hodnotu hlavičky tak, že zadáte požadované hodnoty do příslušných polí. Dále můžete tuto emailovou hlavičku použít pro vytvoření přídatných filtrů.
  - **Uložit email na disk.** Kopie spamového emailu je uložena jako soubor do určené složky. Do příslušného pole zadejte kompletní cestu ke složce.

Poznámka
Tato možnost podporuje pouze emaily ve formátu MIME.

- **Archivovat na účet.** Kopie odhaleného emailu je doručena na určenou emailovou adresu. Tato akce přidá určenou emailovou adresu k seznamu emailových Bcc.

- Ve výchozím nastavení, pokud se email shoduje s rámcem pravidel, je s ním speciálně nakládáno v souladu s daným pravidlem, aniž by byl porovnán s jakýmkoli z dalších zbylých pravidel. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel.**

Konfigurace RBL filtru

Pokud chcete použít RBL filtr, musíte uvést seznam RBL serverů.

Pro nastavení tohoto filtru:

1. Na stránce **Antispam** klikněte na odkaz **Nastavení** pro otevření konfiguračního okna.
2. Do odpovídajících polí uveďte IP adresu DNS serveru, na který se chcete dotazovat, a dobu časového limitu dotazu. Pokud není nastavena žádná adresa DNS serveru, nebo pokud je DNS server nedostupný, RBL filtr používá systémové DNS servery.
3. Pro každý RBL server:
   a. Zadejte jméno hostitelského serveru nebo IP adresu a úroveň důvěryhodnosti, kterou jste serveru přiřadili, do polí pod záhlavím tabulky.
   b. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky.
4. Klikněte na tlačítko **Save**.

Nastavení Whitelistu odesílatelů

Pro známé emailové odesílatele můžete zabránit zbytečné spotřebě zdrojů serveru tak, že je přidáte na seznamy pro důvěryhodné nebo nedůvěryhodné odesílatele. Tím pádem bude mailový server pokaždé buď přijímat, nebo odmítat emaily příchozí od těchto odesílatelů. Například, když vedete vážnou emailovou komunikaci s obchodním partnerem a chcete mít jistotu, že vám přijdou všechny jeho emaily, můžete partnera přidat na whitelist.

Pro vytvoření whitelistu důvěryhodných odesílatelů:

1. Klikněte na odkaz **Whitelist** pro otevření konfiguračního okna.
2. Označte pole **Whitelist odesílatelů**.

3. Zadejte emailové adresy do příslušného pole. Při upravování seznamu můžete použít také následující zástupné znaky pro určení celé emailové domény nebo vzoru emailových adres:
   - Hvězdičku (*), zastupující nula, jeden nebo více znaků.
   - Otazník, (?), zastupující jakýkoli jeden znak.

   Například, pokud zadáte `*.gov`, všechny emaily příchozí z domény `.gov` budou přijaty.
4. Klikněte na tlačítko **Save**.

Poznámka
Pro přidání známých odesílatelů spamu na blacklist použijte možnost **Blacklist připojení** v sekci **Exchange Protection > Obecné > Nastavení**.

Kontrola obsahu

Použijte Kontrolu obsahu pro zvýšení ochrany emailů tím, že budete filtrovat všechen emailový provoz, který není v souladu se zásadami vaší společnosti (nežádaný nebo potenciálně citlivý obsah).

Pro celkovou kontrolu nad veškerým emailovým obsahem, tento modul sestává ze dvou možností filtrování emailů:

- Filtrování obsahu
- Filtrování příloh

Poznámka
Filtrování obsahu a Filtrování příloh jsou k dispozici pro:
- Exchange Server 2016/2013 s rolí Edge Transport nebo Mailbox.
- Exchange Server 2010/2007 s rolí Edge Transport nebo Hub Transport

Správa pravidel filtrování

Filtry Kontroly obsahu jsou závislé na pravidlech. Pro různé uživatele a skupiny uživatelů můžete určit různá pravidla. Každý email, který dorazí na mailový server, je porovnán s pravidly antimalwarového filtrování, v pořadí podle priority, dokud se s některým z pravidel neshodne. Email je poté zpracován na základě možností určených v daném pravidle.

Pravidla filtrování obsahu mají přednost před pravidly filtrování příloh.

Pravidla pro filtrování obsahu a příloh jsou zaznamenána v příslušných tabulkách v pořadí podle priority, kde první pravidlo má nejvyšší prioritu. Pro každé pravidlo jsou zobrazeny následující informace:

- Priorita
- Jméno
- Směr přenosu
- Odesílatelé a skupiny adresátů

Vytváření pravidel

Při vytváření pravidel pro filtrování máte dvě možnosti:

- Začněte z výchozího nastavení podle následujících kroků:
  1. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky pro otevření konfiguračního okna.
  2. Konfigurujte nastavení pravidel. Pro podrobnosti ohledně filtrování určitého obsahu a příloh se podívejte na:
     - Možnosti Pravidel filtrování obsahu
     - Možnosti Pravidel filtrování příloh.
  3. Klikněte na tlačítko **Save**. Pravidlo je v tabulce uvedeno jako první.
- Použijte klon vlastního pravidla jako šablonu podle následujících kroků:
  1. Zvolte požadované pravidlo z tabulky.
  2. Klikněte na tlačítko ⧉ **Klonovat** v horní části tabulky pro otevření konfiguračního okna.
  3. Upravte parametry pravidla dle svých potřeb.
  4. Klikněte na tlačítko **Save**. Pravidlo je v tabulce uvedeno jako první.

Upravování pravidel

Pro úpravu existujícího pravidla:

1. Klikněte na jméno pravidla pro otevření konfiguračního okna.
2. Zadejte nové hodnoty pro možnosti, které chcete změnit.
3. Klikněte na tlačítko **Save**. Změny vejdou v platnost po uložení pravidla.

Nastavení priority pravidel

Pro změnu priority pravidla:

1. Vyberte pravidlo pro přesunutí.
2. Použijte tlačítka ▲ **Nahoru** nebo ▼ **Dolů** v horní části tabulky pro zvýšení nebo snížení priority pravidla.

Mazání pravidel

Můžete odstranit jedno nebo více vlastních pravidel. Vše, co musíte udělat, je:

1. Zvolte pravidla, která chcete smazat.
2. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky. Jakmile je pravidlo smazáno, nelze ho obnovit.

Filtrování obsahu

Filtrování obsahu vám pomáhá filtrovat emailový provoz na základě znakových řetězců, které jste předtím určili. Tyto řetězce jsou porovnány s předmětem emailu, nebo s textovým obsahem jeho těla. Používáním Filtrování obsahu můžete dosáhnout těchto cílů:

- Zabraňte nežádanému emailovému obsahu ve vstupu do emailových schránek Exchange Serveru.
- Blokujte odchozí emaily obsahující důvěrné údaje.
- Archivujte emaily, které splňují určité podmínky, na jiný emailový účet nebo na disk. Například, můžete ukládat emaily odeslané na váš firemní email podpory do složky na místním disku.

Povolení Filtrování obsahu

Pokud chcete používat filtrování obsahu, označte pole **Filtrování obsahu**.

Ohledně vytváření a správy pravidel filtrování obsahu se odkažte na „Správa pravidel filtrování“ (str. 360).

Možnosti pravidel

- **Obecné.** V této sekci musíte nastavit jméno pravidla, nebo ho nemůžete uložit. Označte pole **Aktivní**, pokud chcete, aby se pravidlo aktivovalo po uložení.
- **Rozsah pravidla.** Můžete omezit pravidlo, aby platilo jen pro podmnožinu emailů tak, že nastavíte následující hromadné možnosti rozsahu:
  - **Aplikovat na (směr).** Vyberte směr emailového provozu, pro který pravidlo platí.
  - **Odesílatelé.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny odesílatele, nebo pro určité odesílatele. Pro zúžení škály odesílatelů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.
  - **Adresáti.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny adresáty, nebo pouze pro určité adresáty. Pro zúžení škály adresátů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.

Pravidlo bude uplatněno, pokud se kterýkoli z adresátů shoduje s vaším výběrem. Pokud chcete uplatnit pravidlo pouze v případě, že jsou ve zvolených skupinách všichni adresáti, zvolte **Přiřadit všechny adresáty**.

Poznámka
Adresy v polích **Cc** a **Bcc** se také počítají jako příjemci.

Důležité
Pravidla založená na uživatelských skupinách platí pouze pro role Hub Transport a Mailbox.

- **Nastavení.** Nastavte výrazy, které mají být vyhledávány v emailech, podle popisu níže:
  1. Zvolte část emailu, kterou chcete kontrolovat:
     - Předmět emailu, označením pole **Filtrovat podle předmětu**. Budou filtrovány všechny emaily, jejichž předmět obsahuje jakýkoli z výrazů zadaných do příslušné tabulky.
     - Obsah těla, označením pole **Filtrovat podle obsahu těla**. Budou filtrovány všechny emaily, jejichž tělo obsahuje kterýkoli ze zadaných výrazů.
     - Předmět i obsah těla, označením obou polí. Budou filtrovány všechny emaily, jejichž předmět odpovídá jakémukoli pravidlu z první tabulky A jejich tělo obsahuje kterýkoli z výrazů z druhé tabulky. Například:

       První tabulka obsahuje výrazy: `zpravodaj` a `týdenní`. Druhá tabulka obsahuje výrazy: `nakupování`, `cena` a `nabídka`.

       Email s předmětem "Měsíční **zpravodaj** Vašeho oblíbeného obchodu s hodinkami" a s tělem, které obsahuje frázi "Máme to potěšení Vám představit naši nejnovější **nabídku** senzačních hodinek za neodolatelné **ceny**.", se shoduje s pravidlem a bude filtrován. Pokud je předmět "Novinky od Vašeho prodejce hodinek", email nebude filtrován.
  2. Sestavte seznamy podmínek pomocí polí v záhlaví tabulky. Pro každou podmínku postupujte následovně:
     a. Zvolte typ výrazu používaný ve vyhledávání. Můžete si vybrat, zda zadáte přesný textový výraz, nebo zda vytvoříte textové vzorce s využitím častých výrazů.

        Poznámka
        Syntax častých výrazů je ověřen porovnáním s gramatikou ECMAScript.

b. Zadejte vyhledávací řetězec do pole **Výraz**.

Například:

i. Výraz `5[1-5]\d{2}([\s\-]?\d{4}){3}` se shoduje s s čísly bankovních karet, která začínají padesát jedničkou až po padesát pětku, mají šestnáct číslovek ve skupinách po čtyřech a tyto skupiny mohou být odděleny mezerou nebo pomlčkou. Tudíž bude filtrován jakýkoli email obsahující číslo karty v jednom z těchto formátů: `5257-4938-3957-3948`, `5257 4938 3957 3948` nebo `5257493839573948`.

ii. Tento výraz odhaluje emaily obsahující slova `loterie`, `hotovost` a `cena`, nalezené přesně v tomto pořadí:

```
(lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
```

Pro odhalení emailů, které obsahují každé z těchto slov nezávisle na jejich pořadí, přidejte tři časté výrazy s různým pořadím slov.

iii. Tento výraz odhaluje emaily, které obsahují tři nebo více výskytů slova `cena`:

```
(prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
```

c. Pokud chcete odlišit velká písmena od malých písmen v porovnávání textů, označte pole **Rozlišovat velikost písmen**. Například, pokud je pole označeno, `Zpravodaj` nebude to samé, jako `zpravodaj`.

d. Pokud chcete, aby výraz nebyl součástí ostatních slov, označte pole **Celé slovo**. Například, pokud je pole označeno, výraz `Annina výplata` se nebude shodovat s `MariAnnina výplata`..

e. Klikněte na tlačítko ⊕ **Přidat** v záhlaví sloupce **Akce** pro přidání podmínky do seznamu.

- **Akce.** Na emailech můžete provádět několik možných akcí. Každá akce má, jakmile přijde na řadu, několik proveditelných možností nebo sekundárních akcí. Jejich popis naleznete níže:

  Hlavní akce:
  - **Doručit email.** Odhalený email dorazí do emailových schránek adresátů.

- **Karanténa.** Email je šifrován a uložen do složky karantény na Exchange serveru, aniž by byl doručen adresátům. Emaily v karanténě můžete spravovat ze stránky **Karanténa**.
- **Přesměrovat na.** Email není doručen původním adresátům, ale do emailové schránky, kterou určíte v příslušném poli.
- **Odmítnout / Odstranit email.** Na serverech s rolí Edge Transport je rozpoznaný email odmítnut s chybovým kódem 550 SMTP. Ve všech ostatních případech je email odstraněn bez varování. Této akci se doporučujeme vyhýbat.

Sekundární akce:

- **Označit předmět emailu jako.** Můžete přidat štítek k předmětu problémového emailu, a pomoci tak uživatelům ve filtrování emailů v jejich emailovém klientovi.
- **Přidat hlavičku k emailovým zprávám.** Můžete přidat jméno a hodnotu hlavičkám problémových emailů tak, že zadáte požadované hodnoty do odpovídajících polí.
- **Uložit email na disk.** Kopie problémového emailu je uložena jako soubor do určené složky na Exchange Serveru. Pokud složka neexistuje, bude vytvořena. Do příslušného pole musíte zadat kompletní cestu ke složce.

  Poznámka
  Tato možnost podporuje pouze emaily ve formátu MIME.

- **Archivovat na účet.** Kopie odhaleného emailu je doručena na určenou emailovou adresu. Tato akce přidá určenou emailovou adresu k seznamu emailových Bcc.

- Ve výchozím stavu email, který naplní podmínky pravidla, už není porovnáván s dalšími pravidly. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel**.

Výjimky

Pokud chcete, aby byl určitý emailový přenos pro konkrétní odesílatele nebo adresáty doručen nehledě na jakékoli pravidlo pro filtrování obsahu, můžete nastavit výjimky z filtrování.

Pro vytvoření výjimky:

1. Klikněte na odkaz **Výjimky** vedle zaškrtávacího pole **Filtrování obsahu**. Tato akce otevře konfigurační okno.

2. Zadejte emailové adresy důvěryhodných odesílatelů a/nebo příjemců do příslušných polí. Jakýkoli příchozí email od důvěryhodného uživatele nebo odchozí pro důvěryhodného adresáta je vynechán z filtrování. Při upravování seznamu můžete použít také následující zástupné znaky pro určení celé emailové domény nebo vzoru emailových adres:
   - Hvězdičku (*), zastupující nula, jeden nebo více znaků.
   - Otazník, (?), zastupující jakýkoli jeden znak.

   Například, pokud zadáte `*.gov`, všechny emaily příchozí z domény `.gov` budou přijaty.
3. Pro emaily s více adresáty můžete označit pole **Vynechat email z filtrování pouze v případě, že jsou všichni adresáti důvěryhodní** a aplikovat výjimku pouze, když jsou všichni adresáti emailu přítomni na seznamu důvěryhodných adresátů.
4. Klikněte na tlačítko **Save**.

Filtrování příloh

Modul Filtrování příloh poskytuje filtrovací funkce pro emailové přílohy. Dokáže rozpoznat přílohy s určitým jmenným vzorcem nebo přílohy určitého typu. Používáním Filtrování příloh můžete:

- Blokovat potenciálně nebezpečné přílohy, jako jsou soubory `.vbs` or `.exe`, nebo emaily, které je obsahují.
- Blokujte přílohy s pohoršlivými názvy nebo emaily, které je obsahují.

Povolení Filtrování příloh

Pokud chcete používat filtrování příloh, označte pole **Filtrování příloh**.

Ohledně vytváření a správy pravidel filtrování příloh se odkažte na „Správa pravidel filtrování“ (str. 360).

Možnosti pravidel

- **Obecné.** V této sekci musíte nastavit jméno pravidla, nebo ho nemůžete uložit. Označte pole **Aktivní**, pokud chcete, aby se pravidlo aktivovalo po uložení.
- **Rozsah pravidla.** Můžete omezit pravidlo, aby platilo jen pro podmnožinu emailů tak, že nastavíte následující hromadné možnosti rozsahu:
  - **Aplikovat na (směr).** Vyberte směr emailového provozu, pro který pravidlo platí.
  - **Odesílatelé.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny odesílatele, nebo pro určité odesílatele. Pro zúžení škály odesílatelů klikněte

na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.

– **Adresáti.** Můžete se rozhodnout, jestli bude pravidlo platit pro všechny adresáty, nebo pouze pro určité adresáty. Pro zúžení škály adresátů klikněte na tlačítko **Určití** a vyberte požadované skupiny z tabulky na levé straně. Prohlížejte zvolené skupiny v tabulce napravo.

  Pravidlo bude uplatněno, pokud se kterýkoli z adresátů shoduje s vaším výběrem. Pokud chcete uplatnit pravidlo pouze v případě, že jsou ve zvolených skupinách všichni adresáti, zvolte **Přiřadit všechny adresáty**.

  Poznámka
  Adresy v polích **Cc** a **Bcc** se také počítají jako příjemci.

  Důležité
  Pravidla založená na uživatelských skupinách platí pouze pro role Hub Transport a Mailbox.

- **Nastavení.** Určete soubory, které jsou povolené nebo zakázané v emailových přílohách.

  Emailové přílohy můžete filtrovat podle typu nebo podle názvu souboru.

  Pro filtrování příloh podle typu souboru postupujte podle následujících kroků:
  1. Označte pole **Detekovat podle typu obsahu**.
  2. Zvolte možnost detekce, která lépe vyhovuje vašem potřebám:
     – **Pouze následující kategorie**, pokud máte omezený seznam zakázaných kategorií typů souboru.
     – **Všechno kromě následujících kategorií**, pokud máte omezený seznam povolených kategorií typů souboru.
  3. Ze seznamu vyberte kategorie typů souboru, které vás zajímají. Pro podrobnosti o příponách v každé kategorii se podívejte na „Typy souborů Filtrování příloh“ (str. 567).

     Pokud vás zajímají pouze určité typy souborů, označte pole **Vlastní přípony** a zadejte seznam přípon do příslušného pole.
  4. Označte pole **Povolit detekci skutečného typu** pro kontrolu hlaviček souborů a správnou identifikaci typu přiloženého souboru při skenování pro omezený počet přípon. Toto znamená, že pro obejití pravidel filtrování příloh nelze příponu jednoduše přejmenovat.

Poznámka
Detekce skutečného typu může být náročná na zdroje.

Pro filtrování příloh podle jejich jména označte pole **Detekovat podle názvu souboru** a zadejte jména souborů, která chcete filtrovat, do příslušného pole. Při upravování seznamu můžete použít také následující zástupné znaky pro definování vzorců:

- Hvězdičku (*), zastupující nula, jeden nebo více znaků.
- Otazník, (?), zastupující jakýkoli jeden znak.

Například, pokud zadáte `database.*`, budou detekovány všechny soubory pojmenované `database`, nehledě na jejich příponu.

Poznámka
Pokud povolíte detekci podle typu obsahu i podle názvu souboru (bez detekce skutečného typu), soubor musí současně splňovat podmínky pro oba druhy detekce. Například, pokud jste zvolili kategorii **Multimédia** a zadali jméno souboru `test.pdf`. V tomto případě může přes pravidlo přejít jakýkoli email, protože soubor PDF není multimediální soubor.

Označte pole **Skenování uvnitř archivů**, abyste zabránili blokovaným souborům v ukrývání se ve zdánlivě neškodných archivech, a tím pádem v obcházení filtrovacího pravidla.

Skenování uvnitř archivů je opakované a ve výchozím stavu pokračuje až do čtvrté úrovně hloubky archivu. Skenování můžete optimalizovat následovně:

1. Označte pole **Maximální hloubka archivu (úrovně)**.
2. V příslušné nabídce zvolte jinou hodnotu. Pro nejvyšší výkon zvolte nejnižší hodnotu, pro maximální ochranu zvolte nejvyšší hodnotu.

Poznámka
Pokud jste zvolili skenování archivů, **Skenování uvnitř archivů** je vypnuté a všechny archivy jsou skenovány.

- **Akce.** Na odhalených přílohách nebo na emailech, které je obsahují, můžete provádět několik akcí. Každá akce má, jakmile přijde na řadu, několik proveditelných možností nebo sekundárních akcí. Jejich popis naleznete níže:

Hlavní akce:

- **Nahradit soubor.** Odstraní problémové soubory a přiloží textový soubor, který upozorní uživatele na přijatá opatření.

  Pro nastavení varovného textu:

  1. Klikněte na odkaz **Nastavení** vedle zaškrtávacího pole **Filtrování příloh**.
  2. Zadejte varovnou zprávu do odpovídajícího pole.
  3. Klikněte na tlačítko **Save**.
- **Odstranit soubor.** Odstraní problémové přílohy bez varování. Této akci se doporučujeme vyhýbat.
- **Odmítnout / Odstranit email.** Na serverech s rolí Edge Transport je problémový email odmítnut s chybovým kódem 550 SMTP. Ve všech ostatních případech je email odstraněn bez varování. Této akci se doporučujeme vyhýbat.
- **Vložit email do karantény.** Email je šifrován a uložen do složky karantény na Exchange serveru, aniž by byl doručen adresátům. Emaily v karanténě můžete spravovat ze stránky **Karanténa**.
- **Přesměrovat email na.** Email není doručen původním adresátům, ale na emailovou adresu, kterou určíte v příslušném poli.
- **Doručit email.** Nechá email projít skrz.

Sekundární akce:

- **Označit předmět emailu jako.** Můžete přidat štítek k předmětu problémového emailu, a pomoci tak uživatelům ve filtrování emailů v jejich emailovém klientovi.
- **Přidat hlavičku emailu.** Můžete přidat jméno a hodnotu hlavičkám problémových emailů tak, že zadáte požadované hodnoty do odpovídajících polí.
- **Uložit email na disk.** Kopie problémového emailu je uložena jako soubor do určené složky na Exchange Serveru. Pokud složka neexistuje, bude vytvořena. Do příslušného pole musíte zadat kompletní cestu ke složce.

  Poznámka
  Tato možnost podporuje pouze emaily ve formátu MIME.

- **Archivovat na účet.** Kopie odhaleného emailu je doručena na určenou emailovou adresu. Tato akce přidá určenou emailovou adresu k seznamu emailových Bcc.

- Ve výchozím nastavení, pokud se email shoduje s rámcem pravidel, je s ním speciálně nakládáno v souladu s daným pravidlem, aniž by byl porovnán s jakýmkoli z dalších zbylých pravidel. Jestli chcete pokračovat v kontrole proti ostatním pravidlům, vyčistěte pole **Pokud jsou splněny podmínky pravidla, zastavte zpracování dalších pravidel.**

Výjimky

Pokud chcete, aby byl určitý emailový přenos pro konkrétní odesílatele nebo adresáty doručen nehledě na jakékoli pravidlo pro filtrování příloh, můžete nastavit výjimky z filtrování.

Pro vytvoření výjimky:

1. Klikněte na odkaz **Výjimky** vedle zaškrtávacího pole **Filtrování příloh** Tato akce otevře konfigurační okno.
2. Zadejte emailové adresy důvěryhodných odesílatelů a/nebo příjemců do příslušných polí. Jakýkoli příchozí email od důvěryhodného uživatele nebo odchozí pro důvěryhodného adresáta je vynechán z filtrování. Při upravování seznamu můžete použít také následující zástupné znaky pro určení celé emailové domény nebo vzoru emailových adres:
   - Hvězdičku (*), zastupující nula, jeden nebo více znaků.
   - Otazník, (?), zastupující jakýkoli jeden znak.

   Například, pokud zadáte `*.gov`, všechny emaily příchozí z domény `.gov` budou přijaty.
3. Pro emaily s více adresáty můžete označit pole **Vynechat email z filtrování pouze v případě, že jsou všichni adresáti důvěryhodní** a aplikovat výjimku pouze, když jsou všichni adresáti emailu přítomni na seznamu důvěryhodných adresátů.
4. Klikněte na tlačítko **Save**.

7.2.12. Šifrování

Poznámka
Tento modul je k dispozici pro:

- Windows pro pracovní stanice
- Windows pro servery
- macOS

Modul Encryption spravuje úplné šifrování na koncových bodech pomocí nástroje BitLocker na systémech Windows a FileVault a nástroj příkazového řádku diskutil na makrech.

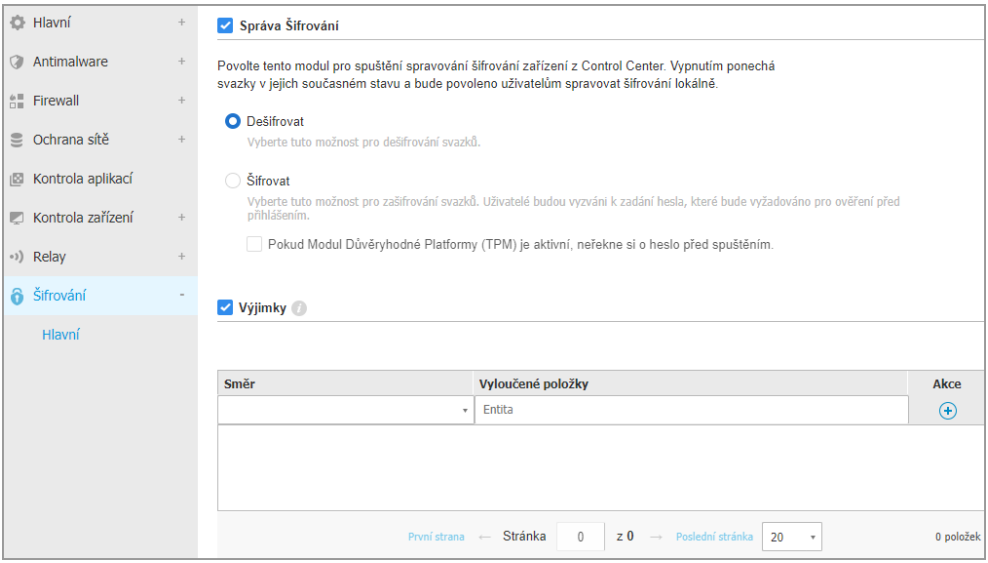
S tímto přístupem, dovede GravityZone dodat stálé konzistentní výhody:

- Data zabezpečená v případě ztráty nebo odcizení zařízení.
- Rozsáhlá ochrana nejoblíbenějších počítačových platforem na světě pomocí doporučených standardů šifrování s plnou podporou společnosti Microsoft a Apple.
- Minimální vliv na výkon koncových bodů díky optimalizovaným nástrojům nativního šifrování.

Modul Encryption používá následující řešení:

- BitLocker verze 1.2 a novější, na koncových bodech systému Windows s modulem TPM (Trusted Platform Module) pro bootovací a nebootovací svazky.
- BitLocker verze 1.2 a novější, v koncových bodech systému Windows bez modulu TPM, pro bootovací a nebootovací svazky.
- FileVault v koncových bodech MacOS, pro spouštěcí svazky.
- diskutil nástroj na koncových bodech s macOS, pro non-boot svazky.

Seznam operačních systémů podporovaných šifrovacím modulem naleznete v příručce GravityZone Instalační příručka.



Stránka Šifrování

Chcete-li zahájit správu šifrování koncových bodů z Control Center, zaškrtněte políčko **Správa šifrování**. Pokud je toto nastavení povoleno, koncoví uživatelé nemohou spravovat šifrování lokálně a všechny jejich akce budou zrušeny nebo vráceny. Zakázání tohoto nastavení ponechá koncové svazky v jejich aktuálním stavu (šifrované nebo nezašifrované) a uživatelé budou moci spravovat šifrování na svých počítačích.

Pro správu procesů šifrování a dešifrování jsou k dispozici tři možnosti:

- **Dešifrovat** - dešifruje svazky a udržuje je dešifrované, když je pravidlo na koncových bodech aktivní.
- **Šifrovat** - šifruje svazky a udržuje je šifrované, když je pravidlo na koncových bodech aktivní.

  Ve volbě Šifrovat můžete zaškrtnout políčko **Pokud je modul TPM (Trusted Platform Module) aktivní, nepožadujte heslo pro šifrování** . Toto nastavení poskytuje šifrování na koncových bodech systému Windows pomocí modulu TPM, aniž by bylo vyžadováno heslo pro šifrování od uživatelů. Více informací naleznete na „Šifrování svazků“ (str. 373).
- **Výjimky**

GravityZone podporuje metodu AES (Advanced Encryption Standard) se 128 a 256bitovými klíči na Windows a MacOS. Skutečný použitý šifrovací algoritmus závisí na konfiguraci každého operačního systému.

Poznámka
GravityZone detects and manages volumes manually encrypted with BitLocker, FileVault and diskutil. Chcete-li spustit správu těchto svazků, agent zabezpečení vyzve uživatele koncového bodu ke změně jejich klíčů pro obnovení. V případě použití jiných šifrovacích řešení musí být svazky před použitím politiky/pravidla GravityZone dešifrovány.

Šifrování svazků

Pro šifrování svazků:

1. Zaškrtněte políčko **Správa šifrování**.
2. Vyberte možnost **Šifrovat**.

Šifrovací proces začne, jakmile je pravidlo aktivováno na koncových bodech, s určitými zvláštnostmi pro Windows a Mac.

Na Windows

Ve výchozím nastavení agent zabezpečení vyzve uživatele ke konfiguraci hesla ke spuštění šifrování. Pokud má stroj funkční TPM, agent zabezpečení vyzve uživatele, aby nakonfigurovali osobní identifikační číslo (PIN) pro spuštění šifrování. Uživatel musí zadat heslo zadané v tomto kroku pokaždé když se spustí stroj v autentizačním okně před spuštěním operačního systému (pre-boot authentication screen).

Poznámka
Agent zabezpečení umožňuje konfigurovat požadavky na složitost PIN kódu a oprávnění uživatelů měnit jejich PIN kód prostřednictvím nastavení BitLocker (GPO) skupinové politiky.

Pokud chcete spustit šifrování aniž by bylo požadováno od uživatele heslo, tak zapněte tuto volbu v označovacím rámečku **Pokud je aktivní Trusted Platform Module (TPM), tak se nedotazovat na heslo pro pre-boot autentizaci**. Toto nastavení je kompatibilní s koncovými body Windows s TPM a UEFI.

Jakmile je zapnuta volba **Pokud je Trusted Platform Module (TPM) aktivní, tak se nedotazovat na heslo před spuštěním (pre-boot password)**:

- V nezašifrovaném koncovém bodě:

  - Šifrování probíhá bez vyžadování hesla.
  - Autentizační obrazovka před spuštěním se při zapnutí stroje nezobrazí.
- Koncový bod šifrovaný s heslem:
  - Heslo je odebráno.
  - Svazky zůstanou šifrované.
- Šifrovaný nebo nešifrovaný koncový bod, s nenalezeným nebo nefungujícím TPM:
  - Uživatel je vyzván k zadání hesla pro šifrování.
  - Při zapnutí stroje se zobrazí autentizační obrazovka před spuštěním.

Jakmile je vypnuta volba **Pokud je Trusted Platform Module (TPM) aktivní, tak se nedotazovat na heslo před spuštěním (pre-boot password)**:

- Uživatel musí zadat heslo pro šifrování.
- Svazky zůstanou šifrované.

Na Mac

Chcete-li spustit šifrování na spouštěcích svazcích, agent zabezpečení vyzve uživatele, aby zadali své systémové přístupy. Šifrování mohou povolit pouze uživatelé, kteří mají místní účty s oprávněními správce.

Chcete-li spustit šifrování na nespouštěcích svazcích (non-boot volumes), agent zabezpečení vyzve uživatele, aby si nastavili své heslo pro šifrování. Toto heslo bude potřeba k odemčení nespouštěcího svazku pokaždé když se počítač spustí. Pokud má počítač více jak jeden nespouštěcí svazek, tak si uživatel musí nastavit šifrovací heslo pro každý z nich.

Dešifrování svazků

Pro dešifrování svazků na koncových bodech:

1. Zaškrtněte políčko **Správa šifrování**.
2. Vyberte možnost **Dešifrovat**.

Dešifrovací proces začne, jakmile je pravidlo aktivováno na koncových bodech, s určitými zvláštnostmi pro Windows a Mac.

Na Windows

Svazky jsou dešifrovány bez interakce uživatelů.

Na Mac

Pro spouštěcí svazky musí uživatelé zadat své přihlašovací údaje do systému. U svazků, které nejsou spouštěny, musí uživatelé zadat heslo nakonfigurované během procesu šifrování.

V případě, že uživatelé zapomenou svá šifrovací hesla, budou potřebovat klíče pro obnovu pro odemčení jejich zařízení. Pro detaily ohledně získání klíčů pro obnovu se obraťte na „“ (str. 103).

S výjimkou oddílů

Seznam vyloučení z šifrování můžete vytvořit přidáním konkrétních písmen jednotek, štítků a názvů oddílů a GUID oddílů. Vytvoření pravidla pro vyloučení diskových oddílů ze šifrování:

1. Zaškrtněte políčko **Vyloučení** .
2. Klikněte na **Typ** a z rozbalovací nabídky vyberte typ jednotky.
3. Do pole **Vyloučené položky** zadejte hodnotu jednotky a zvažte následující podmínky:
   - Pro **písmeno jednotky** zadejte `D:` nebo písmeno vaší jednotky následované dvojtečkou.
   - Pro **Štítek/Název** můžete zadat libovolný štítek, například `Práce` .
   - Pro oddíl **GUID** zadejte hodnotu následovně: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.
4. Kliknutím na **Přidat** ⊕ přidáte vyloučení do seznamu.

Chcete-li vyloučení odstranit, vyberte a položku a klikněte na **Odstranit** ⊗.

7.2.13. NSX

V této sekci můžete ustanovit politiku, aby byla použita jako bezpečnostní profil ve NSX. K tomu, aby jste to provedli:

1. Vyberte zaškrtávací pole **NSX** aby se zobrazoval i ve vSphere Web Client.
2. Zadejte název pomocí kterého budete schopní identifikovat politiku v NSX. Tento název by měl být jiný než název politiky v GravityZone Control Center. Ve vSphere se zobrazí předpona před `Bitdefender_` . Tento název vyberte s rozvahou, protože se stane pouze read-only po uložení politiky.

7.2.14. Ochrana Úložiště

Poznámka
Ochrana úložiště je dostupná pro síťová úložiště (NAS devices) a řešení pro sdílení souborů (file-sharing solutions) kompatibilních s Internet Content Adaptation Protokolem (ICAP).

V této části můžete nakonfigurovat Security Servery jako skenovací službu pro zařízení NAS a řešení pro sdílení souborů kompatibilní s ICAP, jako jsou Nutanix a Citrix ShareFile.

Security Server skenuje jakýkoliv soubor, včetně archivů, kdykoliv je požadováno z úložného zařízení. Security Servery provádějí adekvátní úlohy podle jejich příslušných nastevní s infikovanými soubory, jako jsou například vyléčení souboru nebo zamezení přístupu k souboru.

Nastavení jsou uspořádána do následujících sekcí:

- ICAP
- Výjimky

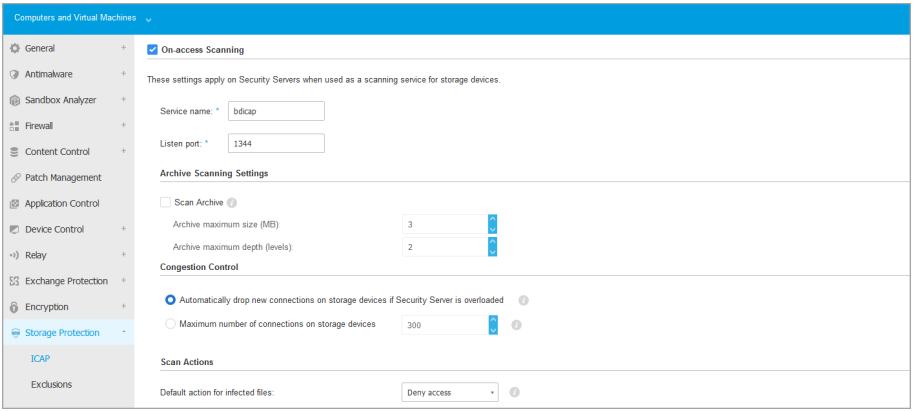
ICAP

Můžete konfigurovat následující volby pro Security Servery:

- Vyberte označovací rámeček volby **Skenování při přístupu (On-access Scanning)** pokud chcete zapnout modul pro ochranu úložišť (Storage Protection module). Požadované nastavení pro komunikaci mezi Security Servery a zařízeními úložišť jsou předdefinovány následovně:
  - Název služby(Service name): `bdicap`.
  - Port na kterém poslouchá (Listen port): `1344`.
- Pod **Nastavení skenování Archivů (Archive Scanning Settings)**, vyberte zatržítko **Skenovat archivy (Scan Archive)** pro zapnutí skenování archivů. Nastavte si maximální velikost a maximální hloubku pro archivy, které mají být skenovány.

  Poznámka
  Pokud nastavíte hodnotu maximální velikosti archivu (archive maximum size) na 0 (nulu),tak Security Server bude skenovat archivy nehledě jejich velikosti.

- Vyberte pod **Kontrola přetížení (Congestion Control)**, preferovanou metodu pro správu připojení na úložných zařízeních (storage devices) v případě že by byl Security Server přetížen:
  - **Automaticky přerušte nová spojení na úložných zařízeních pokud je Security Server přetížen**. Jamile dosáhne jeden Security Server maximální číslo spojení, tak úložné zařízení (storage device) přesměruje přebytečný provoz na druhý Security Server.
  - **Maximální počet spojení na úložném zařízení**. Standartní hodnota je na 300 spojeních.
- Pod **Skenovací úlohy (Scan Actions)** jsou dostupné následující možnosti:
  - **Odepřít přístup (Deny access)** – Security Server odpeře přístup k infikovanému souboru.
  - **Vyléčit (Disinfect)** – Security Server odebere škodlivý (malware) kód z infikovaného souboru.



Politiky - Ochrany Úložišť (Storage Protection) - ICAP

Výjimky

Pokud si přejete specifické objekty aby byly vyjmuty ze skenování, tak si zvolte možnost **Vyjímky (Exclusions)** zatržítkem.

Můžete definovat vyjímky:

- Podle hashe (By hash) – můžete identifikovat vybraný soubor (pro vyjímku) podle toho jaký má SHA-256 hash.
- Podle divoké karty (By wildcard) – můžete identifikovat vyjmutý soubor podle cesty.

Konfigurace vyjímek

Pro přidání výjimky:

1. Z nabídky zvolte typ výjimky.
2. Na základě typu výjimky určete objekt, který má být vyloučen, následujícím způsobem:
   - **Hash** – vložte SHA-256 hashe oddělené čárkou.
   - **Wildcard** – vyspecifikujte si absolutní nebo relativní jméno cesty užitím znaků divoké karty (wildcard characters). Symbol hvězdičky (*) spojí všechny soubory v rámci adresáře. Otazník (?) zastupuje přesně jeden znak.
3. Přidejte popis k vyjímce.
4. Klikněte na tlačítko ⊕ **Přidat**. Nové vyjímky budou vloženy do seznamu.

Pro odstranění pravidla ze seznamu klikněte na odpovídající tlačítko ⊗ **Odstranit**.

Importování a exportování výjimek

Pokud hodláte použít vjímky ve vícero politikách, tak si můžete vybrat je exportovat a importovat.

Pro export vyjímek:

1. Klikněte na **Exportovat** v horní části tabulky výjimek.
2. Uložte soubor CSV na váš počítač. V závislosti na nastavení vašeho prohlížeče se soubor může stáhnout automaticky, nebo budete vyzváni k jeho uložení do nějakého umístění.

Každý řádek v CSV souboru odpovídá jedné vyjímce, přičemž ná pole v následujícím pořadí:

```
<exclusion type>, <object to be excluded>, <description>
```

Toto jsou dostupné hodnoty v polích CSV:

Typ výjimky:

`1`, pro SHA-256 hash

`2`, pro divokou kartu (wildcard)

Objekt, který má být vyloučen:

Hodnota hashe nebo jméno cesty

Popis

Popis za účelem pomoci identifikovat vyjímku.

Příklady vyjímek v CSV souboru:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

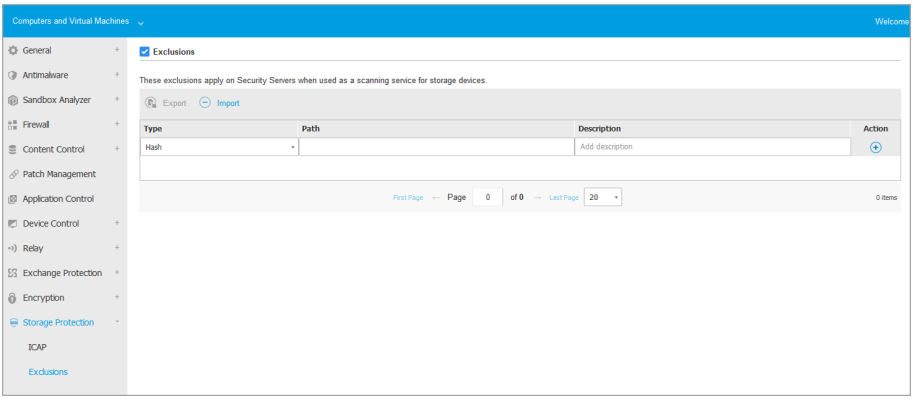
Pro import vyjímek:

1. Klikněte na **Importovat**. Zobrazí se okno **Importovat Výjimky pravidel**.
2. Klikněte na **Přidat** a poté vyberte soubor CSV.
3. Klikněte na tlačítko **Save**. Tabulka je vyplněna platnými vyjímkami. Pokud obsahuje CSV soubor neplatné vyjímky tak se vám zobrazí upozornění s korespondujícími čísly řad, kde se neplatné vyjímky nacházejí.

Editace vyjímek

Pro editaci vyjímky:

1. Klikněte na název vyjímky v sloupci **Cesta (Path)** a nebo v popisu.
2. Editujte vyjímku.
3. Zmáčkěte `Enter` pro ukončení.

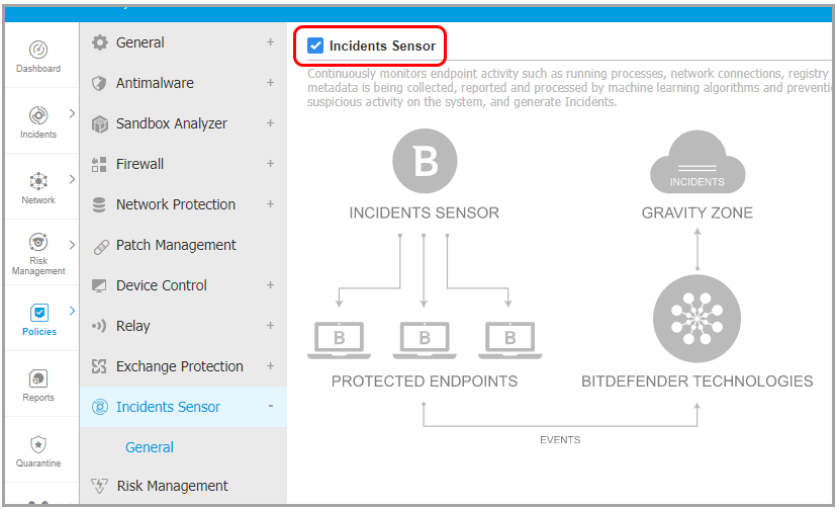


Politiky - Ochrany Úložišť (Storage Protection) - ICAP

7.2.15. Senzor incidentů

Senzor Incident nepřetržitě sleduje činnost koncového bodu, jako jsou spuštěné procesy, síťová připojení, změny registru a chování uživatelů. Tato metadata jsou shromažďována, vykazována a zpracovávána pomocí algoritmů strojového učení a technologií prevence, které detekují podezřelou aktivitu v systému a generují incidenty.

Zaškrtněte políčko Incident Sensor, abyste tento modul povolili.



Senzor incidentů

7.3. Politiky Mobilních Zařízení

Nastavení pravidel může být nastaveno na začátku jejich tvorby. Později je můžete změnit podle svých potřeb.

Pro nastavení parametrů pravidla:

1. Jděte na záložku **Práva**
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Klikněte na název pravidla. Toto otevře stránku nastavení pravidel.
4. Nakonfigurujte nastavení pravidla dle potřeby. Nastavení jsou organizována do následujících kategorií:
   - Hlavní
     - Podrobnosti
   - Správa Zařízení
     - Zabezpečení
     - Heslo
     - Profily

   Můžete vybrat kategorii nastavení pomocí menu na levé straně stránky.

5. Klikněte na **Save** pro uložení změn a aplikování jich na cílová mobilní zařízení. Pro opuštění stránky pravidel bez uložení změn klikněte na **Zrušit**.

7.3.1. Hlavní

Kategorie **General** obsahuje vysvětlující informace ohledně vybrané politiky.

Podrobnosti

Stránka Detaily ukazuje hlavní detaily politiky:

- Název politiky
- Uživatel, který pravidlo vytvořil
- Datum a čas, kdy bylo pravidlo vytvořeno
- Datum a čas, kdy bylo právo naposledy upraveno

Můžete přejmenovat politiku zadáním nového názvu v příslušném poli. Pravidla by měla mít definující jména, aby jste je vy nebo jiný administrátor mohli snadno rozpoznat.

Poznámka
Ve výchozím nastavení může pravidla upravovat pouze uživatel, který je vytvořil. Pro změnu tohoto nastavení musí autor pravidla označit možnost **Povolit ostatním uživatelům měnit toto pravidlo** ze stránky **Podrobnosti** pravidla.

7.3.2. Správa Zařízení

Nastavení správy zařízení umožňuje definování bezpečnostních možností pro mobilní zařízení, uzamykání obrazovky pomocí hesla a také několik profilů pro každou politiku mobilních zařízení.

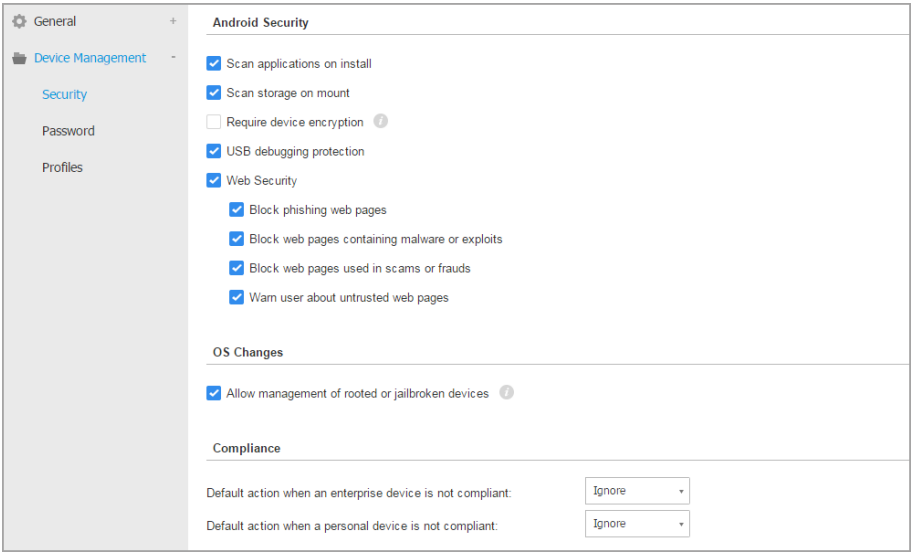
Nastavení jsou uspořádána do následujících sekcí:

- Zabezpečení
- Heslo
- Profily

Zabezpečení

V této sekci můžete nastavit rozdílná bezpečnostní nastavení pro mobilní zařízení, zahrnující antimalware scan pro Android, správa rootnutých a jailbrokenutých zařízení nebo akce na nevyhovujících zařízeních.

Důležité
Antimalwarové skenování probíhá v cloudu, tím pádem musí být mobilní zařízení připojena k internetu.



Pravidla pro Mobilní zařízení - Bezpečnostní nastavení

Ochrana pro Android

- Zvolte **Skenování aplikací při instalaci**, pokud chcete provádět skenování při instalaci nových aplikací na spravovaná zařízení.
- Zvolte **Skenování paměti při namontování**, pokud chcete provést sken každého paměťového zařízení, když je montováno.

Varování
Pokud je nalezen malware, uživatel je vyzván k jeho odstranění. Pokud uživatel neodstraní nalezený malware do jedné hodiny po jeho detekci, mobilní zařízení bude označeno jako v nesouladu a bude uplatněna zvolená akce pro nesoulad (Ignorovat, Zakázat přístup, Uzamknout, Vymazání nebo Odpojit).

- Zvolte **Vyžadovat šifrování zařízení** pro vyzvání uživatele k aktivaci funkce šifrování, dostupné v operačním systému Android. Šifrování chrání data uložená

na zařízeních Android, včetně účtů, nastavení, stažených aplikací, médií a dalších souborů před neoprávněným přístupem. K šifrovaným datům lze přistupovat z externích zařízení pouze po zadání hesla pro odemčení.

Důležité

- Šifrování zařízení je dostupné pro Android 3.0 a novější. Ne všechny modely zařízení podporují šifrování. Podívejte se na okno **Detaily mobilního zařízení** pro informace o podpoře šifrování.
- Šifrování může ovlivnit výkon zařízení.

Varování

- Šifrování zařízení je nevratné a jediný způsob, jak ho vrátit zpět do původního stavu, je vymazat obsah zařízení.
- Před aktivací šifrování zařízení by uživatelé měli zálohovat svá data.
- Uživatelé nesmí přerušit šifrovací proces, nebo částečně či úplně přijdou o svá data.

Pokud povolíte tuto možnost, GravityZone Mobile Client bude zobrazovat přetrvávající upozornění informující uživatele o tom, že má aktivovat šifrování. Uživatel musí kliknout na tlačítko **Vyřešit** pro pokračování na šifrovací obrazovku a pro zahájení procesu. Pokud šifrování není aktivováno během sedmi dní po upozornění, zařízení se stane nevyhovujícím.

Pro povolení šifrování na zařízení Android:

- Baterie musí být nabitá na více než 80%.
- Zařízení musí být připojeno, dokud se šifrování nedokončí.
- Uživatel musí nastavit odemykací heslo, jehož složitost odpovídá požadavkům.

Poznámka

- Zařízení Android používají to samé heslo pro odemykání obrazovky a pro odemykání šifrovaného obsahu.
- Šifrování vyžaduje heslo, PIN nebo FACE pro odemknutí zařízení, a odepře všechna ostatní nastavení odemykací obrazovky.

Šifrovací proces může trvat hodinu nebo déle, a zařízení se mezitím může několikrát restartovat.

Stav šifrování paměti můžete zkontrolovat pro každé mobilní zařízení v okně **Detaily mobilního zařízení**.

- Zařízení Android v režimu USB debugging mohou být připojena k PC přes USB kabel, což umožní pokročilou kontrolu jejich aplikací a operačního systému. V tomto případě může být bezpečnost mobilních zařízení ohrožena. Ve výchozím stavu povolená, možnost **Ochrana pro USB debugging** zabraňuje používání zařízení v režimu USB debugging. Pokud uživatel spustí USB debugging, zařízení se automaticky stane nevyhovujícím a bude uplatněna akce pro nesoulad. Pokud je akce pro nesoulad **Ignorovat**, uživatel bude upozorněn na nebezpečné nastavení.

  Nicméně, tuto možnost můžete vypnout pro mobilní zařízení, která vyžadují práci v režimu USB debugging (jako jsou mobilní zařízení používaná pro vývoj a testování mobilních aplikací).

- Zvolte **Ochranu webu** pro zapnutí funkcí webové ochrany na zařízeních Android.

  Ochrana webu skenuje v cloudu každou navštívenou URL, a poté odešle zpět stav zabezpečení do GravityZone Mobile Client. Stav zabezpečení URL může být: čisté, podvod, malware, phishing nebo nedůvěryhodné.

  Podle stavu zabezpečení může GravityZone Mobile Client uplatit specifické opatření:

  - **Blokovat phishingové webové stránky**. Když se uživatel pokusí o přístup k phishingové webové stránce, GravityZone Mobile Client zablokuje příslušnou URL, a místo ní zobrazí varovnou stránku.
  - **Blokovat webové stránky obsahující malware nebo exploity**. Když se uživatel pokusí o přístup k webové stránce šířící malware nebo webové exploity, GravityZone Mobile Client zablokuje příslušnou URL, a místo ní zobrazí varovnou stránku.
  - **Blokovat webové stránky používané pro padělání a podvody**. Rozšiřuje ochranu na další typy podvodů kromě phishingu (například escrows, falešné příspěvky, hrozby sociálních médií a tak dále). Když se uživatel pokusí o přístup k podvodné webové stránce, GravityZone Mobile Client zablokuje příslušnou URL, a místo ní zobrazí varovnou stránku.
  - **Varovat uživatele o nedůvěryhodných webových stránkách**. Když uživatel přistupuje na stránku, která byla dříve napadená za phishingovými účely, nebo nedávno propagována prostřednictvím spamu či phishingových emailů, zobrazí se vyskakovací okno s upozorněním, bez blokování webové stránky.

Důležité
Funkcionalita bezpečného prohlížení webů (Web Security) funguje pouze od Android verze 5, a pouze s prohlížečem Chrome a zabudovaným Android prohlížečem.

Změny OS

Protože jsou v podnikových sítích považována za nebezpečná, zařízení s rootem nebo jailbreakem jsou automaticky prohlášena za nevyhovující.

- Vyberte **Povolit správu zařízení s rootem nebo jailbreakem**, pokud chcete z Control Center spravovat zařízení s rootem nebo jailbreakem. Mějte na paměti, že protože jsou tato zařízení ve výchozím stavu nevyhovující, je na nich okamžitě po jejich nalezení uplatněno opatření pro zařízení v nesouladu. Proto, abyste na ně mohli aplikovat nastavení bezpečnostních zásad nebo na nich spouštět úlohy, musíte nastavit akci pro nesoulad na Ignorovat.
- Pokud zrušíte označení pole **Povolit správu zařízení s rootem nebo jailbreakem**, automaticky tím odpojíte zařízení s rootem nebo jailbreakem ze sítě GravityZone. V tomto případě aplikace GravityZone Mobile Client vystaví zprávu s oznámením, že se jedná o zařízení s rootem / jailbreakem. Uživatel může kliknout na tlačítko OK, čímž bude přesměrován na registrační stránku. Jakmile je ze zařízení odstraněn root / jailbreak, nebo je pravidlo přenastaveno na povolení správy zařízení s rootem / jailbreakem, je možné je znovu zapsat (s tím samým tokenem pro zařízení Android / s novým tokenem pro zařízení s iOS).

Soulad

Můžete nastavit specifické akce, které budou automaticky uplatněny na zařízeních, která jsou zjištěna jako nevyhovující, na základě vlastnictví zařízení (podnikové nebo osobní).

Poznámka
Když do Control Center přidáváte nové zařízení, budete vyzváni k určení vlastnictví daného zařízení (podnikové nebo osobní). Díky tomu může GravityZone spravovat zvlášť osobní a podniková mobilní zařízení.

- Kritéria pro nesoulad
- Opatření pro nesoulad

Kritéria pro nesoulad

Zařízení je prohlášeno za nevyhovující v následujících situacích:

- **Zařízení Android**
  - Zařízení je rootované.
  - GravityZone Mobile Client není Správcem zařízení.
  - Malware není odstraněn do jedné hodiny po detekci.
  - Pravidlo není naplněno:
    - Uživatel nenastaví heslo zamykací obrazovky do 24 hodin po prvním upozornění.
    - Uživatel nezmění heslo zamykací obrazovky v určený čas.
    - Uživatel neaktivuje šifrování zařízení do sedmi dní po prvním upozornění.
    - Režim USB debugging je aktivován na zařízení, když je povolená možnost pravidla ochrany USB debuggingu.
- **iOS zařízení**
  - Zařízení je jailbreaknuté.
  - GravityZone Mobile Client je odinstalovaný z mobilního zařízení.
  - Pravidlo není naplněno:
    - Uživatel nenastaví heslo zamykací obrazovky do 24 hodin po prvním upozornění.
    - Uživatel nezmění heslo zamykací obrazovky v určený čas.

Výchozí akce, když je zařízení nevyhovující

Když je zařízení prohlášeno za nevyhovující, uživatel je vyzván k nápravě problému, který působí nesoulad. Uživatel musí provést nutné změny během určené doby, nebo bude uplatněna zvolená akce pro nevyhovující zařízení (Ignorovat, Odepřít přístup, Uzamknout, Vymazání nebo Odpojit).

Akci pro nevyhovující zařízení můžete kdykoli změnit v zásadách. Nová akce je aplikována na nevyhovující zařízení po uložení pravidla.

Z nabídky odpovídající každému typu vlastnictví zařízení vyberte akci, která má být uplatněna v případě nesouladu zařízení:

- **Ignorovat**. Pouze upozorní uživatele na to, že zařízení nevyhovuje pravidlu užívání mobilních zařízení.
- **Odepřít přístup**. Blokuje přístup zařízení k podnikovým sítím tak, že vymaže všechna nastavení Wi-Fi a VPN, ale ponechá všechna ostatní nastavení určená v pravidle. Blokovaná nastavení jsou obnovena, jakmile je zařízení opět v souladu.

  Důležité
  Když je pro GravityZone Mobile Client zakázán Správce zařízení, zařízení se stane nevyhovujícím a je automaticky aplikována akce **Odepřít přístup**.

- **Zamknout**. Okamžitě uzamkne zamykací obrazovku.
  - Na Android je obrazovka uzamčena heslem vygenerovaným v GravityZone pouze v případě, že na zařízení není nastavena žádná ochrana zámku. Tímto se nepřepíše již dříve nastavená možnost zamykací obrazovky, jako je vzor, PIN, heslo, otisk prstu nebo Smart Lock.
  - Na iOS, pokud má zařízení nastavený zámek obrazovky, je vyžadován pro jeho odemčení.
- **Vymazání**. Obnoví tovární nastavení mobilního zařízení a trvale odstraní všechna uživatelská data.

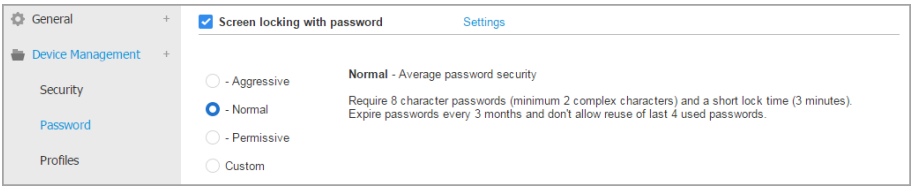
  Poznámka
  Vymazání v tuto chvíli neodstraňuje i data z přídatných zařízení (paměťových karet).

- **Odpojit**. Zařízení je okamžitě odstraněno ze sítě.

  Poznámka
  Pro opětovné připojení zařízení, na které byla aplikována akce Odpojit, musíte zařízení znovu přidat v Kontrolním centru. Zařízení musí být opětovně zaregistrováno s novým aktivačním tokenem. Před opětovným připojením zařízení se ujistěte, že podmínky vedoucí k odpojení zařízení již nejsou naplňovány, nebo změňte nastavení pravidel tak, aby umožňovaly správu zařízení.

Heslo

V této sekci můžete zvolit aktivování funkce zámku obrazovky s heslem, k dispozici v OS mobilních zařízení.



Pravidla pro Mobilní zařízení - Nastavení ochrany heslem

Jakmile je tato funkce zapnutá, upozornění na obrazovce vyzve uživatele k zadání hesla zámku obrazovky. Uživatel musí zadat takové heslo, které naplňuje podmínky pro hesla definované v pravidle. Jakmile uživatel nastaví heslo, všechna upozornění týkající se tohoto problému jsou odstraněna. Zpráva s výzvou pro uživatele k zadání hesla se zobrazí při každém pokusu o odemčení obrazovky.

Poznámka

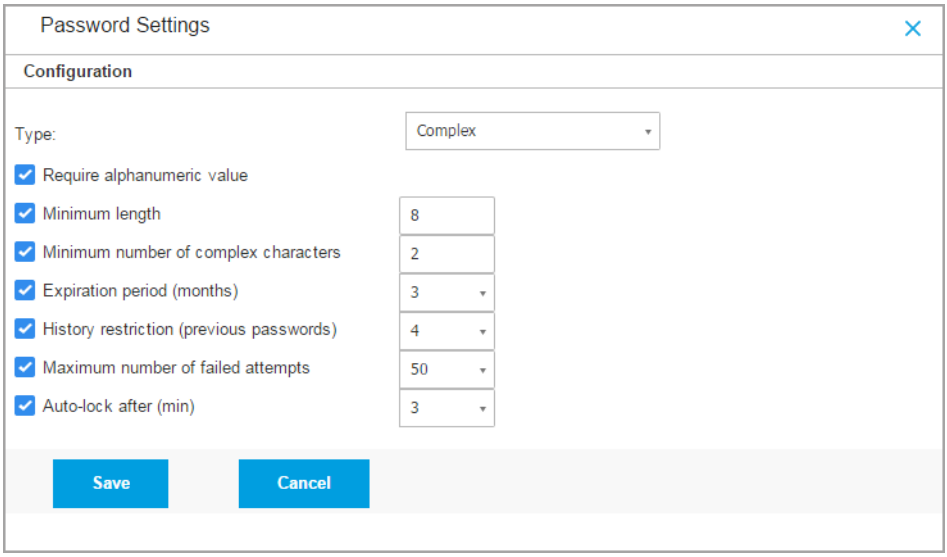
Pokud uživatel poté, co je vyzván, heslo nenastaví, zařízení je možné používat bez zámku obrazovky až do 24 hodin po prvním upozornění. Během této doby se bude na obrazovce každých 15 minut zobrazovat upozornění, vyzývající uživatele k zadání hesla zámku obrazovky.

Varování

Pokud uživatel heslo nenastaví během 24 hodin po prvním upozornění, mobilní zařízení se stane nevyhovujícím a bude uplatněna zvolená akce pro nevyhovující zařízení.

Pro nastavení parametrů hesla zámku obrazovky:

1. Označte pole **Uzamčení obrazovky pomocí hesla**.
2. Zvolte úroveň bezpečnosti hesla, která nejlépe vyhovuje vašim potřebám (agresivní, normální nebo tolerantní). Nastavte svůj výběr pomocí popisu na pravé straně stupnice.
3. Pro pokročilá nastavení zvolte **Vlastní** úroveň zabezpečení a poté klikněte na odkaz **Nastavení**.



Pravidla pro Mobilní zařízení - Pokročilá nastavení ochrany heslem

Poznámka

Pro zobrazení požadavků pro nastavení hesla na přednastavené úrovni ochrany vyberte danou úroveň a klikněte na odkaz **Nastavení**. Když upravíte kteroukoli z možností, úroveň bezpečnosti hesla se automaticky změní na **Vlastní**.

Uživatelské ovládací prvky.

- **Typ**. Můžete po heslu požadovat, aby bylo Jednoduché nebo Složité. Kritéria pro složitost hesla jsou určena v rámci operačního systému zařízení.
  - Na zařízeních Android musí složitá hesla obsahovat alespoň jedno písmeno, jednu číslovku a jeden zvláštní znak.

    Poznámka
    Složitá hesla jsou podporována na Androidu 3.0 a novějších.

  - Na zařízeních s iOS, složitá hesla nepovolují následující se nebo opakované znaky (jako jsou abcdef, 12345 nebo aaaaa, 11111).

V závislosti na zvolené možnosti, poté, co uživatel nastaví heslo zámku obrazovky, operační systém zkontroluje a upozorní uživatele, pokud nejsou naplněna požadovaná kritéria.

- **Požadovat alfanumerickou hodnotu**. Požadovat po heslu, aby obsahovalo písmena i číslice.
- **Minimální délka**. Požadovat od hesla minimální počet znaků, který určíte v odpovídajícím poli.
- **Minimální počet komplexních znaků**. Požadovat od hesla minimální počet nealfanumerických znaků (jako je @, # nebo $), které určíte v odpovídajícím poli.
- **Doba do vypršení platnosti (měsíce)**. Přimějte uživatele, aby změnil heslo zámku obrazovky v určené době (v měsících). Například, když zadáte 3, uživatel bude vyzýván ke změně hesla zámku obrazovky každé tři měsíce.

  Poznámka
  Pro Android je tato funkce podporována na verzi 3.0 a novější.

- **Omezení historie (předchozí hesla)**. Zvolte nebo zadejte hodnotu do odpovídajícího pole pro určení počtu minulých hesel, která nemohou být použita opakovaně. Například, pokud zadáte 4, uživatel nemůže znovu použít heslo, které se shoduje s jedním z naposledy použitých čtyř hesel.

  Poznámka
  Pro Android je tato funkce podporována na verzi 3.0 a novější.

- **Maximální počet nezdařených pokusů**. Určete, kolikrát může uživatel zadat chybné heslo.

  Poznámka
  Na zařízeních s iOS, pokud je toto číslo vyšší než 6: po šesti nezdařených pokusech je na uživatele uvalena časová prodleva předtím, než může znovu zkusit zadat heslo. Časová prodleva se prodlužuje s každým nezdařeným pokusem.

  Varování
  Pokud uživatel překročí maximální počet nezdařených pokusů o odemknutí obrazovky, obsah zařízení bude vymazán (všechna data a nastavení budou odstraněna).

- **Uzamknout automaticky po (min)**. Nastavte dobu nečinnosti (v minutách), po které se zařízení automaticky uzamkne.

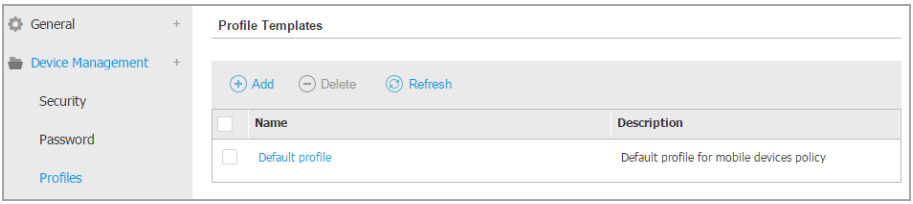
> **Poznámka**
> Zařízení iOS mají přednastavený seznam času pro automatické uzamčení a nepodporují zadávání vlastního času. Když přiřazujete pravidlo s nekompatibilní hodnotou automatického zámku, zařízení prosadí druhý nejvíce omezující časový interval dostupný v seznamu. Například, pokud má pravidlo nastavený automatický zámek na tři minuty, zařízení se automaticky uzamkne po dvou minutách nečinnosti.

Když upravíte pravidlo, nebo vyberete vyšší bezpečnostní úroveň pro heslo zámku obrazovky, uživatele budou vyzváni ke změně hesla v souladu s novými kritérii.

Pokud zrušíte výběr možnosti **Uzamčení obrazovky pomocí hesla**, uživatelé znovu získají plný přístup k nastavení zámku obrazovky na jejich mobilním zařízení. Současné heslo zůstává aktivní, dokud se ho uživatel nerozhodne změnit nebo odstranit.

Profily

V této sekci můžete vytvářet, upravovat a mazat profily užívání pro mobilní zařízení. Profily užívání vám umožňují protlačit nastavení Wi-Fi a VPN a vynutit kontrolu přístupu k webu na spravovaných mobilních zařízeních.



Pravidla pro Mobilní zařízení - Profilové šablony

Můžete nastavit jeden nebo několik profilů, ale v jednu chvíli může být na zařízení aktivní pouze jeden.

- Pokud nastavíte pouze jeden profil, bude tento profil automaticky aplikován na všechna zařízení, ke kterým je pravidlo přiřazeno.
- Pokud nastavíte několik profilů, bude na všechna zařízení, ke kterým je pravidlo přiřazeno, aplikován první profil ze seznamu.

Uživatelé mobilních zařízení mohou prohlížet přiřazené profily a parametry nastavené pro každý z profilů v aplikaci GravityZone Mobile Client. Uživatelé nemohou upravovat existující nastavení profilu, ale mohou přepínat mezi profily, pokud je jich k dispozici několik.

Poznámka
Přepínání profilů vyžaduje připojení k internetu.

Pro vytvoření nového profilu:

1. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky. Zobrazí se stránka nastavení profilů.
2. Nakonfigurujte nastavení profilu dle potřeby. Pro podrobné informace se odkažte na:
   - „Podrobnosti“ (str. 393)
   - „Sítě“ (str. 393)
   - „Přístup k webu“ (str. 397)
3. Klikněte na tlačítko **Save**. Nový profil bude přidán do seznamu.

Pro odstranění jednoho nebo několika profilů označte jejich příslušná pole a klikněte na tlačítko ⊖ **Odstranit** po pravé straně tabulky.

Pro úpravu profilu klikněte na jeho jméno, změňte nastavení dle potřeby a klikněte na **Uložit**.

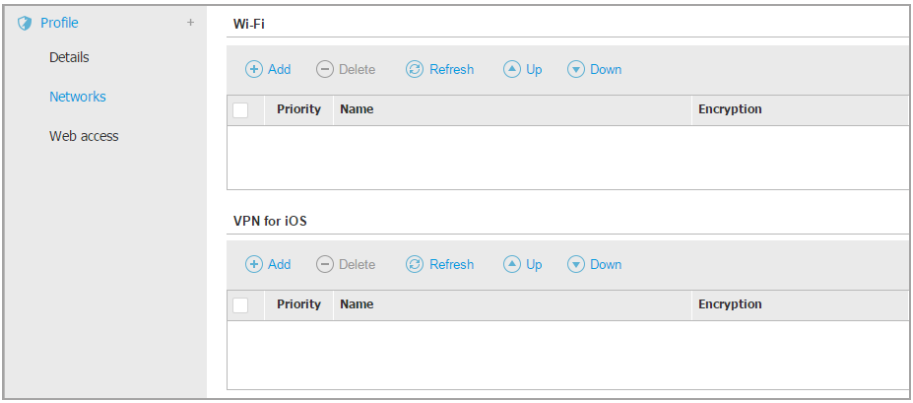
Podrobnosti

Stránka **Detaily** obsahuje obecné informace ohledně profilu:

- **Jméno**. Zadejte požadované jméno profilu. Profily by měly mít definující jména, aby jste je vy nebo jiný administrátor mohli snadno rozpoznat.
- **Popis**. Zadejte podrobný popis profilu. Tato možnost může pomoci administrátorům ve snadném rozpoznání jednoho profilu od ostatních.

Sítě

V této sekci můžete nastavit parametry jedné nebo několika sítí Wi-Fi a VPN. Nastavení VPN je dostupné pouze pro zařízení iOS.



Pravidla pro Mobilní zařízení - Profilová nastavení připojení k síti

Důležité
Před definováním připojení Wi-Fi a VPN se ujistěte, že máte všechny potřebné informace po ruce (hesla, nastavení proxy atd).

Mobilní zařízení, ke kterým je přiřazený příslušný profil, se budou automaticky připojovat k určené síti, kdykoliv je v dosahu. Při tvorbě několika sítí jim můžete nastavit prioritu, přičemž mějte na paměti, že v jednu chvíli může být použita pouze jedna síť. Když je první síť nedostupná, mobilní zařízení se připojí k druhé, a tak dále.

Pro nastavení priority sítí:

1. Označte pole požadované sítě.
2. Použijte prioritní tlačítka na pravé straně tabulky:
   - Klikněte na tlačítko **Nahoru** pro povýšení zvolené sítě.
   - Kliknutím na tlačítko **Dolů** ji posunete dolů.

- **WiFi**

  Můžete přidat tolik sítí Wi-Fi, kolik potřebujete. Pro přidání sítě Wi-Fi:

  1. V sekci **Wi-Fi** klikněte na tlačítko **Přidat** po pravé straně tabulky. Zobrazí se konfigurační okno.
  2. Pod kartou **Obecné** můžete nastavit podrobnosti Wi-Fi připojení:
     - **Jméno (SSID)**. Zadejte název sítě Wi-Fi.

- **Zabezpečení**. Vyberte možnost odpovídající úrovni zabezpečení sítě Wi-Fi:
  - **Žádné**. Vyberte tuto možnost, když je Wi-Fi připojení veřejné (nevyžaduje žádné přihlašovací údaje).
  - **WEP**. Vyberte tuto možnost pro nastavení připojení Wireless Encryption Protocol (WEP). Zadejte heslo požadované pro tento typ připojení do odpovídajícího pole, zobrazeného níže.
  - **WPA/WPA2 Osobní**. Vyberte tuto možnost, pokud je síť Wi-Fi zabezpečena pomocí Wi-Fi Protected Access (WPA). Zadejte heslo požadované pro tento typ připojení do odpovídajícího pole, zobrazeného níže.

3. Pod **TCP/IP** můžete nastavit parametry TCP/IP pro Wi-Fi připojení. Každé Wi-Fi připojení může používat IPv4 nebo IPv6 nebo oboje.
   - **Nastavit IPv4**. Pokud chcete používat metodu IPv4, zvolte metodu přiřazení IP z příslušné nabídky:

     DHCP: pokud je IP adresa přiřazena automaticky DHCP serverem. Pokud je třeba, zadejte do navazujícího pole DHCP Client ID.

     Zakázané: vyberte tuto možnost, pokud nechcete používat protokol IPv4.
   - **Nastavit IPv6**. Pokud chcete používat metodu IPv6, zvolte metodu přiřazení IP z příslušné nabídky:

     DHCP: pokud je IP adresa přiřazena automaticky DHCP serverem.

     Zakázané: vyberte tuto možnost, pokud nechcete používat protokol IPv6.
   - **DNS Servery**. Zadejte adresu alespoň jednoho DNS serveru pro síť.
4. Pod kartou **Proxy** nastavte parametry proxy pro Wi-Fi připojení. Vyberte požadovaný způsob nastavení proxy v nabídce **Typ**:
   - **Vypnuto**. Vyberte tuto možnost, pokud síť Wi-Fi nemá žádná nastavení proxy.
   - **Ruční**. Vyberte tuto možnost pro ruční nastavení parametrů proxy. Zadejte jméno hostitele proxy serveru a port, ze kterého hledá připojení. Pokud proxy server požaduje autentizaci, označte pole **Autentizace** a do příslušných polí zadejte uživatelské jméno a heslo.

- **Automatické**. Vyberte tuto možnost pro načtení nastavení proxy ze souboru Proxy Auto-Configuration (PAC), vydaného místní sítí. Zadejte adresu PAC souboru do pole **URL**.

5. Klikněte na tlačítko **Save**. Nové Wi-Fi připojení je přidáno do seznamu.

- **VPN pro iOS**

  Můžete přidat tolik VPN, kolik potřebujete. Pro přidání VPN:

  1. V sekci **VPN pro iOS** klikněte na tlačítko ⊕ **Přidat** po pravé straně tabulky. Zobrazí se konfigurační okno.
  2. V okně **Připojení VPN** určete nastavení VPN:

     Obecné:

     - **Jméno**. Zadejte název VPN připojení.
     - **Šifrování**. Dostupný autentizační protokol pro tento typ připojení je **IPSec**, který vyžaduje autentizaci uživatele prostřednictvím hesla a strojovou autentizaci pomocí sdíleného tajemství.
     - **Server**. Zadejte adresu VPN serveru.
     - **Uživatel**. Zadejte pro VPN uživatelské jméno.
     - **Heslo**. Zadejte heslo pro VPN.
     - **Jméno skupiny**. Zadejte jméno skupiny.
     - **Tajemství**. Zadejte předsdílený klíč.

     Proxy:

     V této sekci můžete nastavit parametry proxy pro VPN připojení. Vyberte požadovaný způsob nastavení proxy v nabídce **Typ**:

     - **Vypnuto**. Vyberte tuto možnost, pokud připojení VPN nemá žádná nastavení proxy.
     - **Ruční**. Tato možnost vám umožňuje provést ruční nastavení parametrů proxy.
       - **Server**: zadejte název hostitele proxy serveru.
       - **Port**: zadejte číslo proxy portu.
       - Pokud proxy server požaduje autentizaci, označte pole **Autentizace** a do příslušných polí zadejte uživatelské jméno a heslo.

– **Automatické**. Vyberte tuto možnost pro načtení nastavení proxy ze souboru Proxy Auto-Configuration (PAC), vydaného místní sítí. Zadejte adresu PAC souboru do pole **URL**.

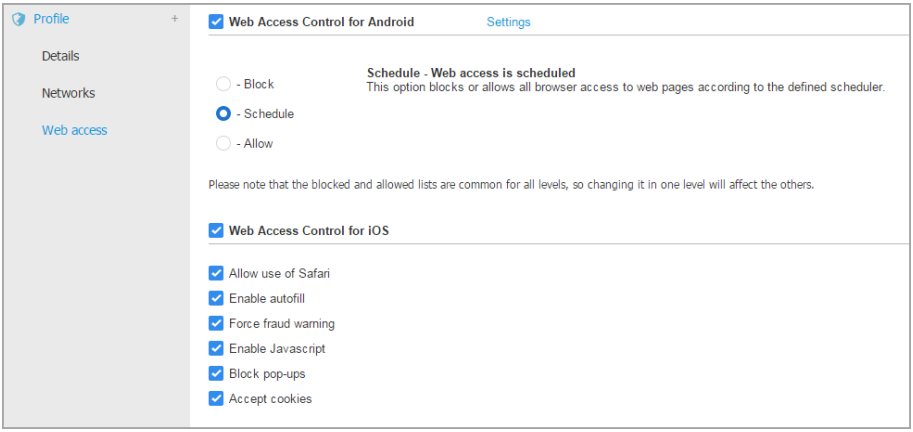
3. Klikněte na tlačítko **Save**. Nové VPN připojení je přidáno do seznamu.

Pro odstranění jedné nebo několika sítí označte jejich příslušná pole a klikněte na tlačítko ⊖ **Odstranit** po pravé straně tabulky.

Pro úpravu sítě klikněte na její jméno, změňte nastavení dle potřeby a klikněte na **Uložit**.

Přístup k webu

V této sekci můžete nastavit kontrolu přístupu k webu pro zařízení Android a iOS.



Pravidla pro Mobilní zařízení - Profilová nastavení přístupu k webu

- **Kontrola přístupu k webu pro Android.** Zapněte tuhle volbu pro filtrování webového přístupu pro Chrome a zabudovaný prohlížeč v Androidu. Můžete na přístup k síti nastavit časová omezení a také výslovně povolit či zakázat přístup ke konkrétním webovým stránkám. Webové stránky blokované Kontrolou přístupu k webu se v prohlížeči nezobrazují. Místo nich se zobrazí výchozí webová stránka, která informuje uživatele, že požadovaná stránka byla zablokována Kontrolou přístupu k webu.

Důležité
Funkcionalita bezpečného přístupu na web (Web Access Security) funguje pouze od Android verze 5, a pouze s prohlížečem Chrome a zabudovaným Android prohlížečem.

Máte tři možnosti konfigurace:

- Vyberte **povolit** pro povolení přístupu k webu pokaždé.
- Vyberte **Blokovat** pro zakázání přístupu k webu pokaždé.
- Vyberte **Plánovač** pro povolení časových omezení při přístupu k webu podle podrobného časového rozvrhu.

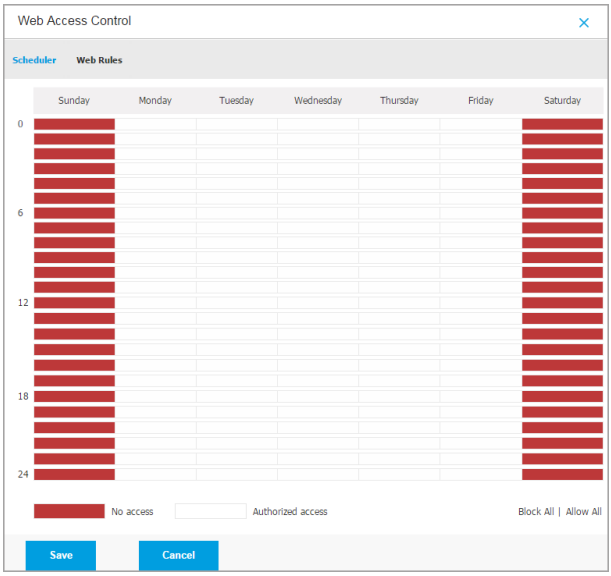
Pokud si vyberete buď povolení nebo blokování přístupu k webu, můžete určit výjimky pro tyto akce, platící pro celé webové kategorie, nebo pouze pro určité webové adresy. Klikněte na **Nastavení** pro konfiguraci vašeho plánu přístupu k webu a výjimek následovně:

Plánovač

Pro omezení přístupu k internetu v určitých denních dobách nebo každý týden:

1. Z mřížky vyberte časové intervaly, během kterých má být přístup blokován.

   Můžete kliknout na jednotlivé buňky nebo můžete kliknout a táhnout pro větší rozmezí. Pro navrácení výběru klikněte znovu do buňky.



Pravidla pro Mobilní zařízení - Plánovač přístupu k webu

Nový výběr začnete kliknutím na **Povolit vše** nebo **Blokovat vše** podle toho, který typ omezení chcete zavést.

2. Klikněte na tlačítko **Save**.

Síťová pravidla

Můžete také definovat síťová pravidla pro výslovné blokování nebo povolení určitých webových adres, a přepsat tak existující nastavení Kontroly přístupu k webu. Například, uživatelé budou mít přístup k určité webové stránce i v případě, že je prohlížení internetu blokováno Kontrolou přístupu k webu.

Pro vytvoření síťového pravidla:

1. Vyberte **Používat výjimky** pro povolení síťových výjimek.
2. Zadejte požadovanou adresu, kterou chcete povolit nebo blokovat, do pole **Webová adresa**.
3. Z nabídky **Povolení** zvolte **Povolit** nebo **Blokovat**.
4. Klikněte na tlačítko ⊕ **Přidat** na pravé straně tabulky pro přidání adresy na seznam výjimek.

5. Klikněte na tlačítko **Save**.

Pro úpravu síťového pravidla:

1. Klikněte na webovou adresu, kterou chcete upravit.
2. Upravte stávající URL.
3. Klikněte na tlačítko **Save**.

Pro odstranění síťového pravidla:

1. Přesuňte kurzor nad webovou adresu, kterou chcete odstranit.
2. Klikněte na tlačítko ⊗ **Odstranit**.
3. Klikněte na tlačítko **Save**.

Použijte zástupné znaky pro určení vzorů webových adres:

– Hvězdička (*) zastupuje nula nebo více znaků.
– Otazník (?) zastupuje přesně jeden znak. Můžete použít několik otazníků pro určení jakékoli kombinace konkrétního počtu znaků. Například, ??? nahrazuje jakoukoli kombinaci přesně tří znaků.

V následující tabulce můžete nalézt několik příkladových syntaxí pro specifikaci webových adres.

Syntax	Použitelnost
`www.example*`	Každá webová stránka, začínající `www.example` (nehledě na koncovku domény). Pravidlo nebude platit pro subdomény specifikované webové stránky, jako je `subdomain.example.com`.
`*example.com`	Jakákoli webová stránka končící na `example.com`, včetně jejich subdomén.
`*řetězec*`	Jakákoli webová stránka, jejíž adresa obsahuje určený řetězec.
`*.com`	Jakákoli webová stránka, která má doménovou koncovku `.com`, včetně dalších jejích stránek a subdomén. Použijte tuto syntaxi pro vynechání všech domén na nejvyšší úrovni ze skenování.

Syntax	Použitelnost
`www.example?.com`	Jakákoli webová adresa začínající na `www.example?.com`, kde ? může být nahrazeno libovolným samostatným znakem. Takové webové stránky mohou být: `www.example1.com` nebo `www.exampleA.com`.

- **Kontrola přístupu k webu pro iOS.** Povolte tuto možnost pro centralizovanou správu nastavení vestavěného iOS prohlížeče (Safari). Uživatelé mobilních zařízení již nebudou moci spravovat daná nastavení na svých zařízeních.
  - **Povolit využívání Safari**. Díky této možnosti můžete ovládat využívání prohlížeče Safari na mobilních zařízeních. Vypnutí této možnosti odstraní zástupce Safari z rozhraní systému iOS, a zabrání tak uživatelům v přístupu k internetu pomocí Safari.
  - **Povolit automatické vyplňování**. Zakažte tuto možnost, pokud chcete prohlížeči zabránit v ukládání položek z formulářů, které mohou obsahovat citlivé informace.
  - **Vynutit varování před podvody**. Vyberte tuto možnost, abyste se ujistili, že uživatelé budou vždy varováni při přístupu k podvodným webovým stránkám.
  - **Povolit Javascript**. Zakažte tuto možnost, pokud chcete, aby Safari ignorovalo Javascript na webových stránkách.
  - **Blokovat vyskakovací okna**. Vyberte tuto možnost pro zabránění automatickému otevírání vyskakovacích oken.
  - **Povolit cookies**. Ve výchozím nastavení Safari podporuje cookies. Zakažte tuto možnost, pokud chcete webovým stránkám zabránit v ukládání informací o prohlížení.

  Důležité
  Řízení přístupu na web pro iOS není v systému iOS 13 podporováno.

8. MONITOROVACÍ KONTROLNÍ PANEL

Správná analýza zabezpečení vaší sítě vyžaduje dostupnost dat a korelaci. Centralizované informace o zabezpečení vám umožňují sledovat a zajišťovat dodržování zásad zabezpečení organizace, rychle identifikovat problémy, analyzovat hrozby a chyby zabezpečení.

8.1. Kontrolní panel

Řídicí panel Control Center je přizpůsobitelný vizuální displej poskytující rychlý přehled zabezpečení všech chráněných koncových bodů a stavu sítě.

Portlety kontrolního panelu zobrazují informace o zabezpečení v reálném čase pomocí snadno čitelných grafů, čímž vám umožňují rychlou identifikaci jakýchkoli problémů, které vyžadují vaši pozornost.

Kontrolní panel

O portletech kontrolního panelu potřebujete vědět následující:

- Control Center je vybavena několika přednastavenými portlety kontrolního panelu.
- Každý portlet kontrolního panelu obsahuje na pozadí detailní hlášení, přístupné jedním kliknutím na graf.
- Je několik typů portletů, které obsahují různé informace ohledně vašeho zabezpečení koncových bodů, jako je stav aktualizací, stav malwaru, aktivita firewallu.

> **Poznámka**
> Ve výchozím stavu portlety načítají data pro aktuální den, a na rozdíl od hlášení nemohou být nastaveny pro delší časový úsek, než je jeden měsíc.

- Informace zobrazené prostřednictvím portletů odkazují pouze ke koncovým bodům spadajícím pod váš účet. Můžete uprav cíl a předvolby každého z portletů pomocí příkazu **Upravit portlet**.
- Klikněte na položky v legendě grafu, pokud jsou k dispozici, pro skrytí nebo zobrazení odpovídající proměnné v grafu.
- Portlety jsou zobrazeny ve skupinách po čtyřech. Pro pohyb mezi skupinami portletů použijte svislý posuvník nebo klávesy se šipkami nahoru a dolů.

- Pro několik typů hlášení můžete okamžitě spustit určité úlohy na cílových koncových bodech, aniž byste pro jejich spuštění museli přecházet na stránku **Síť** (například, skenování infikovaných koncových bodů nebo aktualizace koncových bodů). Použijte tlačítko ve spodní části portletu pro přijetí dostupného opatření.

Kontrolní panel je snadno nastavitelný na základě osobních preferencí. Můžete upravit nastavení portletů, přidat doplňkové portlety, odstranit nebo přeuspořádat současné portlety.

8.1.1. Aktualizace údajů v grafeh

Chcete-li zajistit, aby portlet zobrazoval nejnovější informace, klikněte na **Obnovit** na záhlaví.

Chcete-li aktualizovat informace pro všechny portlety najednou, klikněte na **Obnovit portlety** v horní části řídícího panelu.

8.1.2. Upravování nastavení portletů

Některé portlety nabízejí informace o stavu, zatímco jiné hlásí bezpečnostní události za poslední časový úsek. Můžete kontrolovat a nastavit hlášený úsek portletu kliknutím na ikonu **Upravit portlet** na jeho titulní liště.

8.1.3. Přidání nového portletu

Pro získání potřebných informací můžete přidat další portlety.

Pro přidání nového portletu:

1. Přejděte na stránku **Kontrolní panel**.
2. Klikněte na tlačítko **Přidat portlet** v horní části konzole. Zobrazí se konfigurační okno.
3. Pod kartou **Detaily** nastavte podrobnosti portletu:
   - Typ koncového zařízení (**Počítače**, **Virtuální zařízení** nebo **Mobilní zařízení**)
   - Typ hlášení na pozadí
   - Definující název portletu
   - Časový úsek pro hlášené události

   Pro více podrobností o typech hlášení se odkažte na „Typy hlášení“ (str. 477).
4. Pod kartou **Cíle** zvolte síťové objekty a skupiny, které chcete zahrnout.
5. Klikněte na tlačítko **Save**.

8.1.4. Odstranění portletu

Jakýkoli portlet můžete snadno odstranit kliknutím na ⊗ **Odstranit** na jeho hlavní liště. Jakmile smažete portlet, už ho nelze obnovit. Můžete ale vytvořit jiný portlet s tím samým nastavením.

8.1.5. Přeuspořádání portletů

Můžete přeuspořádat portlety na kontrolním panelu tak, aby lépe vyhovovaly vašim potřebám. Pro přeuspořádání portletů:

1. Přejděte na stránku **Kontrolní panel**.
2. Přetáhněte každý portlet na požadovanou pozici. Všechny ostatní portlety mezi novou a starou pozicí jsou přesunuty, aby bylo zachováno jejich pořadí.

> **Poznámka**
> S portlety můžete pohybovat pouze mezi již obsazenými pozicemi.

9. VYŠETŘOVÁNÍ INCIDENTŮ

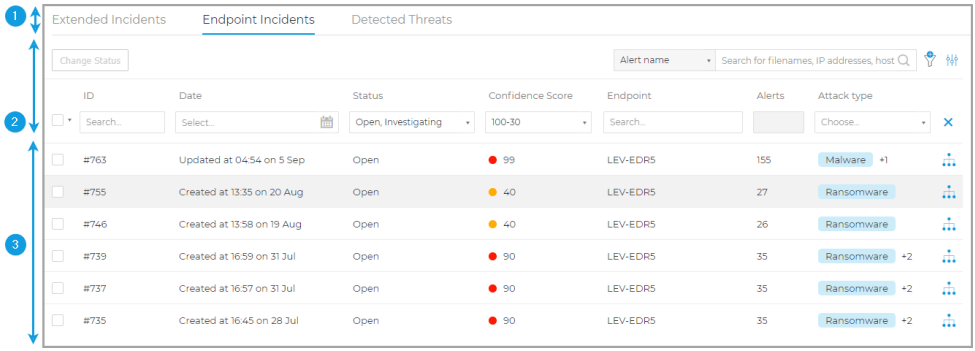
Sekce **Incidenty** vám pomůže filtrovat, vyšetřovat a provádět akce týkající se všech bezpečnostních událostí detekovaných senzorem incidentů v určitém časovém intervalu.

Sekce **Incidents** obsahuje následující stránky:

- **Incidenty**: umožňuje prohlížení a šetření bezpečnostních událostí.
- **Blocklist**: spravuje blokované soubory, které jsou zainteresovány v bezpečnostních událostech.

9.1. Stránka incidentů

Stránka **Incidenty (Incidents)** pro filtrování a správu bezpečnostních událostí.



Přehledová stránka incidentů

Poznámka
Dostupnost těchto karet se může lišit v závislosti na licenci obsažené ve vašem aktuálním plánu.

Tato stránka obsahuje následující oblasti:

1. Lišta okna se záložkami, které obsahují různé typy incidentů:
   - **Incidenty koncových bodů** : zobrazí všechny podezřelé incidenty zjištěné na úrovni koncových bodů, které vyžadují vyšetřování a u nichž ještě nebyla provedena žádná akce.

- **Zjištěné hrozby** : zobrazí všechny bezpečnostní události identifikované jako hrozby moduly prevence GravityZone. Tyto incidenty jsou detekovány na úrovni koncového bodu a jsou řešeny pomocí akcí předdefinovaných v zásadách zabezpečení použitých ve vašem prostředí.

2. Možnosti filtrování k přizpůsobení tabulky:
   - Kliknutím na tlačítko **Zobrazit/skrýt sloupce** přidejte nebo odeberte sloupce filtru.

     Stránka se automaticky aktualizuje a načte karty bezpečnostních událostí informacemi odpovídajícími přidaným sloupcům.
   - Kliknutím na tlačítko **Zobrazit/skrýt filtry** zobrazíte nebo skryjete panel filtrů.
   - Klepnutím na tlačítko **Vymazat filtry** resetujte všechny filtry.
3. Mřížka Incidenty, která zobrazuje seznam bezpečnostních událostí podle použitých filtrů.

Poznámka
Tato funkce již neposkytuje podporu pro Internet Explorer.

Lišta Přehled

Lišta **Přehled** uvádí otevřené incidenty, hlavní výstrahy, ovlivněná zařízení a další relevantní data, aby vám poskytla rychlý přehled o celkové situaci ohrožení kterému vaše prostředí čelí.

Lišta Přehled

Poznámka
Dostupnost a obsah lišty **Přehled** se může lišit v závislosti na licenci obsažené ve vašem aktuálním plánu.

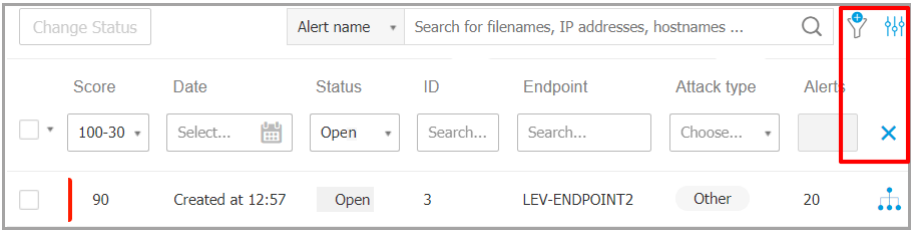
Filtrování incidentů z lišty Přehled

Seznam incidentů můžete filtrovat výběrem hodnot na panelu Přehled:

- Pokud kliknete na hodnotu v sekci **OTEVŘENÉ INCIDENTY** , zobrazí se pouze incidenty s vybranou úrovní závažnosti.
- Pokud kliknete na hodnotu v sekci **TOP ALERTY** , vyplní se do vyhledávacího pole název výstrahy a zobrazí se pouze incidenty, u kterých byla výstraha detekována.
- Pokud kliknete na hodnotu v sekci **TOP TECHNIKY** , vyplní se do vyhledávacího pole název techniky a zobrazí se pouze incidenty, kde byla technika zjištěna.
- Pokud kliknete na hodnotu v sekci **TOP DOTČENÁ ZAŘÍZENÍ** , zobrazí se pouze incidenty ovlivňující vybrané zařízení.

9.1.1. Tabulka filtrů

Stránka **Incidenty** vám umožňuje zvolit, jaké incidenty se mají zobrazit úpravou tabulky filtrů.



Tabulka filtrů

- Kliknutím na tlačítko **Zobrazit/skrýt sloupce** přidejte nebo odeberte sloupce filtru.

  Stránka se automaticky aktualizuje a načte karty bezpečnostních událostí informacemi odpovídajícími přidaným sloupcům.
- Kliknutím na tlačítko **Zobrazit/skrýt filtry** zobrazíte nebo skryjete panel filtrů.
- Klepnutím na tlačítko **Vymazat filtry** resetujte všechny filtry.

Podrobnosti o dostupných možnostech filtrování naleznete v následující tabulce:

Možnost filtrování	Podrobnosti
Skóre	Skóre důvěryhodnosti je číslo mezi 100 a 10, což ukazuje, jak potenciálně nebezpečná je bezpečnostní událost. Čím vyšší je skóre, tím je jistější, že událost je nebezpečná. Poskytuje kontext postavený na indikátorech útoku (attack indicators), a také na &CK Technikách, pokud to je aplikovatelné. Chcete-li filtrovat podle skóre důvěryhodnosti, přetáhněte posuvník na vybrané hodnoty. Nebo můžete použít číselná pole pod posuvníkem. Výběr skóre potvrďte kliknutím na **OK** .
Datum	Pro filtrování podle datumu: 1. Kliknutím na ikonu kalendáře nebo do pole **Datum** otevřete stránku s konfigurací datumů. 2. Vyberte časový rámec, ve kterém k incidentu došlo: • Kliknutím na karty **Od** a **Do** vyberte datumy definující časový interval. **Poznámka** Přesný čas pro datum zahájení a ukončení můžete určit pomocí polí hodin a minut pod kalendářem. • Můžete také vybrat předem určený časový rámec, relativně k aktuálnímu času. 3. Klepnutím na tlačítko **OK** se aplikuje filtr.
Stav	Filtrujte incidenty podle jejich aktuálního stavu zaškrtnutím jedné nebo více možností stavu dostupných v rozbalovací nabídce **Stav** : • **Otevřít** : pro nevyřešené bezpečnostní události • **Vyšetřované (Investigating)**: pro bezpečnostní události které jsou ve stavu investigace • **Falešně Pozitivní** : pro bezpečnostní události označené jako falešný poplach • **Uzavřené (Closed)**: pro bezpečnostní události u kterých byla investigace již uzavřena

Možnost filtrování	Podrobnosti
ID	Seznam incidentů se zúží vyhledáním konkrétního čísla ID bezpečnostní události.
Koncový bod	Seznam incidentů se zúží vyhledáním konkrétního názvu koncového bodu ze spravované sítě.
Typ Útoku	Typ útoku je dynamický seznam nejběžnějších typů útoků, který se mění na základě indikátorů útoku nalezených v uvedených bezpečnostních událostech.
Výstrahy	Sloupec **Upozornění** zobrazuje počet upozornění spuštěných na incident.
OS koncového bodu	Tato možnost filtruje události zabezpečení podle operačního systému příslušných koncových bodů.

Poznámka
Možnosti filtrování se mohou lišit v závislosti na typu licenčního klíče obsaženého ve vašem aktuálním plánu.

Chcete-li vyhledat další prvky, které nejsou viditelné v tabulce filtru, vyberte jednu z možností vyhledávání z rozbalovací nabídky **Hledat** :

- **Název výstrahy** - 3 až 1000 znaků maximálně.
- **ATT&CK Technika** - 100 znaků maximálně.
- **IP koncového zařízení** - 45 znaků maximálně.
- **MD5** - 32 znaků maximálně.
- **SHA256** - 64 znaků maximálně
- **Název uzlu** - 360 znaků maximálně.
- **Uživatelské jméno** - 1000 znaků maximálně.

Stránka se aktualizuje automaticky a načte pouze karty událostí zabezpečení odpovídající hledanému prvku. Pro podrobnější vyhledávání můžete vytvořit vyhledávací dotazy na Vyhledávací stránce.

9.1.2. Zobrazit seznam bezpečnostních událostí

Na stránce **Incidenty** se zobrazuje seznam bezpečnostních událostí odpovídajících vybraným filtrům.

Ve výchozím nastavení je na stránce zobrazeno 20 událostí, které jsou rozděleny podle data. Stránka se automaticky obnovuje v pravidelných intervalech, protože nové události jsou spuštěny pomocí funkce EDR.

Důležité
Všechny události zabezpečení starší než 90 dnů jsou automaticky odstraněny jak v sekci **Události koncového bodu**, tak v části **Zjištěné hrozby** a také z úložiště událostí zabezpečení.

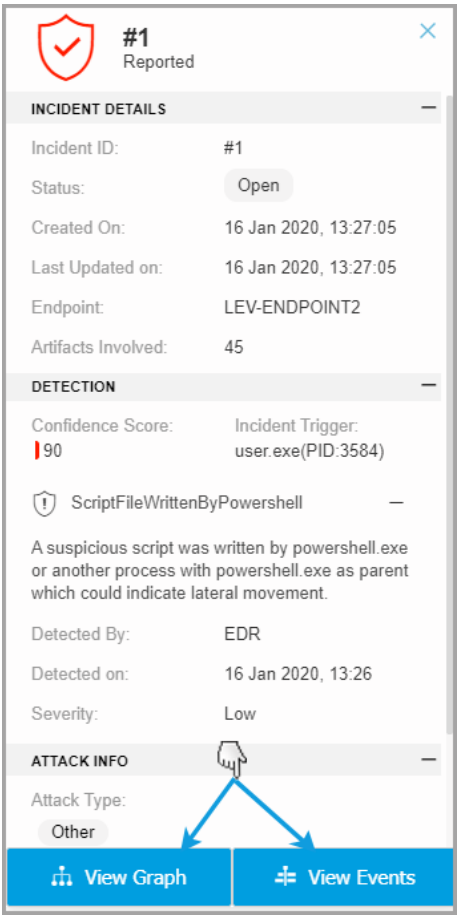
Chcete-li procházet stránkou, použijte šipky, rolovací kolečko nebo klepněte na posuvník. Změňte počet zobrazovaných událostí ve spodní části stránky. Můžete nastavit až na 100 událostí pro stránku.

Každá položka bezpečnostní události je uvedena ve formátu bohaté karty a poskytuje přehled o každé události s informacemi založenými na vybraných filtrech.

Poznámka
Prozkoumejte si barvy na levém okraji za účelem rychlého vyhodnocení úrovně důvěry (confidence level) (nízká, střední nebo vysoká).

Karta bezpečnostních událostí

- Pokud klepnete na odpovídající tlačítko **Zobrazit graf** kartu zabezpečení události, otevře ji na nové stránce, kde můžete incident podrobně analyzovat a podniknout příslušné kroky.
- Pokud kliknete na kartu události zabezpečení, otevře se panel rychlého zobrazení s informacemi o vybraném incidentu.



Rychlý náhled na podrobnosti incidentu

- Klepnutím na tlačítko **Zobrazit graf** získáte přístup k grafické vizualizaci incidentu.
- Kliknutím na tlačítko **Zobrazit události** se dostanete na časovou osu incidentu.

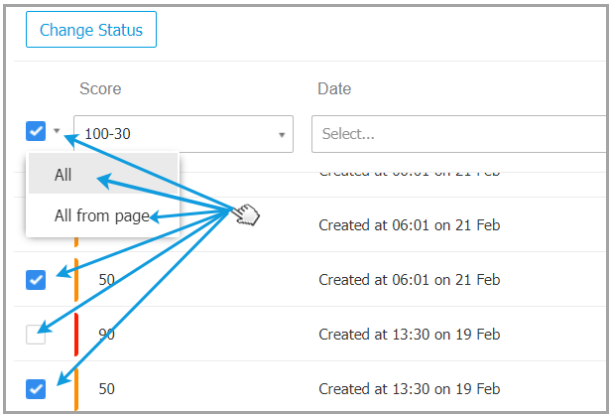
- Pokud zaškrtnete políčko jakékoli karty událostí zabezpečení, aktivuje tlačítko **Změnit stav**, což vám umožní změnit aktuální stav incidentu.

Změna stavu bezpečnostních událostí

Stav kontroly vám pomůže sledovat incidenty, které již byly zkontrolovány a označeny jako uzavřené nebo falešně pozitivní, incidenty, které jsou v současné době předmětem kontroly, a otevřené nebo nové incidenty, které dosud nebyly analyzovány.

Můžete se rozhodnout změnit stav jedné nebo více bezpečnostních událostí najednou:

1. Zaškrtněte políčka karet událostí, které projdou změnou stavu.

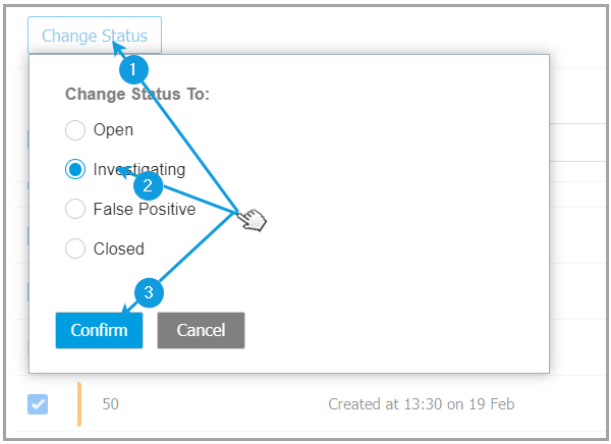


Výběr karet bezpečnostní události

Můžete je vybrat jednotlivě nebo pomocí možností hromadného výběru v rozbalovací nabídce.

Poznámka
Při výběru můžete také procházet několik stránek bezpečnostních událostí.

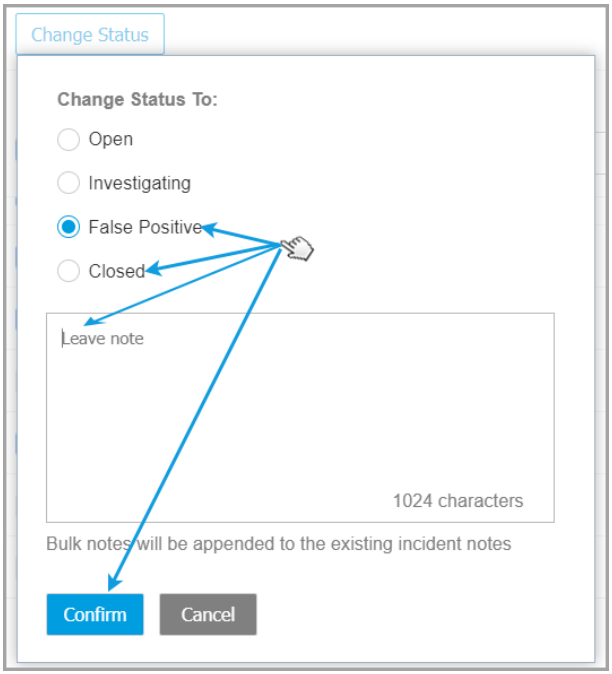
2. Klikněte na tlačítko **Změnit stav** a vyberte požadované možnosti:



Změna stavu bezpečnostní události

- **Open** - pokud bezpečnostní událost ještě není otestována.
- **Vyšetřované (Investigating)**- pokud jste začali investigovat událost.
- **Falešně Pozitivní** - když jste událost analyzovali a identifikovali ji jako falešně pozitivní.
- **Uzavřené (Closed)**- pokud jste dokončili investigaci.

> **Poznámka**
> Při změně stavu událostí na **Falešně Pozitivní** nebo **Uzavřeno** se otevře okno, kde můžete zanechat poznámku o důvodech změny stavu události pro pozdější konzultaci.



Zanechání poznámky pro falešně pozitivní a uzavřené události

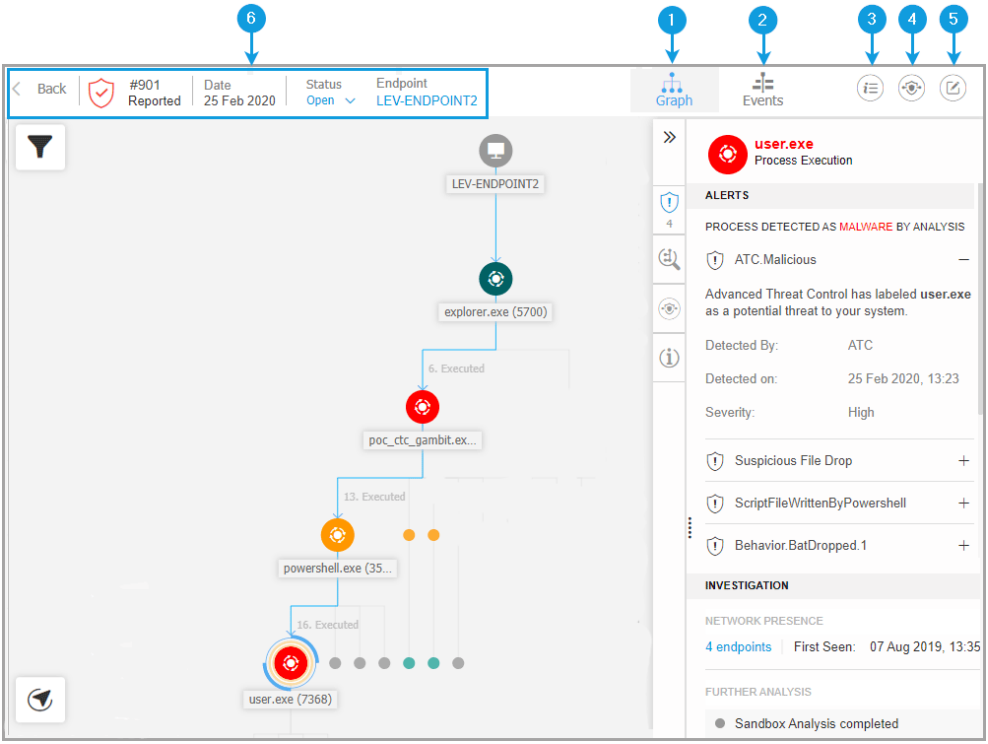
Poznámka
Poznámka bude připojena k těm, které již existují uvnitř filtrovaných incidentů.

3. Kliknutím na **Confirm** aplikujete zvolené možnosti.

9.1.3. Vyšetřování incidentu koncového bodu

Na stránce **Incidenty** určete bezpečnostní událost, kterou chcete analyzovat, a klikněte na **Zobrazit graf** a zobrazí se na nové stránce.

Každý bezpečnostní incident má vyhrazenou stránku obsahující podrobné informace o posloupnosti událostí (zobrazené v grafu jako propojené uzly bezpečnostních událostí), které vedly ke spuštění incidentu, a poskytuje možnosti pro provedení nápravných opatření.


6
1
2
3
4
5
Back
#901
Reported
Date
25 Feb 2020
Status
Open
Endpoint
LEV-ENDPOINT2
Graph
Events
LEV-ENDPOINT2
explorer.exe (5700)
6. Executed
poc_ctc_gambit.ex...
13. Executed
powershell.exe (35...
16. Executed
user.exe (7368)
user.exe
Process Execution
ALERTS
PROCESS DETECTED AS MALWARE BY ANALYSIS
ATC.Malicious
Advanced Threat Control has labeled user.exe as a potential threat to your system.
Detected By: ATC
Detected on: 25 Feb 2020, 13:23
Severity: High
Suspicious File Drop
ScriptFileWrittenByPowershell
Behavior.BatDropped.1
INVESTIGATION
NETWORK PRESENCE
4 endpoints
First Seen: 07 Aug 2019, 13:35
FURTHER ANALYSIS
Sandbox Analysis completed

1. Karta Graf

   Graf zobrazuje bezpečnostní incident a jeho jednotlivé prvky, zvýrazňuje kritickou cestu incidentu a zobrazuje podrobnosti o uzlu, který incident spustil, na panelu **Node Details**.

2. Karta Události

   Karta Události zobrazuje filtrovatelné zjištěné systémové události a výstrahy a jejich odpovídající popisy.

3. Informační panel incidentů

   Tento panel obsahuje rozbalovací části s podrobnostmi, jako je ID incidentu, aktuální stav, časové razítko, kdy byl vytvořen a naposledy aktualizován, počet zúčastněných artefaktů, název a informace o útoku.

4. Nápravný panel

   Tento panel obsahuje rozkládací sekce s akcemi, které GravityZone provádí automaticky, a doporučené kroky, kterými můžete incident zmírnit.

5. schránka poznámek

   Kliknutím na tlačítko **Notes** se otevře schránka, do které můžete přidat poznámky k aktuální události, kterou si můžete přečíst při pozdější revizi incidentu.

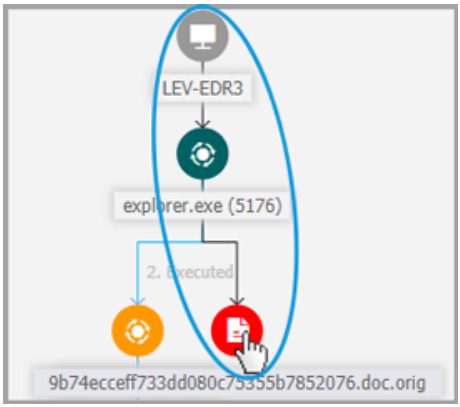
6. Lišta stav incidentů

   Stavová lišta nabízí podrobnosti o ID incidentu, čase a datu kdy byl vygenerován, stavu spouštění incidentu na koncovém bodu, který ovlivňuje. Kliknutím na tlačítko **Back** se dostanete zpět na hlavní stránku **Incidents**.

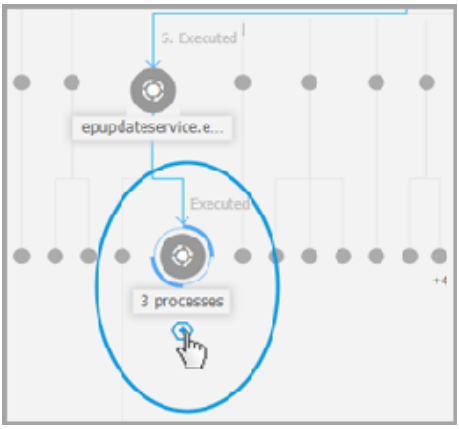
Uzly událostí zabezpečení

Vše co potřebujete znát o uzlech bezpečnostních událostí:

- Každý uzel představuje specifický prvek zapojený do testovaného incidentu.
- Všechny uzly, které vytvářejí kritickou cestu, jsou ve výchozím nastavení podrobně zobrazeny, když otevřete incident, zatímco ostatní prvky jsou vybledlé, aby nedocházelo k nepřehlednému zobrazení.
  - Umístěním kurzoru na uzel, který není součástí kritické cesty, se zvýrazní a zobrazí se zdrojová cesta, aniž by došlo k přerušení Critical Path.



- Tři nebo více stejných akcí ke stejnému typu událostí, které přichází z nadřazeného uzlu, jsou seskupeny do rozšířeného uzlu.



  - V případe kolapsu cluster-node budou skryty z grafu dopadu pouze uzly bez podřízených prvků.
  - Uzly, u nichž byla zjištěna podezřelá aktivita, nebudou přidány do cluster-node.
- Kliknutím na uzel se zobrazí následující podrobnosti:

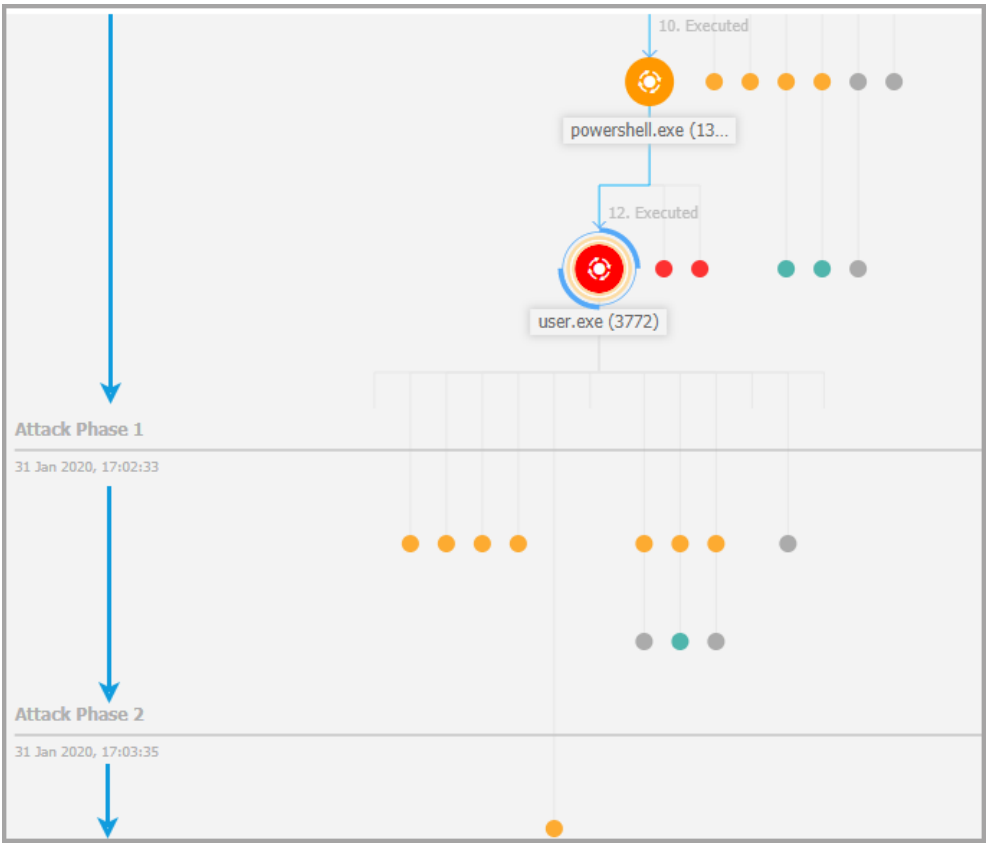
  - Modře zvýrazní cestu k uzlu koncového bodu spolu se všemi ostatními zahrnutými prvky.
  - Boční panel s rozšířenými částmi, který poskytuje detailní informace o vybraném uzlu, upozornění v případě detekce na dostupné akce a doporučení. Další informace naleznete v části „Podrobnosti o uzlu“ (str. 429).
- Uzly jsou spojeny pomocí šipek označujících průběh akcí, ke kterým došlo v koncovém bodě během incidentu. Každý řádek je označen názvem akce a jejím chronologickým číslem.

Následující prvky incidentu mohou být nazývány jako uzly.

Typ uzlu	Popis
Koncový bod	Zobrazuje detaily o koncovém bodu a stav záplat.
Doména	Zobrazuje informace o hostované doméně a jejich koncových bodech.
Proces	Zobrazuje podrobnosti o roli procesu v aktuálním incidentu, informace o souboru, podrobnosti o provedených procesech, chování v síti a možnosti dalšího testování.
Soubor	Zobrazuje podrobnosti o roli souboru v aktuálním incidentu, informace o souboru, chování v síti a dalších možnostech otestování.
Registr	Zobrazí informace o registru a podrobnosti o nadřazeném procesu.

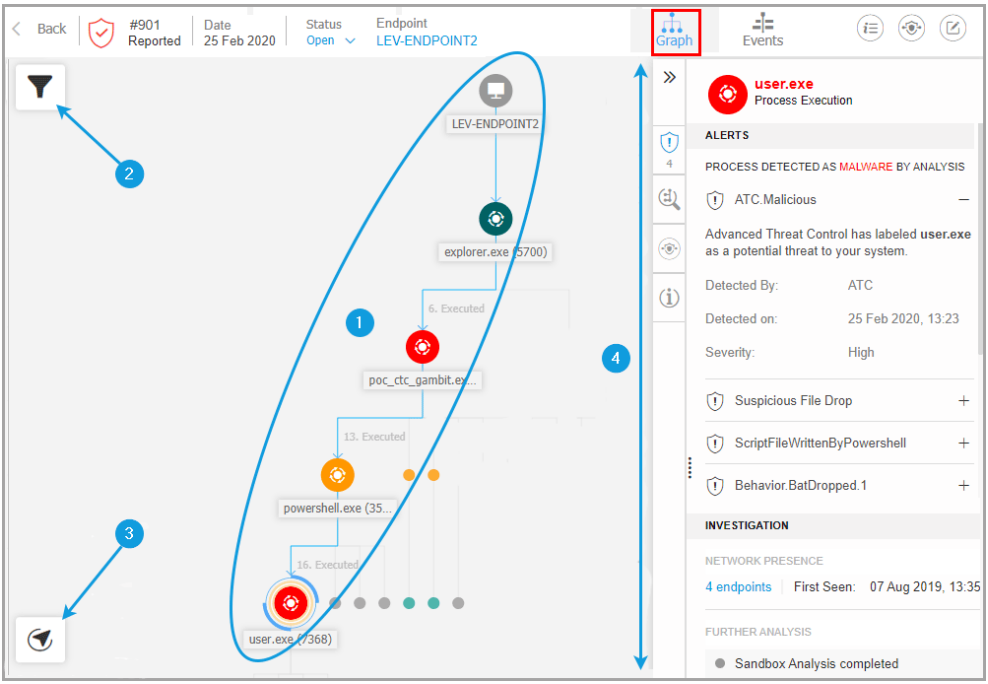
Graf

Graf **Graph** poskytuje interaktivní grafické znázornění otestovaného incidentu a jeho kontextu a zvýrazňuje sled prvků, které se přímo podílejí na jeho spuštění, známé jako **Critical Path** incidentu, jakož i všech ostatních zúčastněných prvků, které jsou ve výchozím nastavení vybledlé. V případě složitých incidentů, které se postupem času vyvíjejí, se v grafice zobrazuje každá jednotlivá fáze útoku.



Postupný útok

Graf obsahuje možnosti filtrování, které umožňují přizpůsobení incidentové grafiky ke zlepšení vizualizace, funkce pro navigaci po incidentové mapě a panely detailů s více informacemi o každém prvku.



Karta Graf

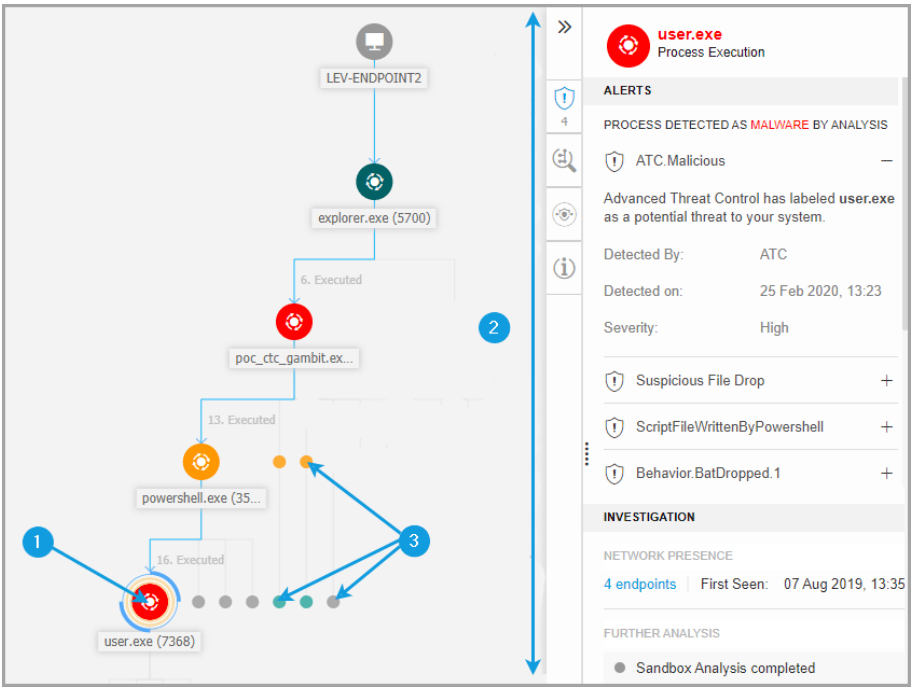
1. Kritická cesta
2. Nabídka filtrů
3. Nabídka navigátoru
4. Panel Detail uzlu

Kritická cesta

Critical Path je posloupnost propojených bezpečnostních událostí, které vedly k vypnutí výstrahy, počínaje bodem vniknutí do sítě až po uzel události, který spustily incident . Kritická cesta incidentu je standardně zvýrazněna v grafu spolu se všemi sestávajícími uzly událostí, zatímco ostatní prvky jsou minimalizovány.

Spouštěcí uzel je zvýrazněn od ostatních prvků v grafu, je obklopen dalšími zvýrazňujícími prvky (dva oranžové kruhy) a související informační panel je

standardně zobrazen vedle grafu dopadu, což poskytuje podrobné informace o spouštěném uzlu.



Kritická cesta

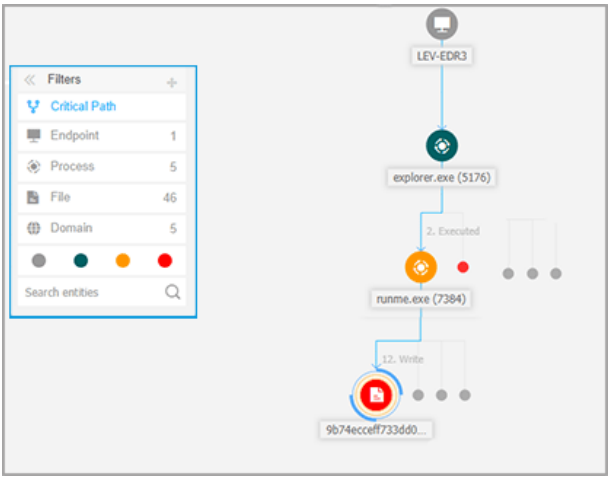
1. Spouštěcí uzel
2. Panel Podrobnosti uzlu s informacemi seskupenými do kategorií a skládacích sekcí
3. Vybledlé uzly nepřímo zapojené do incidentu

Poznámka
Kliknutím na jakýkoli jiný prvek než spouštěcí uzel přeruší kritickou cestu a zvýrazní cestu od začátku, od vybraného uzlu až zpětbě po uzel koncového bodu.

Filtry

Nabídka **Filters** vám poskytuje vylepšené možnosti filtrování, které umožňují plnou manipulaci s grafikou incidentu, zvýrazněním prvků na základě jejich typu nebo relevance, nebo jejich skrytím, aby byl incident kompaktnější a snáze analyzovatelný.

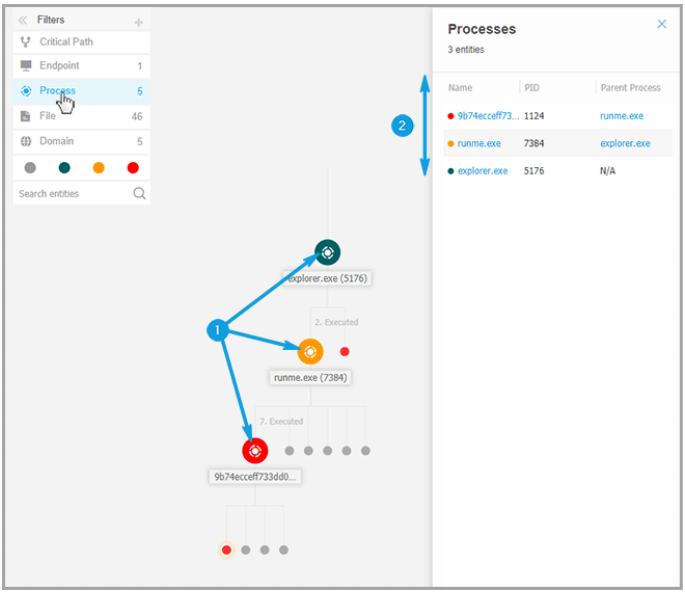
Kliknutím a podržením ikony **Přetáhněte** umístěte plovoucí filtry panelu kdekoli uvnitř grafu incidentu.



Filtry grafů incidentů

Při filtrování typu prvku:

1. grafický incident se oddálí a zvýrazní všechny prvky vybraného typu, zatímco prvky jiného typu jsou vybledlé.
2. kamžitě otevře panel se seznamem všech zvýrazněných prvků.



Poznámka
Výběr prvku ze zobrazeného seznamu jej zvýrazní v grafice incidentu a otevře panel detailů s informacemi o tomto prvku.
Naraz lze použít pouze jeden filtr.

Možnosti filtrování obsahují:

- **Critical Path**: Ukazuje kritickou cestu incidentu ohrožení.
- **Endpoint**: Označuje koncové body ovlivněné incidentem.
- **Process**: Zdůrazňuje všechny typu procesu na uzlech zapojených do incidentu.
- **File**: Zdůrazňuje typy souborů na uzlech zapojených do incidentu.
- **Domain**: Zdůrazňuje všechny typy domén na uzlech zapojených do incidentu.
- **Registry**: Zdůrazňuje všechny typu registru na uzlech zapojených do incidentu.

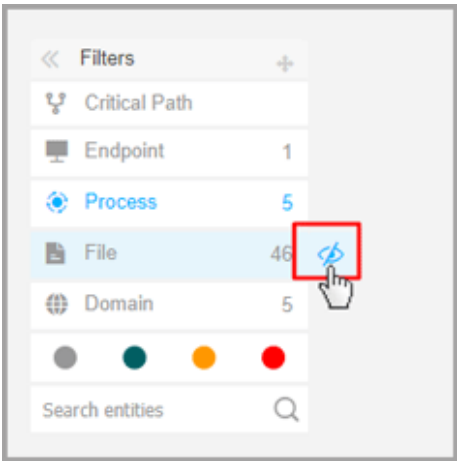
- **Element Relevance**: Můžete také filtrovat prvky podle jejich důležitosti uvnitř incidentu.
  - **Neutral node**: Prvky bez přímého dopadu na bezpečnostní incident.
  - **Important node**: Prvky s důležitou roli v bezpečnostním incidentů.
  - **Původní uzel** : Vstupní bod útoku uvnitř sítě .
  - **Suspicious node**: Prvky s podezřelým chováním, s přímou učástí na bezpečnostním incidentu.
  - **Malicious node**: Prvky, které způsobily poškození vaší sítě .

    Poznámka
    Podržením kurzoru nad některým z barevných filtrů se zobrazí, kolik prvků se stejným významem je zahrnuto do incidentu.

- **Vyhledávací entity** : Ve vyhledávacím poli můžete vyhledávat jména nebo přípony souborů incidentů a výsledky se zobrazí na bočním panelu.

Pokud nejsou vybrány žádné filtry, graf dopadu se vrátí do výchozího stavu se zvýrazněnými koncovými body, zdroji a spouštěnými prvky, zatímco ostatní prvky jsou vybledlé.

Můžete také skrýt určité prvky z grafu dopadu kliknutím na tlačítko **Show/Hide**, které se zobrazí při posunutí myši nad filtry typu: Soubor, Doména a Registr.



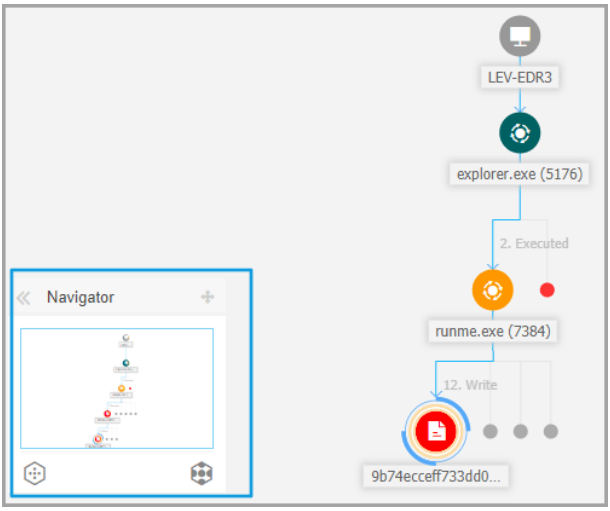
Skrytí typu prvku překreslí graf dopadu odstraněním všech odpovídajících prvků, i když jsou oddálené, s výjimkou spouštěcího uzlu a uzlů s podřízenými prvky.

Navigátor

Navigator vám umožňuje pohybovat se rychle v grafu incidentů a prozkoumat všechny zobrazené prvky pomocí miniaturní mapy a různých úrovní vizualizace.

Kliknutím a podržením ikony **Přetažení** umístěte plovoucí navigátor panel kdekoli uvnitř grafu incidentu.

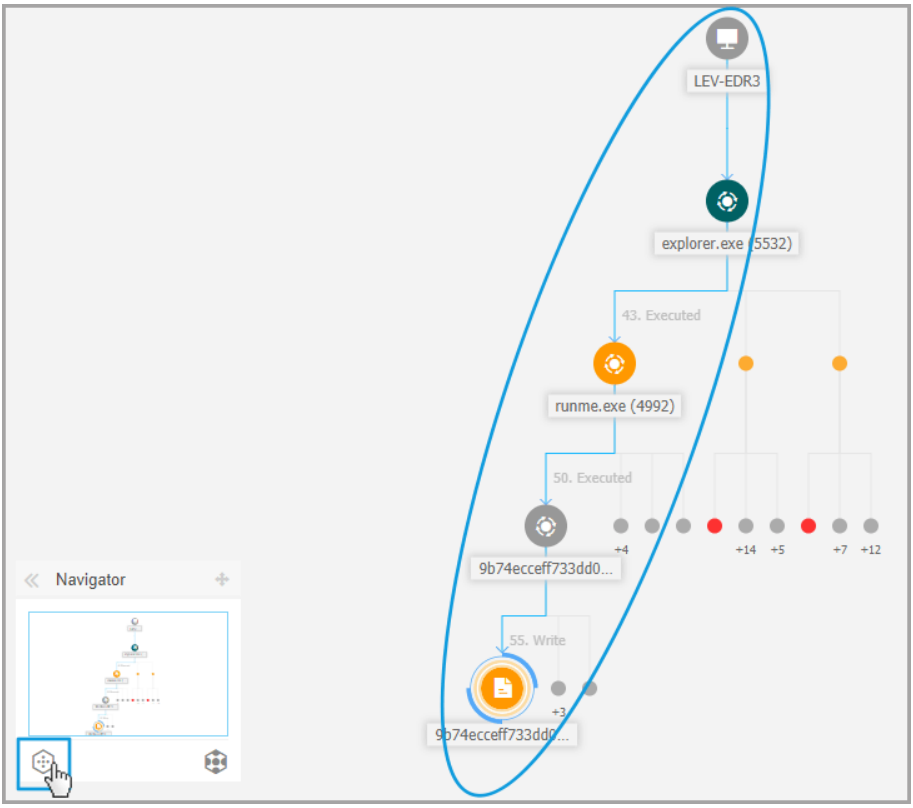
Navigator je ve výchozím nastavení sbalen. Při jeho rozbalení se v nabídce zobrazí miniaturizovaná verze celé mapy incidentů a akční tlačítka pro úpravu vizualizace.



Navigátor

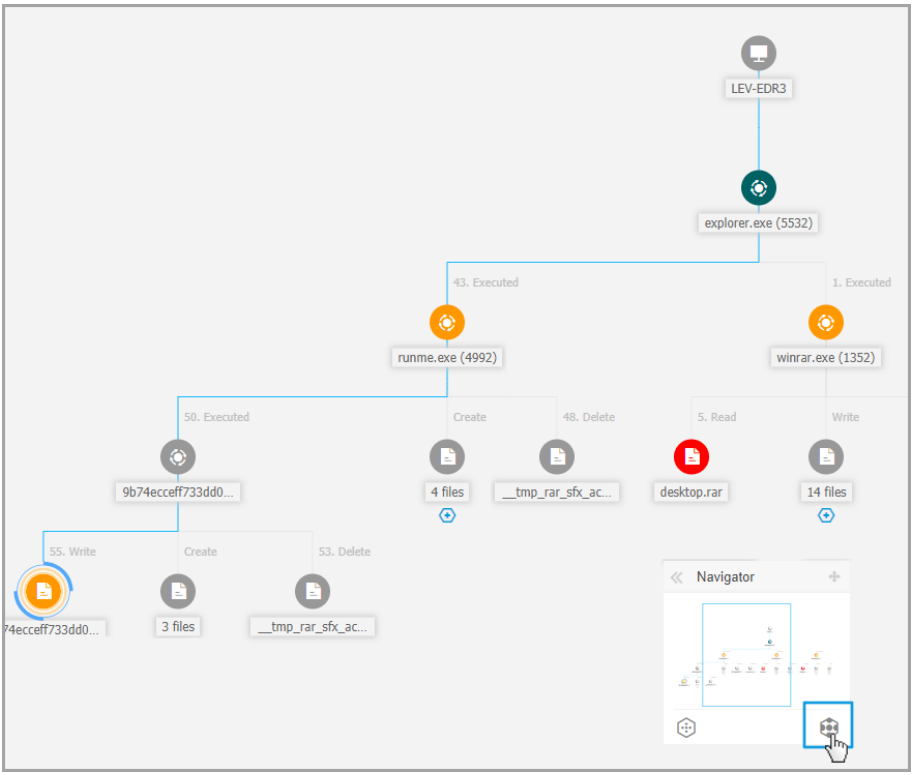
Nabídka **Navigator** nabízí dvě akční tlačítka pro úpravu způsobu, jakým si vizualizujete graf incidentu, **Fewer Details** tlačítko, a **More Details** tlačítko.

Když kliknete na tlačítko **Fewer Details**graf je nastaven do výchozího stavu a zvýrazňuje pouze kritickou cestu incidentu.



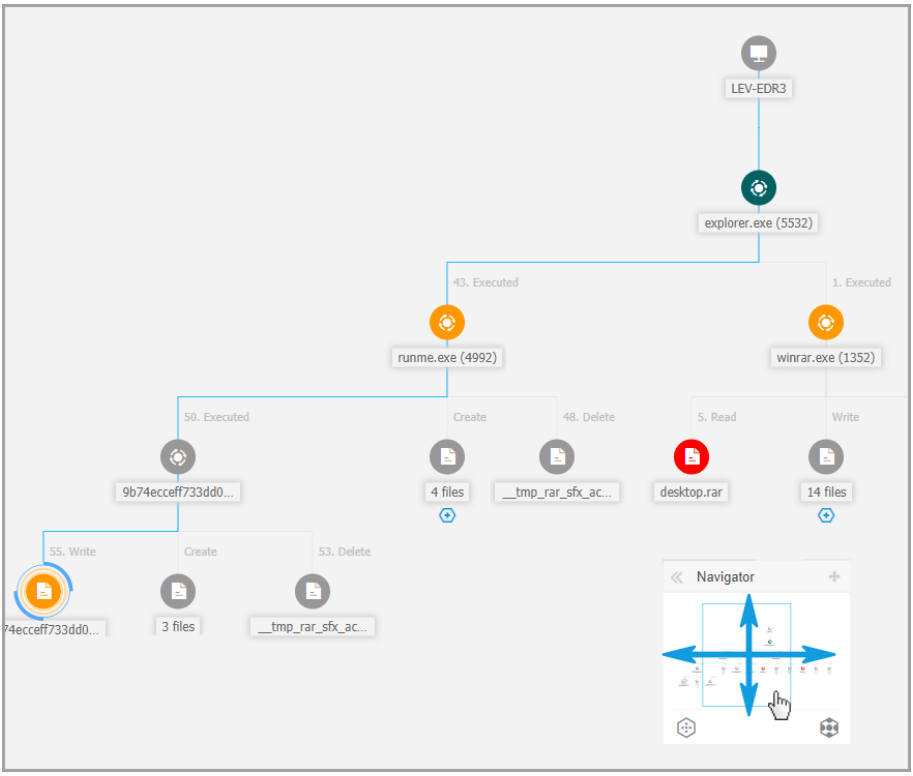
Přehled Vizualizace

Když kliknete na tlačítko **More Details**, všechny prvky grafu dopadu jsou rozšířeny a zvýrazňují každý uzel i shluky uzlů.



Zvětšená vizualizace

Když je incident zvětšený a všechny prvky jsou zvýrazněny, může se graf často rozšířit za hranice obrazovky. V takovém případě podržte a přetáhněte volič mapy v mini-mapě navigátoru, abyste se snadno dostali do požadované oblasti mapy incidentu, nebo jednoduše přetáhněte oblast grafu do požadovaného směru.

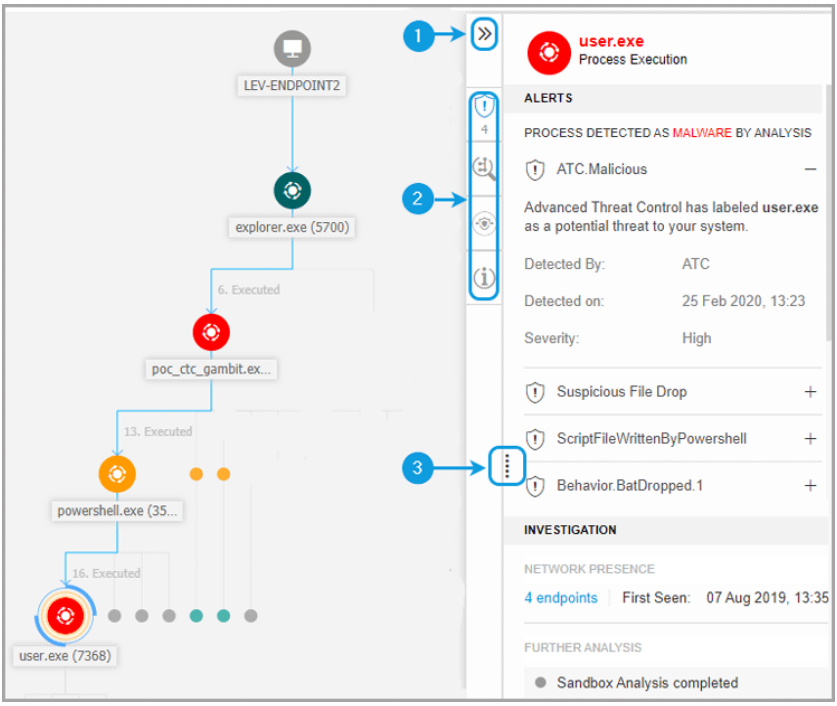


Mini-map Selector

Podrobnosti o uzlu

Panel **Podrobnosti o uzlu** obsahuje oddíly s podrobnými informacemi o vybraném uzlu, včetně preventivních nebo nápravných akcí, které můžete podniknout, aby se incident zmírnil, podrobnosti o typu detekce a výstrahy detekované na uzel, přítomnost v síti, podrobnosti provádění procesu, další doporučení ke správě bezpečnostní události nebo akce k dalšímu prozkoumání prvku.

Pro shlédnutí těchto informací a provedení akce uvnitř panelu, si vyberte uzel (node) uvnitř mapy bezpečnostních událostí.



Panel Detail uzlu

1. Kliknutím na tlačítko **Sbalit** můžete panel **Podrobnosti o uzlu** rozbalit nebo sbalit.
2. Informace zobrazené na panelu **Podrobnosti o uzlu** můžete snadno procházet kliknutím na ikony každé ze čtyř hlavních kategorií:
   - **UPOZORNĚNÍ**

     Tato část zobrazuje jednu nebo více detekcí spuštěných ve vybraném uzlu, včetně podrobností o technologii Bitdefender, která zahrnovala prvek v incidentu, důvodu, který spustil detekci, název detekce a datum, kdy došlo k její detekci.
   - **KONTROLA**

     Tato část zobrazuje časová razítka pro počáteční detekci a všechny koncové body, kde byl tento prvek spatřen.

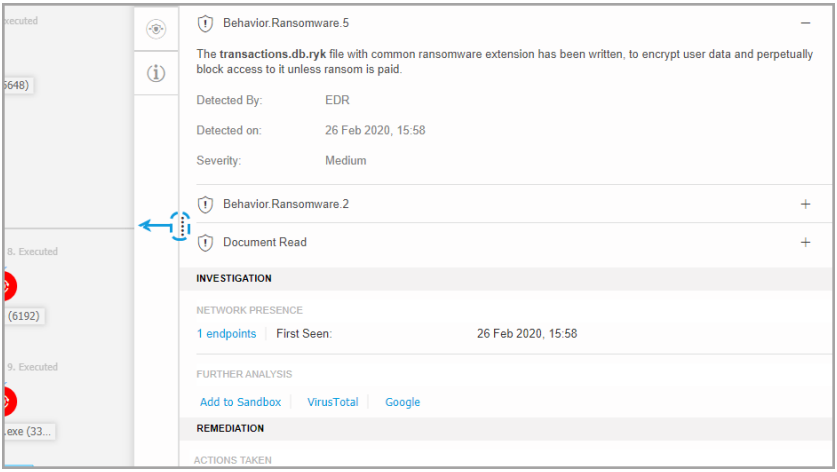
- **NÁPRAVA**

  Tato část zobrazuje akce provedené automaticky pomocí GravityZone, akce, které můžete okamžitě podniknout, aby se zmírnilo ohrožení, jakož i podrobná doporučení pro každou výstrahu detekovanou ve vybraném uzlu, která vám pomůže zmírnit incident a zvýšit úroveň zabezpečení. vašeho prostředí.

- **INFO**

  Tato část zobrazuje obecné informace o každém souboru a konkrétní informace v závislosti na typu vybraného uzlu.

3. Přetažením panelu **Podrobnosti uzlu** směrem do středu obrazovky můžete snadno procházet jeho obsahem.



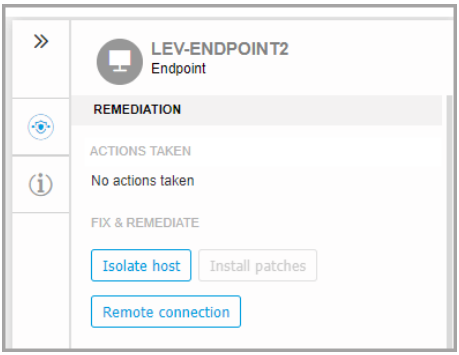
Rozbalený panel

Panel podrobností pro uzly koncového bodu

Panel **Podrobnosti o uzlu** pro koncové body obsahuje dvě kategorie:

- **NÁPRAVA**

  Zobrazuje informace o akcích, které GravityZone provádí automaticky, aby zmírnil hrozby a akce, které můžete provést:

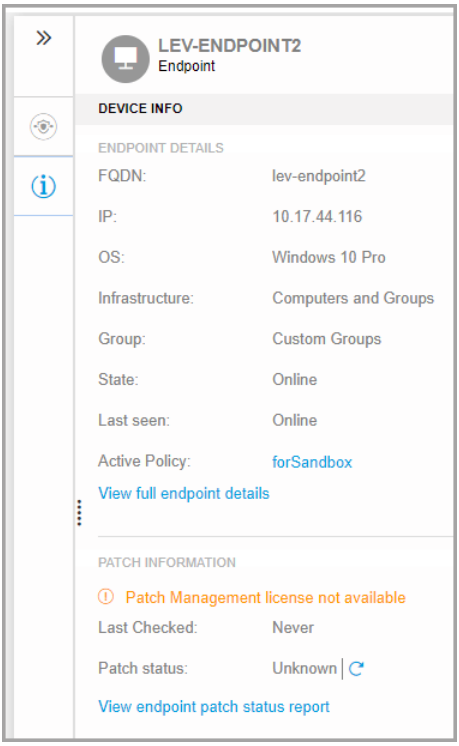


- **Isolate host** - Pomocí tohoto řešení izolujte koncový bod od sítě.
- **Install patches** - Pomocí této akce nainstalujte chybějící bezpečnostní opravy do cílového koncového bodu Tato funkce je viditelná pouze s Patch Management Modulem, a tento add-on je dostupný pomocí separátního licenčního klíče. Další informace naleznete v části Patch Install.
- **Remote Connection** - Tato akce slouží k navázání vzdáleného připojení ke koncovému bodu zapojeného do aktuální události a ke spuštění příkazů přímo v jeho operačním systému, aby se zabránilo okamžité hrozbě nebo pro sběr dat k další vyhodnocení.

  Kliknutím na toto tlačítko se zobrazí okno Remote Connection

- **INFORMACE O ZAŘÍZENÍ**

  Zobrazí obecné informace o ovlivněném koncovém bodu, jako je název koncového bodu, adresa IP, operační systém, příslušná skupina, stav, aktivní zásady a odkaz, který otevře nové okno, kde se zobrazí úplné podrobnosti koncového bodu.



Poskytuje také informace, jako je počet nainstalovaných oprav, neúspěšných oprav nebo chybějících oprav zabezpečení a jiných oprav. K tomu navíc si můžete vygenerovat report stavu záplat na koncových bodech (endpoint patch status report). Tato část je na vyžádání poskytována pro cílový koncový bod.

Uvnitř panelu můžete provádět následující akce:

– Podívejte se na informaci o záplatách na cílovém koncovém bodu. Podrobnosti o opravě zobrazíte kliknutím na **Obnovit** v této sekci.

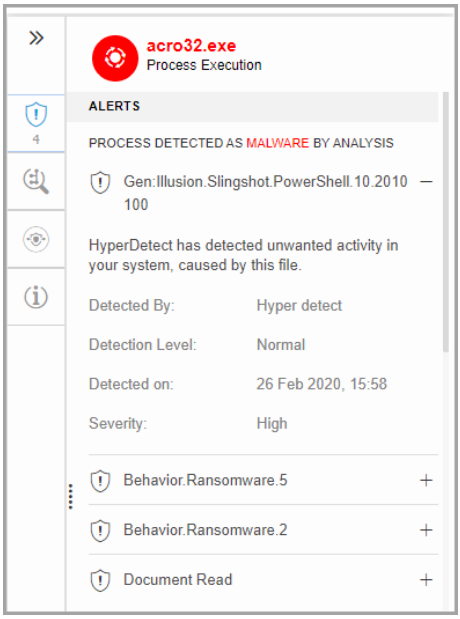
– Podívejte se na report stavu záplat (patch status report) pro cílový koncový bod. Pro vygenerování reportu, klikněte na **Zobrazení reportu stavu záplat (View endpoint patch status report)**.

Panel podrobností pro procesní uzly

Panel **Podrobnosti o uzlu** pro procesní uzly obsahuje čtyři kategorie:

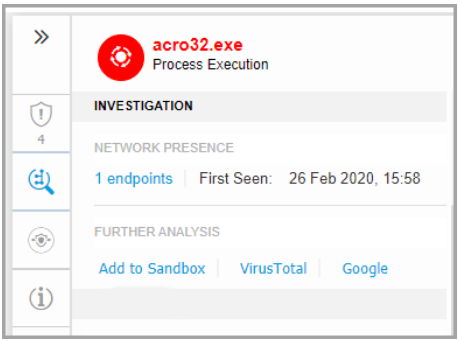
- **UPOZORNĚNÍ**

  Zobrazuje jednu nebo více detekcí spuštěných ve vybraném uzlu, včetně podrobností o technologii Bitdefender, která zahrnovala tuto entitu do incidentu, důvodu, který spustil detekci, názvu detekce a datum kdy byla detekována. Popis každého upozornění se řídí nejnovějšími standardy MITER

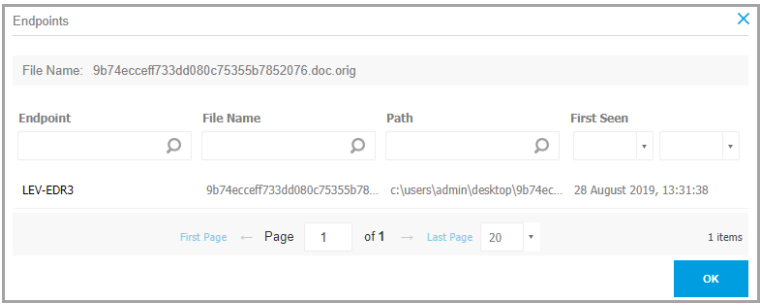


- **KONTROLA**

  Zobrazuje datová razítka pro počáteční detekci a všechny koncové body, kde byl tento prvek spatřen.



Chcete-li zobrazit tento seznam, klikněte na číslo zobrazené v poli **koncové body** a objeví se nové okno.

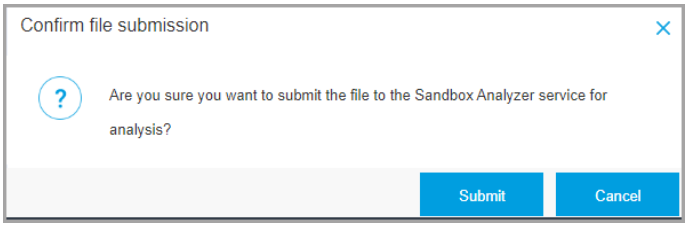


Tato část také poskytuje externí analýzu prostřednictvím interních komponent a řešení třetích stran.

K dispozici jsou následující akce:

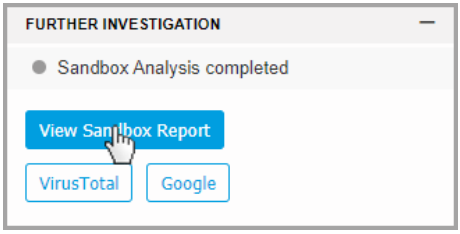
– **Add to Sandbox** - Pomocí této akce vygenerujete Sandbox Analyzer report

  Výběrem **Add to Sandbox** se zobrazí obrazovka s výzvou k potvrzení odeslání souboru.



Po potvrzení budete automaticky přesměrováni na stránku pro zaslání souboru.

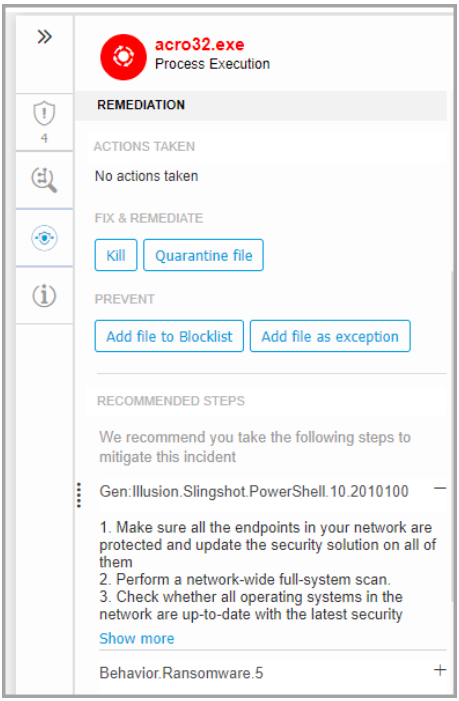
Po dokončení analýzy kliknutím na tlačítko **View Sandbox Report** otevřete úplnou zprávu.



- **VirusTotal** - Použijte tuto akci k odeslání souboru k externí analýze.
- **Google** - Použijte tuto akci pro vyhledání hash hodnoty souboru.

- **NÁPRAVA**

  Zobrazuje informace o akcích, které GravityZone provádí automaticky, aby zmírnil hrozby a akce, které můžete provést:



- **Kill** - Pomocí této akce zastavíte aktuální proces. Tato akce provede úlohu ukončení procesu (kill process task) viditelnou v liště spouštěných procesů (process execution bar). `System32` a Bitdefender procesy jsou vyjmuty z této akce.
- **Quarantine file** - Pomocí této akce uložíte dotyčnou položku do karantény pro zjištění jejiho skutečného využití. Tato akce vyžaduje, aby byl modul Firewall nainstalován na cílovém koncovém bodě.
- **Add file to Blocklist** - Spravujte blokované položky v části Blocklist.
- **Add file as Exception** - Tuto možnost použijte, chcete-li vyloučit danou aktivitu z konkrétní politiky. Pokud zvolíte tuto akci, v konfiguračním okně se zobrazí výzva k výběru politiky, do které chcete přidat výjimku. Spravujte si vyjímky v **Politiky (Policies) > Antimalware > Nastavení (Settings)**.

– **Přidat jako výjimku EDR** - Pomocí této možnosti vytvoříte vlastní pravidlo, které již nebude tento proces považovat za podezřelé nebo škodlivou detekci EDR.

1. Když kliknete na tlačítko **Přidat jako výjimku EDR** , objeví se nové okno s výzvou k potvrzení akce nebo k jejímu zrušení.
2. Po potvrzení akce vás GravityZone upozorní, že nové pravidlo je k dispozici v tabulce Pravidla pro výjimky . Všimněte si, že název všech pravidel vytvořených v grafu incidentu začíná číslem incidentu.

Poznámka
Když přejdete do podrobností pravidla, abyste je upravili, všimnete si, že všechna kritéria pro toto pravidlo byla vyplněna automaticky a bylo přidáno kritérium jen pro čtení s názvem výstrahy.

Důležité
Funkce **Přidat jako výjimku EDR** je k dispozici pouze pro:

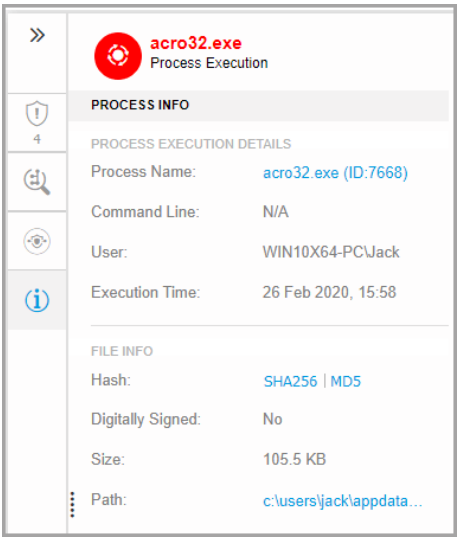
- upozornění vyvolaná technologií EDR
- uzly vytvořené jiným procesem
- podezřelé a škodlivé uzly

Pokud je vyloučený proces součástí kritické cesty incidentu, nebudou budoucí incidenty odpovídající tomuto kritériu vyloučení již generovány v síti incidentů. Pokud vyloučený proces není součástí kritické cesty incidentu, budou budoucí incidenty odpovídající tomuto kritériu vyloučení stále generovány v síti incidentů, ale nebudou tento proces nadále považovat za podezřelý nebo škodlivý.

Tato část také obsahuje podrobná doporučení pro každou výstrahu detekovanou ve vybraném uzlu, která vám pomůže při zmírnění incidentu a zvýšení úrovně zabezpečení vašeho prostředí.

- **PROCESNÍ INFORMACE**

  Zobrazuje podrobnosti o vybraném uzlu procesu, včetně názvu procesu, provedeného příkazového řádku, uživatele, času provedení, počátku a cesty souboru, hodnoty hash nebo digitálního podpisu.



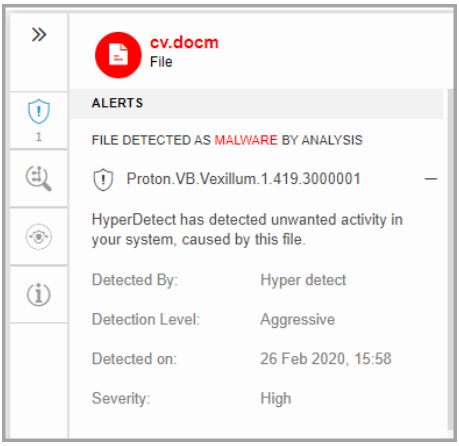
Hodnotu hash můžete zkopírovat do schránky kliknutím na dostupné algoritmy hashování v poli **Hash** a poté **Kopírovat do schránky** a použít ji k přidání hodnoty hashe souboru do **Blocklistu** . Pro více informací si přečtěte **Seznam blokovaných souborů (Blocklisting Files)**.

Panel Podrobnosti pro uzly souborů

Panel **Podrobnosti o uzlech** pro uzly souborů obsahuje čtyři kategorie:

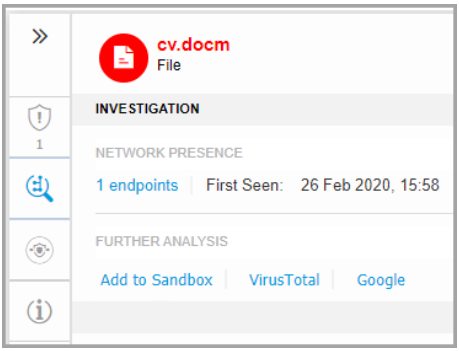
- **UPOZORNĚNÍ**

  Zobrazuje jednu nebo více detekcí spuštěných ve vybraném uzlu, včetně podrobností o technologii Bitdefender, která zahrnovala tuto entitu do incidentu, důvodu, který spustil detekci, názvu detekce a datum kdy byla detekována. Popis každého upozornění se řídí nejnovějšími standardy MITER

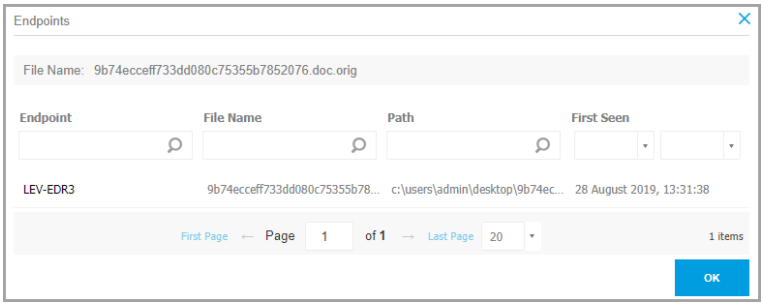


- **KONTROLA**

  Zobrazuje datová razítka pro počáteční detekci a všechny koncové body, kde byl tento prvek spatřen.



  Chcete-li zobrazit tento seznam, klikněte na číslo zobrazené v poli **koncové body** a objeví se nové okno.

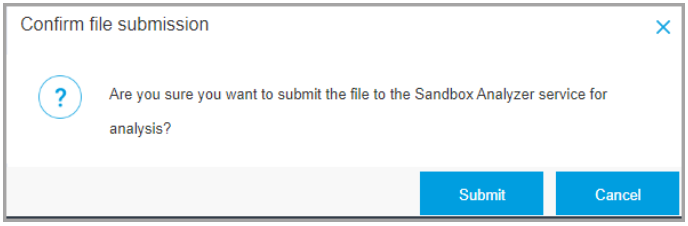


Tato část také poskytuje externí analýzu prostřednictvím interních komponent a řešení třetích stran.

K dispozici jsou následující akce:

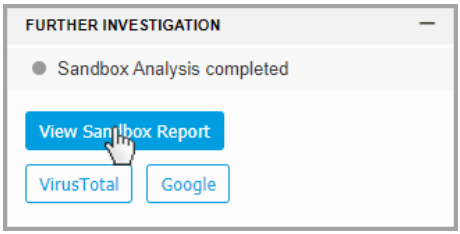
– **Add to Sandbox** - Pomocí této akce vygenerujete Sandbox Analyzer report

  Výběrem **Add to Sandbox** se zobrazí obrazovka s výzvou k potvrzení odeslání souboru.



  Po potvrzení budete automaticky přesměrováni na stránku pro zaslání souboru.

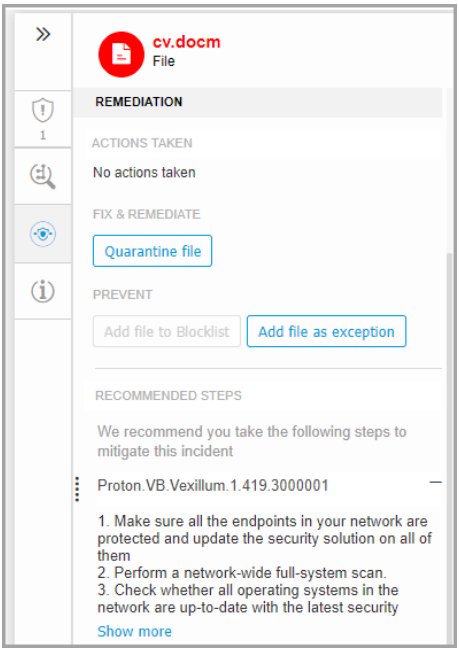
  Po dokončení analýzy kliknutím na tlačítko **View Sandbox Report** otevřete úplnou zprávu.



  - **VirusTotal** - Použijte tuto akci k odeslání souboru k externí analýze.
  - **Google** - Použijte tuto akci pro vyhledání hash hodnoty souboru.

- **NÁPRAVA**

  Zobrazuje informace o akcích, které GravityZone provádí automaticky, aby zmírnil hrozby a akce, které můžete provést:



- **Quarantine file** - Pomocí této akce uložíte dotyčnou položku do karantény pro zjištění jejího skutečného využití. Tato akce vyžaduje, aby byl modul Firewall nainstalován na cílovém koncovém bodě.
- **Add file to Blocklist** - Spravujte blokované položky v části Blocklist.
- **Add file as Exception** - Tuto možnost použijte, chcete-li vyloučit danou aktivitu z konkrétní politiky. Pokud zvolíte tuto akci, v konfiguračním okně se zobrazí výzva k výběru politiky, do které chcete přidat výjimku. Spravujte si vyjímky v **Politiky (Policies) > Antimalware > Nastavení (Settings)**.
- **Přidat jako výjimku EDR** - Pomocí této možnosti vytvoříte vlastní pravidlo, které již nebude soubor považovat za podezřelou nebo škodlivou detekci EDR.

  1. Když kliknete na tlačítko **Přidat jako výjimku EDR** , objeví se nové okno s výzvou k potvrzení akce nebo k jejímu zrušení.

2. Po potvrzení akce vás GravityZone upozorní, že nové pravidlo je k dispozici v tabulce Pravidla pro výjimky . Všimněte si, že název všech pravidel vytvořených v grafu incidentu začíná číslem incidentu.

Poznámka
Když přejdete do podrobností pravidla, abyste je upravili, všimnete si, že všechna kritéria pro toto pravidlo byla vyplněna automaticky a bylo přidáno kritérium jen pro čtení s názvem výstrahy.

Důležité
Funkce **Přidat jako výjimku EDR** je k dispozici pouze pro:

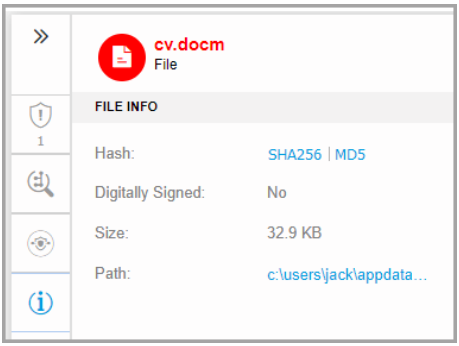
- upozornění vyvolaná technologií EDR
- uzly vytvořené jiným procesem
- podezřelé a škodlivé uzly

Pokud je vyloučený soubor součástí kritické cesty incidentu, nebudou budoucí incidenty odpovídající tomuto kritériu vyloučení již generovány v síti incidentů. Pokud vyloučený soubor není součástí kritické cesty incidentu, budou budoucí incidenty odpovídající tomuto kritériu vyloučení stále generovány v tabulce Incidenty, ale nebudou tento proces nadále považovat za podezřelý nebo škodlivý.

Tato část také obsahuje podrobná doporučení pro každou výstrahu detekovanou ve vybraném uzlu, která vám pomůže při zmírnění incidentu a zvýšení úrovně zabezpečení vašeho prostředí.

- **INFORMACE O SOUBORU**

  Zobrazuje podrobnosti o vybraném uzlu souboru, včetně původu a cesty souboru, hodnoty hash nebo digitálního podpisu.



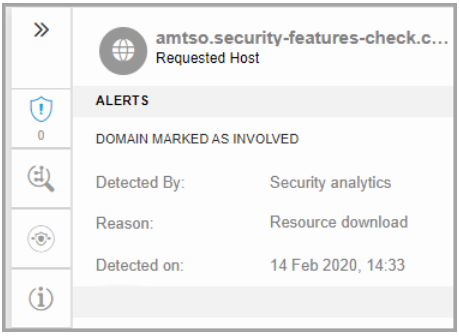
Hodnotu hash můžete zkopírovat do schránky kliknutím na dostupné algoritmy hashování v poli **Hash** a poté **Kopírovat do schránky** a použít ji k přidání hodnoty hashe souboru do **Blocklistu** . Pro více informací si přečtěte **Seznam blokovaných souborů (Blocklisting Files)**.

Panel podrobností pro uzly domén

Panel **Podrobnosti o uzlu** pro uzly domény obsahuje čtyři kategorie:

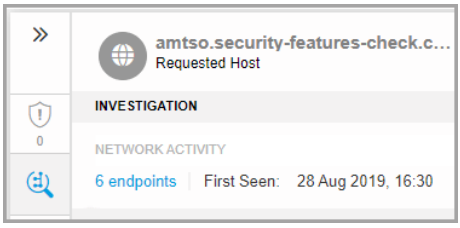
- **UPOZORNĚNÍ**

  Zobrazuje závažnost domény označenou technologií Bitdefender, která zahrnovala tuto entitu do incidentu, důvod, který spustil detekci, a datum, kdy byla detekována.

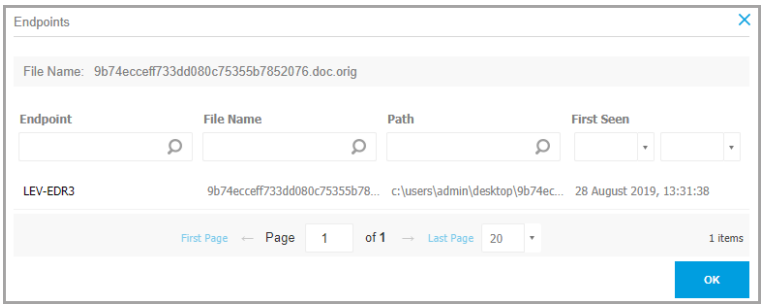


- **KONTROLA**

Zobrazuje datová razítka pro počáteční detekci a všechny koncové body, kde byl tento prvek spatřen.

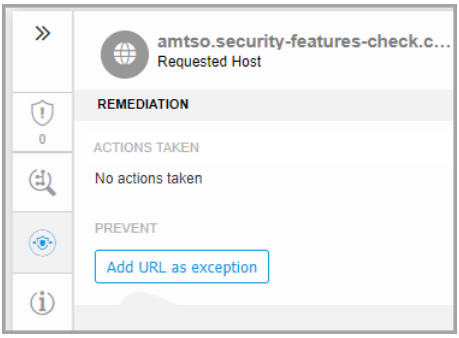


Chcete-li zobrazit tento seznam, klikněte na číslo zobrazené v poli **koncové body** a objeví se nové okno.



- **NÁPRAVA**

  Zobrazuje informace o akcích, které GravityZone provádí automaticky, aby zmírnil hrozby a akce, které můžete provést:



- **Add URL as Exception** - Tuto možnost použijte, chcete-li vyloučit danou aktivitu z konkrétní politiky. Pokud zvolíte tuto akci, v konfiguračním okně se zobrazí výzva k výběru politiky, do které chcete přidat výjimku. Spravujte si vyjímky v **Politiky (Policies) > Antimalware > Nastavení (Settings)**.
- **Přidat jako výjimku EDR** - Pomocí této možnosti vytvoříte vlastní pravidlo, které již nebude považovat doménu za podezřelou nebo škodlivou detekci EDR.

  1. Když kliknete na tlačítko **Přidat jako výjimku EDR** , objeví se nové okno s výzvou k potvrzení akce nebo k jejímu zrušení.
  2. Po potvrzení akce vás GravityZone upozorní, že nové pravidlo je k dispozici v tabulce Pravidla pro výjimky . Všimněte si, že název všech pravidel vytvořených v grafu incidentu začíná číslem incidentu.

Poznámka
Když přejdete do podrobností pravidla, abyste je upravili, všimnete si, že všechna kritéria pro toto pravidlo byla vyplněna automaticky a bylo přidáno kritérium jen pro čtení s názvem výstrahy.

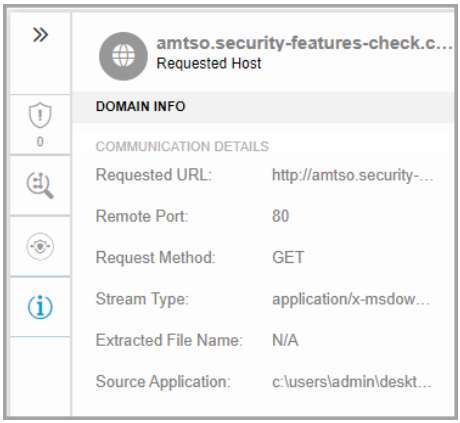
Důležité
Funkce **Přidat jako výjimku EDR** je k dispozici pouze pro:

- upozornění vyvolaná technologií EDR
- uzly vytvořené jiným procesem
- podezřelé a škodlivé uzly

Pokud je vyloučená doména součástí kritické cesty incidentu, nebudou budoucí incidenty odpovídající tomuto kritériu vyloučení již generovány v síti incidentů.
Pokud vyloučená doména není součástí kritické cesty incidentu, budou budoucí incidenty odpovídající tomuto kritériu vyloučení stále generovány v tabulce incidentů, ale nebudou tento proces nadále považovat za podezřelý nebo škodlivý.

- **INFO O DOMÉNĚ**

  Zobrazuje podrobnosti o vybraném uzlu domény, včetně požadované adresy URL, použitého portu, metody požadavku, typu datového toku, extrahovaného názvu souboru, zdrojové aplikace.

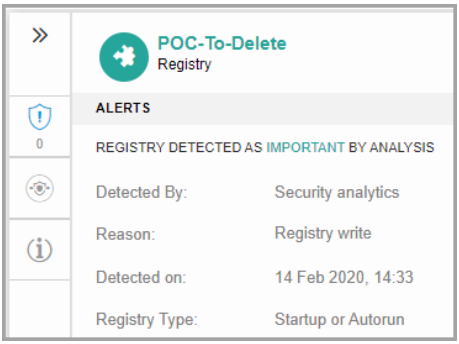


Panel Podrobnosti pro uzly registru

Panel **Podrobnosti o uzlech** pro uzly registru obsahuje tři kategorie:

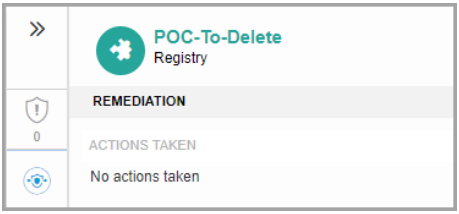
- **UPOZORNĚNÍ**

  Zobrazuje závažnost manipulace s registrem označenou technologií Bitdefender, která zahrnovala tuto entitu do incidentu, důvod, který spustil detekci, datum, kdy byla detekována, a typ registru.



- **NÁPRAVA**

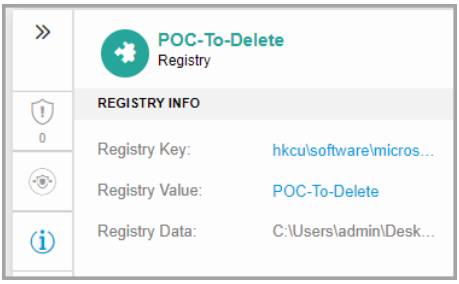
  Zobrazuje informace o akcích provedených automaticky pomocí GravityZone.



  Sekce **NÁPRAVA** pro uzly registru neposkytuje žádnou možnost akce uživatele.

- **INFO O REGISTRU**

  Zobrazuje podrobnosti o vybraném uzlu registru, včetně klíče registru, hodnoty a dat.

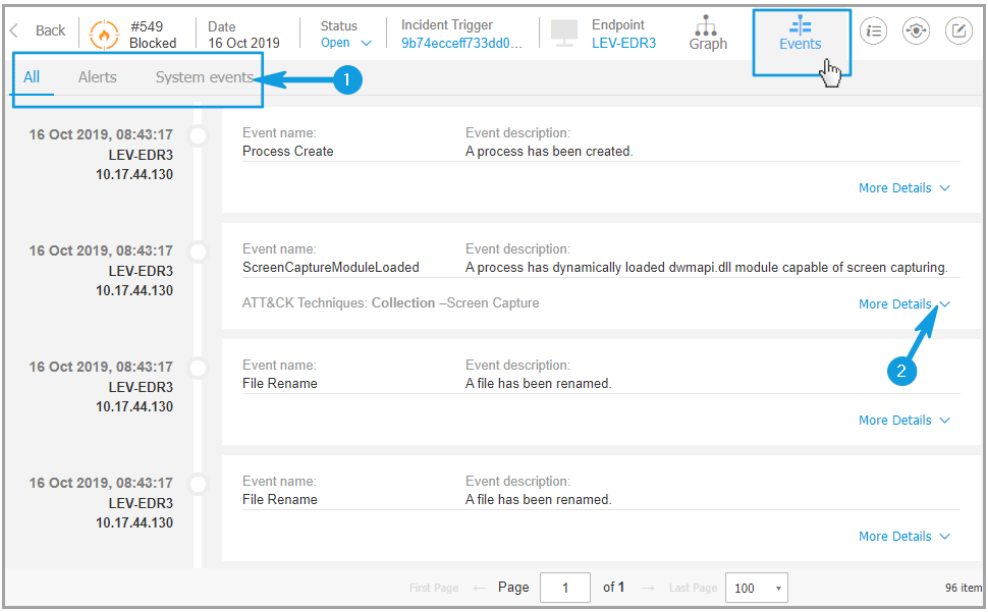


Kliknutím na klíč registru a jeho hodnotu zkopírujete do schránky pro účely další analýzy.

Události

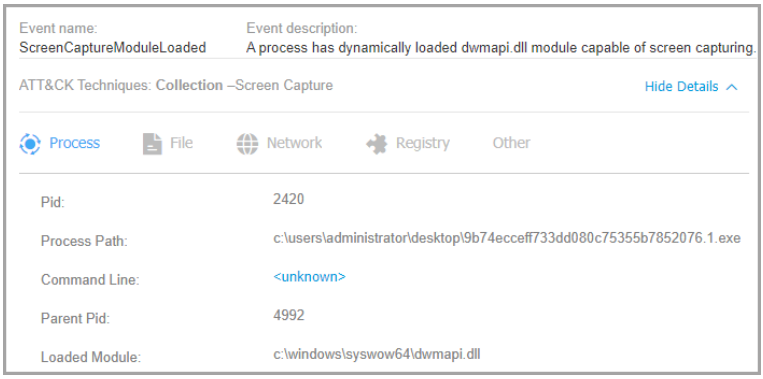
Na kartě **Events** si můžete prohlédnout, jak se odvíjí sekvence událostí od spuštění vyšetřovaného incidentu. Toto okno zobrazuje korelované systémové události a výstrahy detekované technologiemi GravityZone, jako jsou EDR, Network Attack Defense, detekce anomálií, pokročilý anti-exploit, rozhraní Windows Antimalware Scan (AMSI).

Každá komplexní událost má podrobný popis vysvětlující, co bylo detekováno a co by se mohlo stát, pokud by se artefakt používal ke škodlivým účelům, v souladu s nejnovějšími technikami a taktikou MITER.



přehled událostí

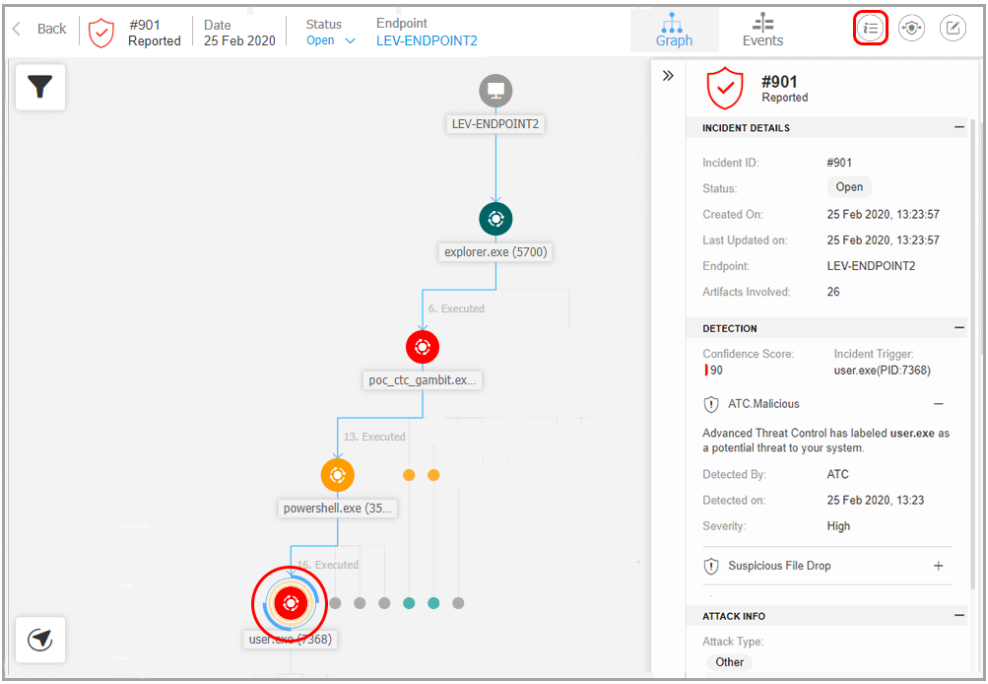
1. Použijte možnosti filtrování k zobrazení všech událostí, systémových událostí nebo komplexních událostí (upozornění).
2. Kliknutím na tlačítko **More details** rozbalíte jednotlivé události a získáte přístup k dalším informacím.



Informace o incidentu

Tento panel obsahuje sbalitelné sekce s podrobnostmi, jako je ID incidentu, aktuální stav, čas a datum, kdy byl vytvořen a naposledy aktualizován, počet zahrnutých artefaktů, název a popis spouštěče a informace o útoku.

Z této části můžete přistupovat k rozšířenému incidentu, který zahrnuje tento incident koncového bodu, pokud se jedná o případ.

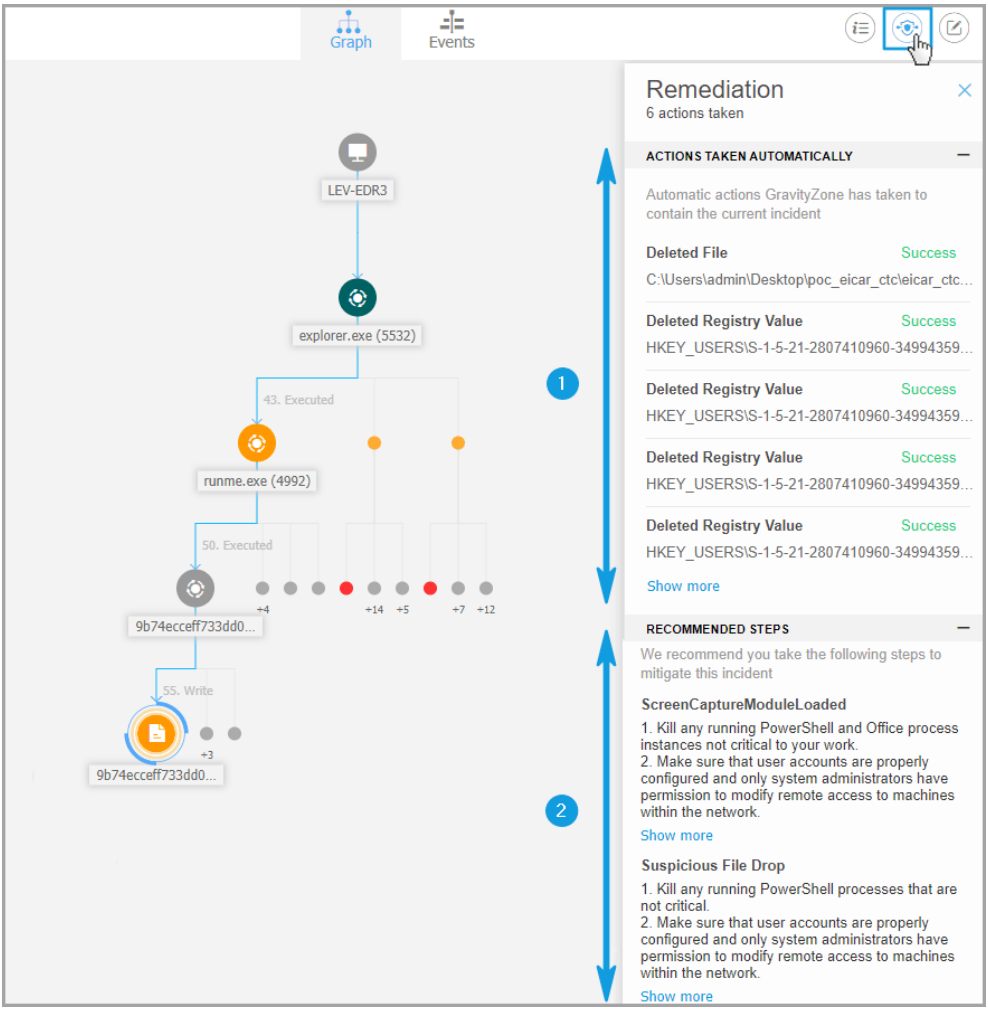


Informační panel incidentů

Panel také obsahuje upozornění zjištěná v části, která spustila incident.

Náprava

Panel **Remediation** vám poskytuje přehledné informace o tom, jaké nápravné akce byly automaticky provedeny GravityZone v případě útoků blokovaných technologií, jako je Advanced Threat Control (ATC), HyperDetect, Antimalware a doporučené kroky, které můžete podniknout, aby se incident zmírnil a zvýšila se úroveň zabezpečení vašeho systému.



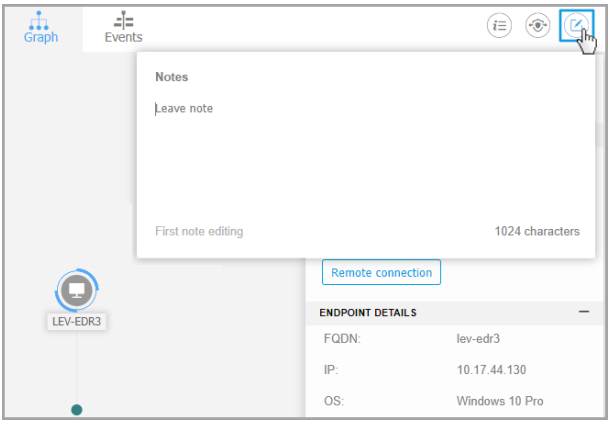
Nápravný panel

1. Akce provedené automaticky pomocí GravityZone.
2. Doporučení pro další zmírnění incidentu a zvýšení bezpečnosti.

Poznámka
Doporučené kroky odpovídají výstrahám detekovaným v uzlu, který spustil vyšetřovaný incident.

Poznámky

Sekce **Poznámky (Notes)** vám umožňuje přidávat poznámky pro sledování nedávných změn a usnadňuje změnu vlastníka incidentu.

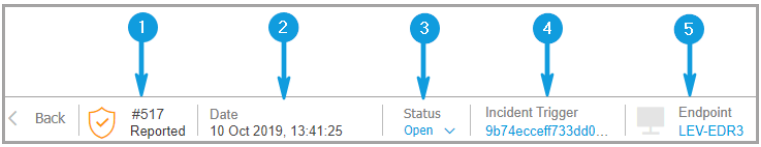


schránka poznámek

1. Pro zanechání poznámky k aktuální události, klikněte na tlačítko **Poznámky (Notes)** za účelem zobrazení nového okna.
2. Zadejte vaši zprávu do tohoto okna (maximálně 2048 znaků).

Lišta stav incidentů

Lišta stav incidentů poskytuje přehled událostí zabezpečení, které vám mohou pomoci zjistit klíčové informace o příslušných koncových bodech sítě.



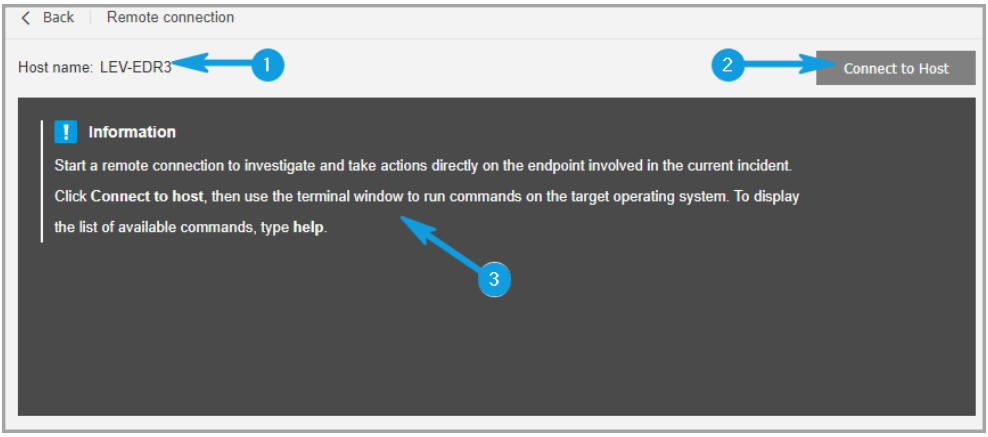
Lišta stav incidentů

1. ID incidentu - identifikační číslo vyšetřované události, a pokud je událost blokována nebo pouze nahlášena.
2. Časové razítko detekce - datum a čas spuštění incidentu.
3. Incident status - aktuální stav incidentu.
4. Spouštěč incidentů - název prvku, který incident vytvořil.
5. Koncový bod - název cílového koncového bodu.

Kliknutím na tlačítko **Zpět** se dostanete zpět na hlavní stránku **Incident**.

Vzdálené připojení

Tato karta slouží k navázání vzdáleného připojení ke koncovému bodu zapojenému do aktuálního incidentu a spuštění řady vlastních příkazů prostředí přímo v jeho operačním systému, k okamžitému zrušení hrozby nebo ke sběru dat pro další vyšetřování.



Karta Vzdálené připojení

Karta **Vzdálené připojení** obsahuje následující položky:

1. Název koncového bodu, který je součástí aktuální bezpečnostní události
2. Tlačítko pro ovládání vzdáleného připojení (připojení / odpojení)
3. Okno terminálu

Podmínky pro terminálové spojení

- Verze Bitdefender agenta instalovaného na koncovém bodu podporuje funkci vzdáleného spojení.
- Koncový bod musí být zapnutý a být online.
- Koncový bod musí mít windows OS.
- GravityZone je schopná kommunikovat s koncovým bodem.
- Váš GravityZone účet musí mít práva ke správě cílového koncového bodu.

Vytváření vzdáleného připojení

Takto funguje vzdálené připojení:

1. Spusťte živou relaci klepnutím na tlačítko **Připojit k hostiteli**

   Stav připojení se zobrazí vedle názvu koncového bodu.

   Pokud se spojení nezdaří, zobrazí se v terminálovém okně chybové hlášení

   Poznámka
   Současně můžete otevřít maximálně pět relací terminálu se stejným koncovým bodem.

2. Po připojení terminál zobrazí seznam dostupných příkazů a jejich popis. Zadejte požadovaný příkaz do okna terminálu následovaného klávesou `Enter`.

   Chcete-li se dozvědět více o příkazu, zadejte `help` následovaný názvem příkazu (například `help ps`).

3. Terminál zobrazí výstup příkazu, pokud je příkaz úspěšný.

   Pokud koncový bod nedokončí provedení příkazu v daném čase, příkaz bude vyřazen.

   Do terminálového okna se zapíše historie příkazů. Můžete však zobrazit dříve zadané příkazy stisknutím kláves se šipkami.

4. Chcete-li připojení ukončit, klepněte na tlačítko **Ukončit relaci** .

   Konec relace vyprší automaticky po pěti minutách nečinnosti.

   Navigace mimo štítek **Vzdálené spojení** během spojení s koncovým bodem také zruší terminálové spojení.

Příkazy Terminálového spojení

EDR příkazy terminálového spojení jsou vlastní upravené shell příkazy, nezávislé na platformě, používající generickou syntaxi. Níže naleznete seznam dostupných příkazů které můžete používat na koncových bodech během terminálového spojení:

- `ps`
  - **Popis (Description)**: Zobrazí informace o aktuálně běžících procesech na cílovém koncovém bodu, jakožto je process ID (PID), jméno, cesta nebo utilizace paměti.
  - **Syntaxa**: `ps`
  - **Aliasy**: `seznam úkolů`
  - **Parametry**: -
- `kill`
  - **Popis (Description)**: Terminuje běžící process nebo aplikaci na cílovém koncovém bodu pomocí jeho PID. K získání PID použijte příkaz `ps/tasklist`.
  - **Syntax**: `kill [PID]`
  - **Aliasy**: -
  - **Parametry**: `[PID]` - ID procesu z cílového koncového bodu.
- `ls (dir)`
  - **Popis**: Zobrazí informace o všech souborech a složkách ze zadaného adresáře, například název, typ, velikost a datum změny. Umožňuje specifikovat cestu pomocí zástupných znaků. Například:

    `C:\Users\admin\Desktop\s*` veškerý obsah plochy začínající na "s"

    `C:\Users\publ??` zobrazí seznam všech zadaných cest s posledními dvěma písmeny.

- **Syntaxa**: `ls [path]`
- **Aliasy**: `dir`
- **Parametry**: `[Path]` - cesta k souboru nebo složce v cílovém koncovém bodu.

- `rm (del, smazat)`
  - **Popis**: Odstraní soubory a složky ze zadané cesty v cílovém koncovém bodu.
  - **Syntaxa**: `rm [path]`
  - **Aliasy**: `del/smazat`
  - **Parametry**: `[Path]` - cesta k souboru nebo složce v cílovém koncovém bodu.
- `reg query`
  - **Popis**: Vrátí všechny informace (název, typ a hodnotu) pro zadanou cestu klíče registru.
  - **Syntax**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Aliasy**: -
  - **Parametry**:
    - `keypath`- Vrátí všechny informace klíčů registru ze zadané cesty.
    - `/k [keyname]` - filtruje výsledky klíčů registru podle specifického názvu klíče. Můžete také použít zástupné znaky (*,?) Pro filtrování širšího rozsahu názvů.
    - `/v [valuename]` - filtruje hodnoty registru podle specifického názvu hodnoty. V názvu hodnoty můžete také použít zástupné znaky (*,?) Pro filtrování širšího rozsahu názvů.
- `reg add`
  - **Popis**: Přidá nový klíč registru nebo hodnotu. Pokud již existuje, přepíše hodnotu registru Při přepisování informací o registru musíte zadat všechny definované parametry.
  - **Syntaxa**: `reg přidat [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Aliasy**: -

- **Parametry**:
  - `[keyname]` - název klíče registru.
  - `/v [valuename]` - název hodnoty registru. To také vyžaduje přidání alespoň /d [data] parametru.
  - `/t [datatype]` - datový typ hodnoty registru. Můžete přidat jeden z následujících datových typů:

    `REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY, REG_DWORD_LITTLE_ENDIAN, REG_LINK, REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`

    Pokud není specifikováno, je typ `REG_SZ` přiřazen standardně.

    Když je typ nastaven na `REG_BINARY`, data registru jsou interpretována jako hexadecimální hodnoty.

- `reg smazat`
  - **Description**: Odstraní klíč registru nebo jeho hodnoty.
  - **Syntaxe**:

    ```
    reg smazat [keyname] [/v] [valuename]
    ```

    ```
    reg smazat [keyname] [/va]
    ```

  - **Aliasy**: -
  - **Parametry**:

    `[keyname]` - odstraní klíč registru a všechny jeho hodnoty.

    `/v [valuename]` - odstraní zadanou hodnotu registru.

    `/va` - odstraní všechny hodnoty zadaného klíče registru.

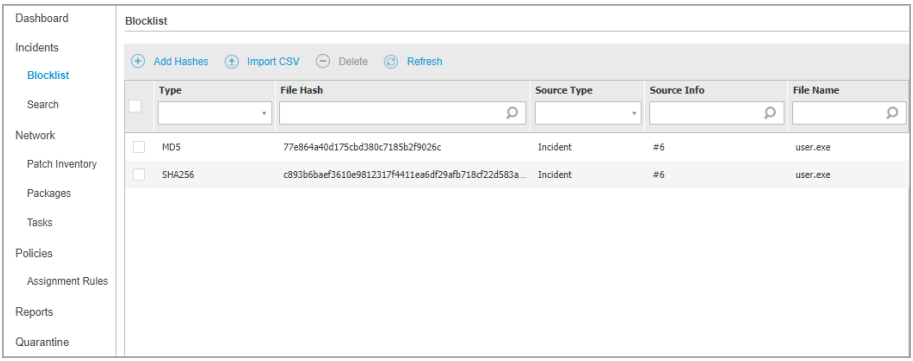
- `cd`
  - **Popis**: Mění pracovní adresu v adresáře na vámi specifikovanou. Tento příkaz potřebuje mít cestu adresáře k síťovému disku nebo složce specifikovanou jako parametr z cílového koncového bodu.
  - **Syntaxa**: `cd [path]`
  - **Aliasy**: -

  - **Parametry**: `[Path]` - cesta k souboru nebo složce v cílovém koncovém bodu.

- `pomoc`
  - **Popis**: Bez určení parametru nápověda zobrazí seznam všech dostupných příkazů spolu s krátkým popisem. Při zadávání nápovědy následované parametrem se zobrazí úplná syntaxe tohoto příkazu, krátký popis a příklad použití.
  - **Syntaxa**: `help [command]`
  - **Aliasy**: -
  - **Parametry** název příkazu (například: `cd, kill, ls, ps`)
- `clear (cls)`
  - **Popis**: Vymaže okno terminálu a zobrazí výzvu s aktuální pracovní složkou.
  - **Syntaxa**: `vyčistit`
  - **Aliasy**: `cls`
  - **Parametry**: -

9.2. Přidání na seznam blokovaných souborů (Blocklisting Files)

Na stránce **Seznam blokovaných (Blocklist)** si můžete zobrazit a spravovat položky bodle jejich hodnot. Prohlížet záznamy aktivit v Záznam aktivity uživatelů (User Activity Log).



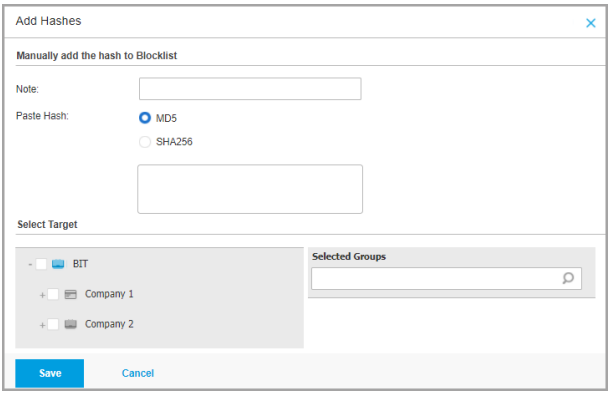
Stránka seznamu blokovaných (Blocklist page)

V tabulce dat můžete vidět následující detaily ke každé položce:

- Typ souborů (File type):
  - MD5
  - SHA256
- Hodnota hash souboru (File Hash Value)
- Druh zdroje (Source Type):
  - Incident
  - Import
  - Manuální
- Zdrojové informace
- Název souboru
- Společnost

Přidejte hodnoty hash do existujícího seznamu blokovaých:

1. Zkopírujte hodnotu hash z **Informace o souboru (File Info)**.
2. Vyberte si z **MD5** nebo **SHA256** a vložte hodnotu do tabulky níže. Přidejte poznámku pokud je to potřeba.
3. Klikněte na tlačítko **Save**.



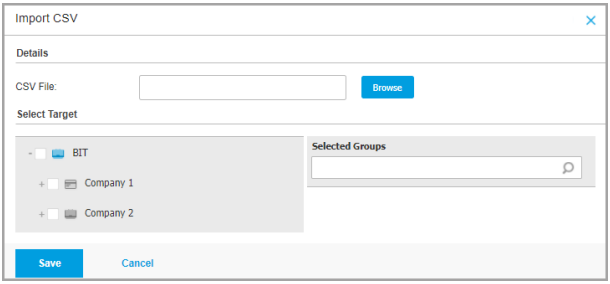
Přidejte okno hodnoty hash

Důležité

Incident Senzor blokuje spustitelný soubor, jehož hodnota hash byla přidána do **Blocklist** , od zahájení procesu.

Naimportuje záznamy hash do existujícího seznamu blokovaných. Pro import CSV souboru:

1. Klikněte na **Import CSV**.
2. Vyberte váš CSV soubor a klikněte na **Uložit (Save)**.



Okno importu CSV

Můžete také importovat místní soubory CSV ze svého zařízení na záložku **Blocklist**, nejdřív se však musíte ujistit, že je váš soubor CSV platný.

Chcete-li vytvořit platný soubor CSV pro import, musíte naplnit první tři sloupce těmito údaji:

1. První sloupec souboru CSV musí obsahovat typ hash: buď `md5` nebo `sha256` .
2. Druhý sloupec musí obsahovat odpovídající hexadecimální hodnoty hash.
3. Třetí sloupec může obsahovat volitelné informace související se sloupcem **Source Info** na stránce **Blocklist**.

Poznámka
Odpovídající informace z dalších sloupců v záložce **Blocklist** budou automaticky vyplněny při importu souboru CSV.

9.3. Vlastní Pravidla

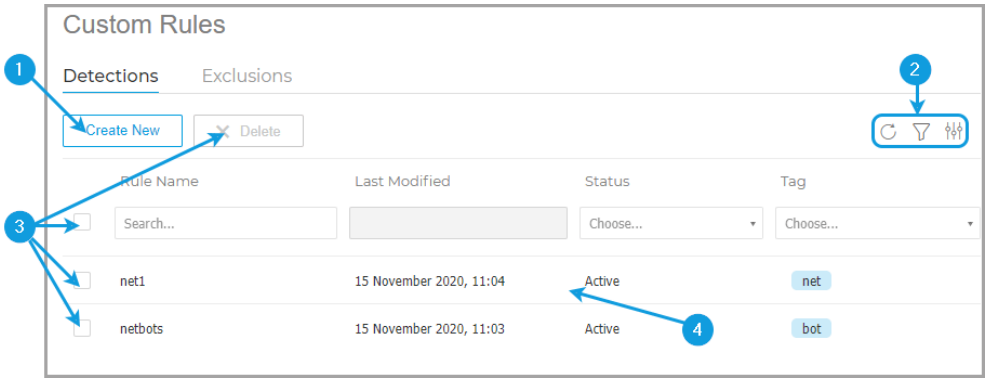
Stránka **Vlastní pravidla** poskytuje rámec pro vytváření a správu vlastních pravidel pro zahrnutí nebo vyloučení konkrétního chování ze spouštění incidentů.

Tato funkce EDR zahrnuje dvě hlavní kategorie:

- Detekce
- Výjimky

9.3.1. Detekce

Karta **Detekce** poskytuje rámec pro vytváření a správu vlastních pravidel detekce, označení konkrétního chování z vašeho prostředí jako platnou detekci a generování odpovídajících incidentů na stránce Incidenty.



Karta Detekce

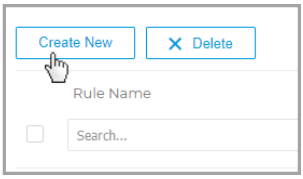
1. Kliknutím na tlačítko **Vytvořit nové** vytvoříte nové vlastní pravidlo detekce. Další podrobnosti najdete v části Vytvořit vlastní pravidla detekce .
2. K přizpůsobení mřížky použijte tato akční tlačítka:
   - Kliknutím na tlačítko **Zobrazit/skrýt sloupce** přidejte nebo odeberte sloupce filtru.

     Stránka se automaticky aktualizuje a načte karty s informacemi odpovídajícími přidaným sloupcům.

     Sloupce filtru můžete kdykoli resetovat pomocí tlačítka **Reset** uvnitř rozbalovací nabídky **Zobrazit/skrýt sloupce** .
   - Kliknutím na tlačítko **Zobrazit/skrýt filtry** zobrazíte nebo skryjete panel filtrů.
   - Seznam aktualizujte kliknutím na tlačítko **Obnovit** .
3. Vyberte globální zaškrtávací políčko nebo jednotlivá pole pravidel, která chcete vybrat, a kliknutím na **Odstranit** je odeberte ze seznamu.
4. Kliknutím na pravidlo v seznamu rozbalte jeho panel podrobností, zobrazte podrobnosti pravidla a v případě potřeby jej aktualizujte nebo odstraňte. Další informace najdete na panelu podrobností pravidla detekce .

Vytvořte vlastní pravidla detekce

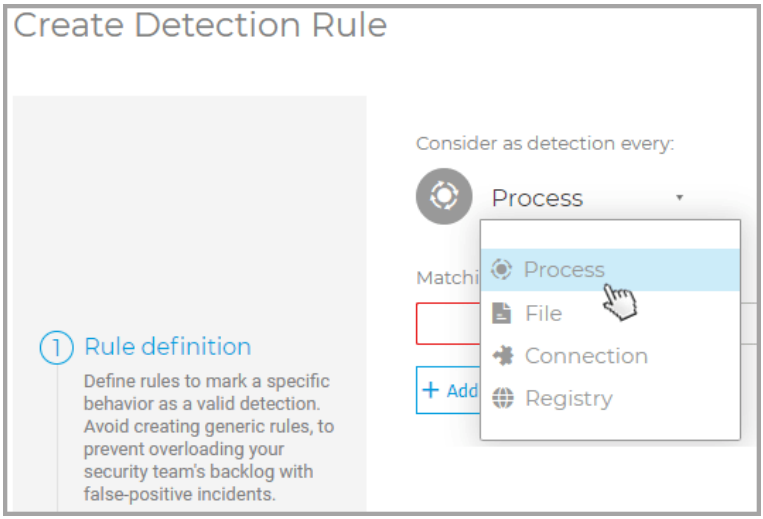
Chcete-li vytvořit vlastní pravidlo detekce, klikněte na tlačítko **Vytvořit nové** .



Vytvořte nové pravidlo detekce

Dostanete se do okna **Vytvořit pravidlo detekce** v části **Definice pravidla** , kde můžete začít upravovat pravidlo:

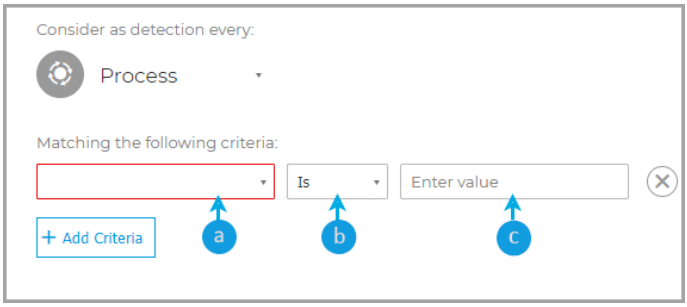
1. Vyberte, jaký typ prvku chcete zahrnout do pravidla vyloučení.



Můžete si vybrat z:

- Proces
- Soubor
- Připojení
- Registr

2. Každý typ prvku má specifická kritéria shody, která si můžete vybrat z rozbalovací nabídky:



a. Vyberte jednu z dostupných možností kritérií.

b. Vyberte typ vztahu mezi kritérii shody a jeho hodnotou:

- **Je** - bude zahrnovat všechny incidenty s prvky, které odpovídají přesné hodnotě zadané v poli hodnoty.
- **Obsahuje** - bude zahrnovat všechny incidenty s prvky, které obsahují hodnotu zadanou v poli hodnoty (například zástupné znaky, přípony souborů atd.).

  Důležité
  Použití zástupných znaků při vytváření pravidla detekce zvyšuje riziko, že bude příliš obecné, čímž se zvýší možnost přetékání nevyřízených položek vaší práce s falešně pozitivními incidenty.

- **Je jedním z** - bude zahrnovat všechny incidenty s prvky, které odpovídají jedné z hodnot zadaných v poli hodnoty (je použit operátor **OR** mezi zadanými hodnotami).

c. Zadejte konkrétní hodnotu pro každé kritérium.

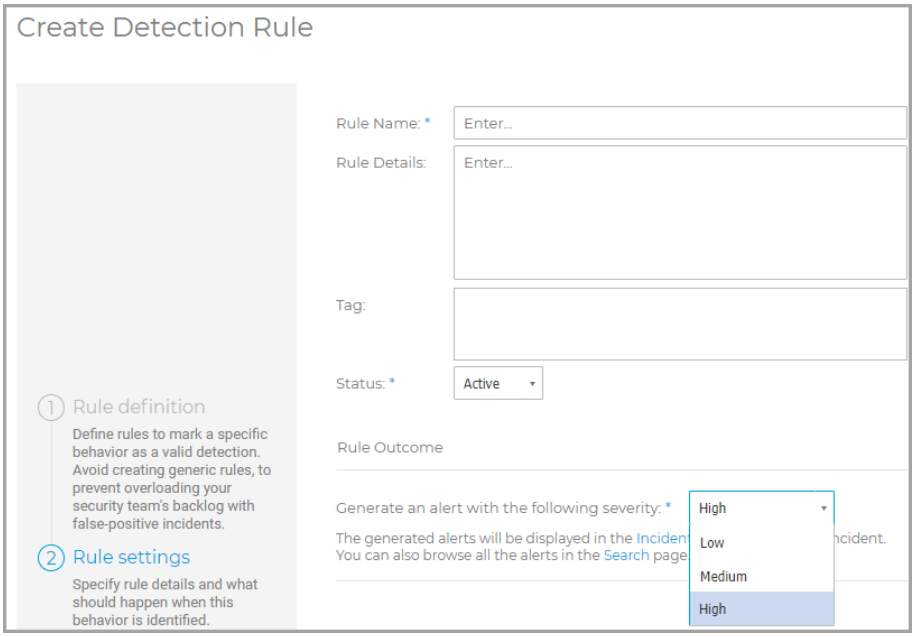
  Poznámka
  Při zadávání více hodnot pro kritérium (při použití podmínky **Je jedna z**) musíte stisknout klávesu **Enter** za každou hodnotu pro dokončení akce.

3. Pomocí **Přidat kritéria** přidejte do pravidla nová kritéria.

Poznámka
Pravidlo spustí incidenty, které zahrnují všechna definovaná kritéria (operátor **AND** je použit mezi přidanými více kritérii).

4. Po definování všech kritérií klikněte na **Další krok** .

   Dostanete se do sekce **Nastavení pravidel** , kde musíte vyplnit podrobnosti pravidla.



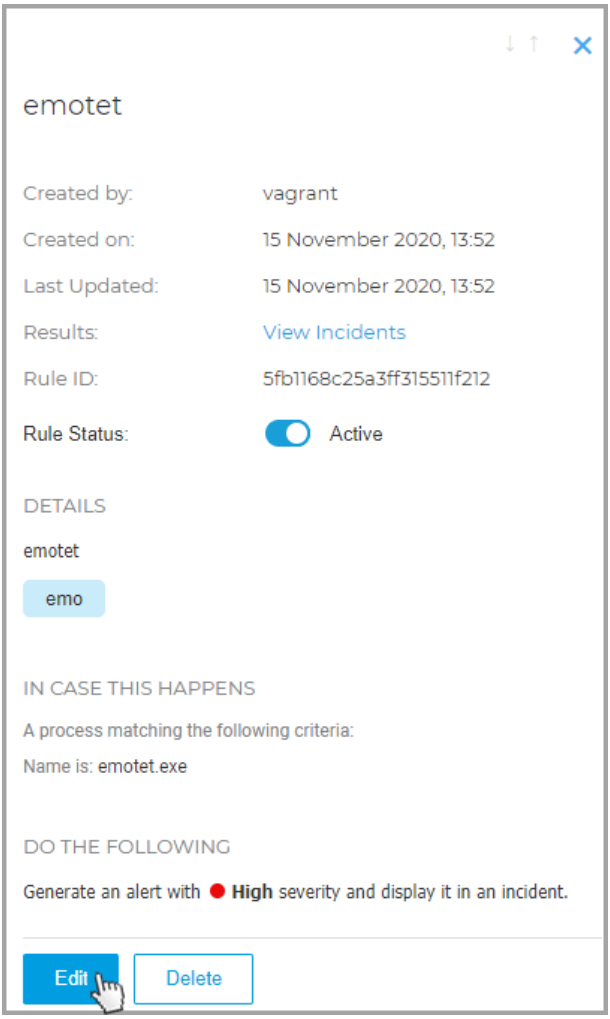
5. Pojmenujte nové pravidlo do pole **Název pravidla** . Toto pole je povinné.
6. Do textové oblasti **Podrobnosti pravidla** přidejte stručný popis pravidla.
7. Přidejte značky specifické pro toto pravidlo do pole **Značka** , což usnadní seskupování a správu pravidel.
8. V rozbalovací nabídce **Stav** nastavte stav pravidla na Aktivní nebo Neaktivní.
9. Z rozevírací nabídky nastavte závažnost výstrah spouštěných tímto pravidlem na Nízká / Střední / Vysoká.

10. Kliknutím na **Vytvořit pravidlo** dokončete vytváření vlastního pravidla výjimky.

    Nové pravidlo je k dispozici na kartě **Detekce** .

Panel podrobností pravidla detekce

Panel **Podrobnosti pravidla** obsahuje podrobné informace o vybraném pravidle, včetně data vytvoření a kdo ho vytvořil, data, kdy bylo naposledy aktualizováno, jedinečného ID a stavu a také odkaz na seznam událostí odpovídajících kritériím pravidel. Zahrnuje také popis pravidla, přidružené značky, zahrnutá kritéria shody a výsledek pravidla.

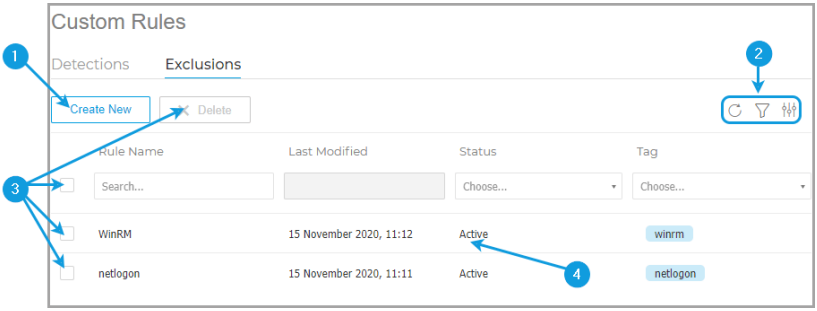


Panel podrobností pravidel

- Kliknutím na **Upravit** přejděte do okna **Vytvořit pravidlo detekce** , kde můžete aktualizovat definici pravidla.
- Klepnutím na **Odstranit** odstraníte pravidlo výjimky ze seznamu.

9.3.2. Výjimky

Karta **Výjimky** vám poskytuje rámec pro vytváření a správu vlastních pravidel výjimek, která vylučují případy, které považujete za irelevantní pro vaši organizaci a které by jinak EDR označil. na stránce Incidenty .



Karta Výjimek

1. Kliknutím na tlačítko **Vytvořit nové** vytvoříte nové vlastní pravidlo výjimky. Další podrobnosti naleznete v části Vytvořit vlastní pravidla pro výjimky .

   Alternativně můžete vždy vytvořit pravidlo přímo z grafu dopadu tak, že vyberete cílový uzel a přidáte jej jako výjimku z panelu jeho postranních údajů. Další podrobnosti naleznete ve funkci Přidat jako výjimku EDR .

2. K přizpůsobení mřížky použijte tato akční tlačítka:

   - Kliknutím na tlačítko **Zobrazit/skrýt sloupce** přidejte nebo odeberte sloupce filtru.

     Stránka se automaticky aktualizuje a načte karty s informacemi odpovídajícími přidaným sloupcům.

     Sloupce filtru můžete kdykoli resetovat pomocí tlačítka **Reset** uvnitř rozbalovací nabídky **Zobrazit/skrýt sloupce** .

   - Kliknutím na tlačítko **Zobrazit/skrýt filtry** zobrazíte nebo skryjete panel filtrů.

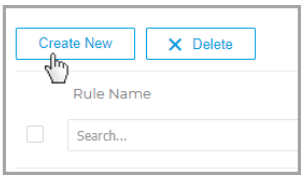
   - Seznam aktualizujte kliknutím na tlačítko **Obnovit** .

3. Vyberte globální zaškrtávací políčko nebo jednotlivá pole pravidel, která chcete vybrat, a kliknutím na **Odstranit** je odeberte ze seznamu.

4. Kliknutím na pravidlo v seznamu rozbalte jeho panel podrobností, zobrazte podrobnosti pravidla a v případě potřeby jej aktualizujte nebo odstraňte. Další informace najdete na panelu podrobností pravidla výjimky .

Vytvořte vlastní pravidla pro výjimky

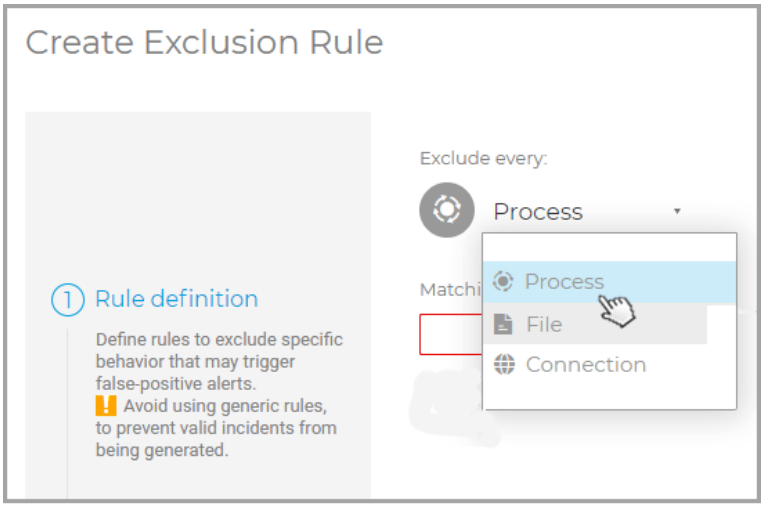
Chcete-li vytvořit vlastní pravidlo výjimek, klikněte na kartě **Výjimek** na tlačítko **Vytvořit nové** .



Vytvořte nové pravidlo výjimky

Zobrazí se stránka **Vytvořit pravidlo výjimky** v části **Definice pravidla** , kde můžete začít upravovat pravidlo:

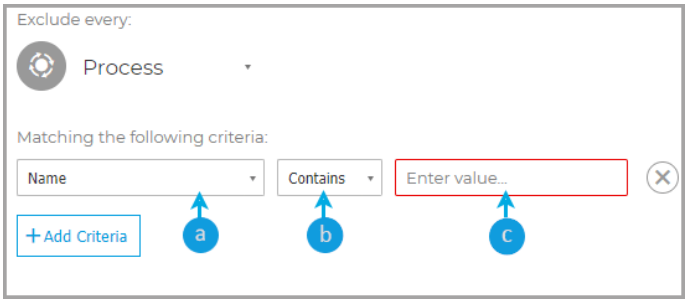
1. Vyberte, jaký typ prvku chcete zahrnout do pravidla vyloučení.



Můžete si vybrat z:

- Proces
- Soubor
- Připojení

2. Každý typ prvku má specifická kritéria shody, která si můžete vybrat z rozbalovací nabídky:



a. Vyberte jednu z dostupných možností kritérií.

b. Vyberte typ vztahu mezi kritérii shody a jeho hodnotou:

- **Je** - vyloučí všechny incidenty s prvky, které odpovídají přesné hodnotě zadané do pole hodnoty.
- **Obsahuje** - vyloučí všechny incidenty s prvky, které obsahují hodnotu zadanou v poli hodnota (například zástupné znaky, přípony souborů atd.).

  Důležité
  Použití zástupných znaků při vytváření pravidla vyloučení zvyšuje riziko, že je příliš obecný, čímž se zvyšuje možnost ignorovat skutečné hrozby a zvýšit zranitelnost vaší společnosti.

- **Je jedním z** - vyloučí všechny incidenty s prvky, které odpovídají jedné z hodnot zadaných do hodnotového pole (je použit operátor **NEBO**) mezi zadanými hodnotami).

c. Zadejte konkrétní hodnotu pro každé kritérium.

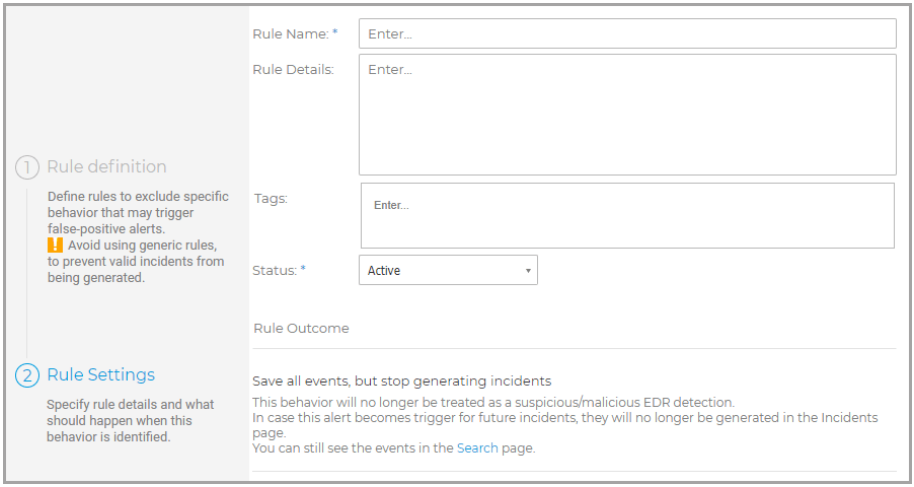
Poznámka
Při zadávání více hodnot pro kritérium (při použití podmínky **Je jedna z**) musíte stisknout klávesu **Enter** za každou hodnotu pro dokončení akce.

3. Pomocí **Přidat kritéria** přidejte do pravidla nová kritéria.

Poznámka
Pravidlo vyloučí incidenty, které zahrnují všechna definovaná kritéria (mezi více přidanými kritérii se použije operátor **A**).

4. Po definování všech kritérií klikněte na **Další krok** .

   Dostanete se do části **Nastavení pravidel** , kde musíte vyplnit podrobnosti pravidla.

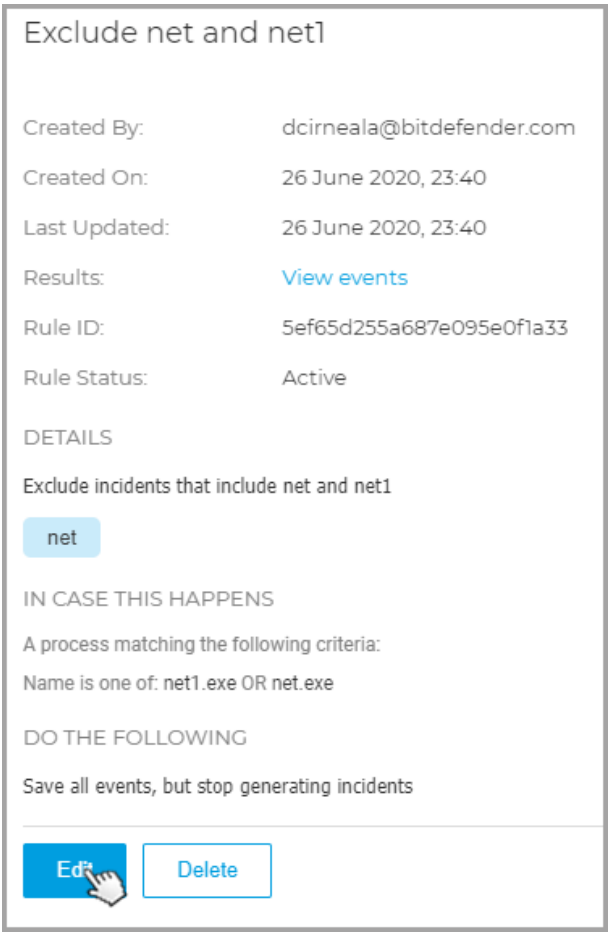


5. Pojmenujte nové pravidlo do pole **Název pravidla** . Toto pole je povinné.
6. Do textové oblasti **Podrobnosti pravidla** přidejte stručný popis pravidla.
7. Přidejte značky specifické pro toto pravidlo do pole **Značka** , což usnadní seskupování a správu pravidel.
8. V rozbalovací nabídce *Stav* nastavte stav pravidla na Aktivní nebo Neaktivní.
9. Kliknutím na **Vytvořit pravidlo** dokončete vytváření vlastního pravidla výjimky.

   Nové pravidlo je k dispozici na stránce **Pravidla pro výjimky** .

Panel Pravidel podrobností výjimek

Panel **Podrobnosti pravidla** obsahuje podrobné informace o vybraném pravidle, včetně data vytvoření a kdo ho vytvořil, data, kdy bylo naposledy aktualizováno, jedinečného ID a stavu a také odkaz na seznam událostí odpovídajících kritériím pravidel. Zahrnuje také popis pravidla, přidružené značky, zahrnutá kritéria shody a výsledek pravidla.



Panel podrobností pravidel

- Kliknutím na **Upravit** přejdete na stránku **Vytvořit pravidlo výjimky** , kde můžete aktualizovat definici pravidla.
- Klepnutím na **Odstranit** odstraníte pravidlo výjimky ze seznamu.

10. POUŽÍVÁNÍ HLÁŠENÍ

Control Center vám umožňuje tvořit a prohlížet centralizovaná hlášení ohledně stavu zabezpečení spravovaných síťových objektů. Hlášení mohou být použita pro různé účely, například:

- Monitorování a zajištění souladu s bezpečnostními zásadami společnosti.
- Kontrola a hodnocení stavu zabezpečení sítě.
- Identifikace problémů se zabezpečením sítě, hrozeb a zranitelností.
- Sledování bezpečnostních incidentů.
- Poskytuje vyššímu vedení snadno interpretovatelné údaje ohledně zabezpečení sítě.

K dispozici je několik různých typů, takže můžete snadno získat potřebné informace. Informace jsou podány ve snadno čitelných interaktivních grafech a tabulkách, umožňujících rychlou kontrolu stavu zabezpečení sítě a identifikaci bezpečnostních problémů.

Hlášení mohou sjednocovat data z celé sítě spravovaných síťových objektů, nebo pouze ze specifických skupin. Tímto způsobem můžete z jediného hlášení zjistit následující:

- Statistické údaje ohledně všech spravovaných síťových objektů, nebo jejich skupin.
- Podrobné informace o každém spravovaném objektu v síti.
- Seznam počítačů, které odpovídají určitým kritériím (například ty, které mají vypnutou antimalwarovou ochranu).

Některá hlášení také umožňují rychlou opravu problémů nalezených ve vaší síti. Například můžete snadno aktualizovat všechny cílové síťové objekty přímo z hlášení, aniž byste museli spouštět aktualizační úlohu na stránce **Síť**.

Všechny naplánovaná hlášení jsou k dispozici v Control Center, ale můžete si je uložit do počítače nebo je poslat na email.

Dostupné formáty zahrnují Přenosný formát dokumentů (PDF) a hodnoty oddělené čárkou (CSV).

10.1. Typy hlášení

Pro každý typ koncového bodu jsou dostupné různé typy hlášení:

- Hlášení pro počítače a virtuální stroje
- Hlášení Exchange

- Hlášení mobilních zařízení

10.1.1. Hlášení pro počítače a virtuální stroje

Toto jsou dostupné typy hlášení pro fyzické a virtuální stroje:

Antiphishingová činnost

Informují vás o aktivitě modulu Antiphishing v Bitdefender Endpoint Security Tools. Na zvolených koncových bodech můžete prohlížet počet blokovaných phishingových stránek a uživatele, který byl přihlášený v době poslední detekce. Kliknutím na odkazy ve sloupci **Blokované webové stránky** můžete prohlížet také URL webových stránek, kolikrát byly blokovány a kdy k poslednímu blokování došlo.

Blokované aplikace

Informuje vás o činnosti následujících modulů: Antimalware, Firewall, Kontrola obsahu, Kontrola aplikací,Advanced Anti-Exploit, ATC/IDS a HVI. Na zvolených koncových bodech můžete prohlížet počet blokovaných aplikací a uživatele, který byl přihlášený v době poslední detekce.

Klikněte na číslo přiřazené k cíli pro zobrazení doplňkových informací k blokovaným aplikacím, počtu proběhlých událostí a data a času posledního zablokování.

V tomto hlášení můžete vydat rychlý příkaz ochranným modulům pro povolení zvolené aplikace ve spuštění se na cílovém koncovém bodě:

- Klikněte na tlačítko **Přidat výjimku** pro definování výjimek v následujících modulech: Antimalware, ATC, Kontrola obsahu, Firewall a HVI. Zobrazí se potvrzovací okno informující o novém pravidle, které změní současné zásady na tom konkrétním koncovém bodě.
- Klikněte na tlačítko **Přidat pravidlo** pro definování pravidla pro aplikaci nebo proces v Kontrole aplikací. V konfiguračním okně přidejte pravidlo k existující zásadě. Zpráva vás upozorní na nové pravidlo, které změní zásady přiřazené k tomu danému koncovému zařízení. V hlášení uvidíte také počet pokusů o přístup a zda modul pracoval v Testovacím, nebo Produkčním režimu.

Zablokované webové stránky

Informují vás o činnosti modulu Kontrola webu v Bitdefender Endpoint Security Tools. Pro každý cíl můžete prohlížet počet blokovaných webových stránek. Kliknutím na toto číslo můžete prohlížet doplňující informace, jako jsou:

- URL a kategorie webové stránky

- Počet pokusů o přístupu na stránku
- Datum a čas posledního pokusu a také uživatele, který byl přihlášen v době detekce.
- Důvod zablokování, který zahrnuje plánovaný přístup, malwarovou detekci, filtrování kategorií a blacklisting.

Ochrana dat

Informují vás o činnosti modulu Ochrana dat v Bitdefender Endpoint Security Tools. Na zvolených koncových bodech můžete prohlížet počet blokovaných emailů a webových stránek a uživatele, který byl přihlášený v době poslední detekce.

Činnost Kontroly zařízení

Informuje vás o událostech, ke kterým došlo při přístupu ke koncovým bodům skrze monitorovaná zařízení. Pro každý koncový bod můžete zobrazit počet povolených / zablokovaných přístupů, včetně událostí s přístupem pouze pro čtení. Pokud k nějakým událostem došlo, kliknutím na odpovídající čísla zpřístupníte doplňující informace. Podrobnosti odkazují na:

- Uživatel přihlášený ke stroji
- Typ a ID zařízení
- Prodejce a produktové ID zařízení
- Datum a čas události

Stav šifrování koncového bodu

Poskytuje údaje ohledně stavu šifrování na koncových bodech. Koláčový graf ukazuje počet strojů, které jsou, případně nejsou, v souladu s nastavením zásad šifrování.

Tabulka pod koláčovým grafem dodává podrobnosti jako:

- Název koncového bodu.
- Plně oprávněné jméno domény (FQDN).
- IP stroje.
- Operační systém.
- V souladu se zásadami pro zařízení:
  - **Vyhovující** - pokud všechny diskové oddíly jsou buď šifrovány nebo dešifrovány podle nastavení politik.

- **Nevyhovující** - když se stav svazků neshoduje s přiřazenými zásadami (například, když je šifrovaný pouze jeden ze dvou svazků, nebo když na daném svazku probíhá šifrovací proces).

- Zásady zařízení (**Šifrovat** nebo **Dešifrovat**).
- Klikněte na čísla ve sloupci Přehled svazků pro zobrazení informací o svazcích každého koncového bodu: ID, jméno, stav šifrování (**Šifrované** nebo **Nešifrované**), problémy, typ (**Boot** nebo **Non-boot**), velikost, ID klíče pro obnovu.

Stav modulů koncového bodu

Poskytuje přehled pokrytí ochranných modulů na zvolených cílech. V detailech hlášení můžete pro každý vybraný koncový bod prohlížet, které moduly jsou aktivní, vypnuté nebo neinstalované, a také používané skenovací jádro. Kliknutím na jméno koncového bodu se zobrazí **Informační** okno s podrobnostmi o koncovém bodě a nainstalovaných ochranných vrstvách.

Kliknutím na tlačítko **Překonfigurovat klienta** můžete zahájit úlohu, která změní počáteční nastavení jednoho nebo několika vybraných koncových bodů. Podrobnosti najdete v Překonfigurovat klienta .

Stav ochrany koncového bodu

Poskytuje vám rozmanité informace o stavu vybraných koncových bodů ve vaší síti.

- Stav antimalwarové ochrany
- Aktualizační stav Bitdefender Endpoint Security Tools
- Stav aktivity v síti (online/offline)
- Stav správy

Můžete aplikovat filtry podle bezpečnostního hlediska a stavu pro nalezení informací, které hledáte.

Aktivita Firewallu

Informuje vás o činnosti modulu Firewall v Bitdefender Endpoint Security Tools. Uvidíte počet blokovaných pokusů o přenos a počet blokovaných skenování portů na zvolených koncových bodech, a také uživatele, který byl přihlášený v době poslední detekce.

Činnost HyperDetectu

Informuje vás o činnosti modulu HyperDetect v Bitdefender Endpoint Security Tools.

V grafu v horní části stránky hlášení je zobrazena dynamika útočných pokusů během určeného období, a jejich šíření podle typu útoku. Přesunutím myši na položky v legendě se v grafu zvýrazní odpovídající typ útoku. Kliknutím na položku zobrazíte nebo skryjete odpovídající linku v grafu. Kliknutím na jakýkoli bod na lince můžete filtrovat údaje zobrazené v tabulce podle zvoleného typu. Například, když kliknete na jakýkoli bod na oranžové lince, v tabulce se zobrazí pouze exploity.

Podrobnosti v dolní části hlášení vám pomáhají identifikovat narušení ve vaší síti, a zda byla adresovaná. Odkazují k:

- Cesta ke škodlivému souboru, nebo zjištěné URL, v případě nakažených souborů. Pro bezsouborové útoky mu je poskytnuto jméno spustitelného souboru použitého při útoku, s odkazem k oknu s detaily, které zobrazuje důvod detekce a škodlivý příkazový řetězec.
- Koncový bod, na kterém k detekci došlo
- Ochranný modul, který odhalil hrozbu. Protože je HyperDetect přídatná vrstva k modulům Antimalware a Kontrola obsahu, hlášení bude poskytovat informace pouze o jednom z těchto dvou modulů, v závislosti na typu detekce.
- Typu zamýšleného útoku (cílený útok, grayware, exploity, ransomware, podezřelé soubory a síťový přenos)
- Stav ohrožení
- Úroveň ochrany na modulu, na které byla hrozba odhalena (Tolerantní, Normální, Agresivní)
- Počet, kolikrát byla hrozba nalezena
- Nejnovější detekce
- Identifikace jako bezsouborový útok (ano nebo ne), pro rychlé filtrování detekcí bezsouborových útoků

Poznámka
Soubor může být použit u více typů útoků. Z tohoto důvodu, GravityZone opakovaně nahlašuje soubory, které už byli použity u jiných typů útoků.

Z tohoto hlášení, můžete rychle vyřešit falešné poplachy přidáním výjimek do příslušných politik. K tomu, aby jste to provedli:

1. Vyberte v tabulce tolik vstupů, kolik potřebuteje.

   Poznámka
   Detekce file-less útoků nemůže být přidána do výjimek, z důvodu že detekovaný spustitelný soubor nemusí být obsahovat malware, ale může být hrozbou při použití příkazové řádky.

2. Klikněte na tlačítko **Add exception** v horní části tabulky.
3. V okně nastavení vyberte politiku, na kterou výjimka se má aplikovat a klikněte **Přidat**.

   Ve výchozím nastavení, relevantní informace pro každou výjimku je odeslána do laboratoře Bitdefender ke zlepšení schopností detekcí produktů Bitdefender. Můžete kontrolovat tuto akci použitím zaškrtávacího tlačítka **Odeslat zpětnou vazbu do Bitdefender pro zlepšení analýzy**.

Pokud hrozba byla detekována Antimalware modulem, výjimka bude aplikována jak pro skenovaní při čtení (On-Access) tak i pro plánované skenování (On-Demand).

Poznámka
Tyto výjimky najdete v následujících sekcích vámi vybraných politik: v **Antimalware > Nastavení** pro soubory, a v **Kontrola obsahu > Internetový provoz** pro URL.

Stav malwaru

Pomáhá vám zjistit, kolik a které z vybraných koncových bodů bylo ovlivněno malwarovou aktivitou v určitém čase, a jakým způsobem byly hrozby vyřešeny. Také můžete vidět, který uživatel byl přihlášen v okamžiku poslední detekce.

Koncové body jsou seskupeny na základě těchto kritérií:

- Koncové body bez detekcí (žádné malware hrozby nebyly detekovány během určité doby)
- Koncové body s vyřešenými malware hrozbami (všechny detekované soubory byli úspěšně dezinfikovány nebo přesunuty do karantény)
- Koncové body, které jsou stále infikovány malwarem (k některým detekovaným souborům byl zamítnut přístup)

Pro každý koncový bod, kliknutím na odkazy, které jsou dostupné ve sloupci pro výsledky dezinfekce, můžete zobrazit seznam hrozeb a cest nebezpečných souborů.

V tomto přehledu můžete rychle spustit úlohu Úplná kontrola u nevyřešených cílů kliknutím na tlačítko **Kontrola infikovaných cílů** z panelu nástrojů Akce nad tabulkou dat.

Síťové události

Informuje vás o činnosti modulu Network Attack Defense. Graf zobrazuje počet pokusů o útok detekovaných během zadaného intervalu. Detailní report obsahuje:

- Název koncového bodu, IP a FQDN
- Uživatelské jméno
- Název detekce
- Technika útoku
- Počet pokusů
- IP adresa útočníka
- Cílená IP adresa a port
- Když byl útok naposledy zablokován

Kliknutím na tlačítko **Přidat výjimky** pro vybranou detekci se automaticky vytvoří položka v **Globální Výjimky** z **Network Protection** sekce.

Stav Síťových oprav

Zkontrolujte stav aktuálnosti softwaru nainstalovaného ve vaší síti. Hlášení ukazuje následující podrobnosti:

- Cílový stroj (název koncového bodu, IP a operační systém).
- Bezpečnostní opravy (nainstalované opravy, neúspěšné opravy, chybějící bezpečnostní a jiné než bezpečnostní opravy).
- Stav a čas posledních úprav na vybraných koncových bodech.

Stav Ochrany Sítě

Poskytuje podrobné informace o celkovém stavu zabezpečení cílových koncových bodů. Můžete například zobrazit informace o:

- Jméno, IP, a FQDN
- Stav:
  - **Má problémy** - koncový bod obsahuje chyby zabezpečení (bezpečnostní agent není aktuální, jsou detekovány bezpečnostní hrozby atd.)

- **Žádné problémy** - koncový bod je chráněn a nejsou důvody k obavám.
- **Neznámé** - koncový bod byl při vygenerování zprávy offline.
- **Nespravováno** - agent zabezpečení dosud není v koncovém bodě nainstalován.

- Dostupné vrstvy ochrany
- Spravované a nespravované koncové body (agent zabezpečení je nainstalován nebo není)
- Typ a stav licence (další sloupce související s licencí jsou ve výchozím nastavení skryté)
- Stav infekce (koncový bod je „čistý“ nebo ne)
- Aktualizujte stav produktu a obsahu zabezpečení
- Stav patchů zabezpečení softwaru (chybějící patche zabezpečení nebo jiné patche)

U nespravovaných koncových bodů uvidíte v ostatních sloupcích stav **Nespravováno**.

Testování na požádání

Poskytuje informace ohledně skenování na vyžádání, které proběhlo na zvolených cílech. V koláčovém grafu je zobrazena statistika úspěšných a neúspěšných skenování. Tabulka pod grafem obsahuje podrobnosti ohledně typu skenování, výskytu a posledního úspěšného skenování pro každý koncový bod.

Soulad se zásadami

Poskytuje informace ohledně bezpečnostních zásad platných na zvolených cílech. V koláčovém grafu je zobrazen stav pravidla. V tabulce pod grafem uvidíte přiřazené pravidlo pro každý koncový bod, jeho typ a také datum a uživatele, který ho přiřadil.

Sandbox Analyzer Odeslání selhalo

Zobrazuje všechna neúspěšná odeslání objektů odeslaných z koncových bodů do Sandbox Analyzer během určitého období. Podání je považováno za neúspěšné po několika opakovaných pokusech.

V grafickém náhledu uvidíte změny neúspěšných odeslání během zvoleného období, zatímco v tabulce v hlášení uvidíte, které soubory nemohly být odeslány do Sandbox Analyzer, stroj, ze kterého byla položka odeslána, datum a čas

každého pokusu, vrácený kód chyby, popis každého neúspěšného pokusu a název společnosti.

Sandbox Analyzer Výsledky (zastaralé)

Poskytuje vám podrobné informace ohledně souborů na zvolených koncových bodech, které byly analyzovány v sandboxu během určitého období. Čárový graf zobrazuje počet čistých nebo nebezpečných analyzovaných souborů, zatímco tabulka vám představí podrobnosti o každém případu.

Můžete vytvořit hlášení o výsledcích Sandbox Analyzer pro všechny analyzované soubory, nebo pouze pro ty, které byly odhaleny jako nebezpečné.

Můžete zobrazit:

- Posudek analýzy, rozhodující zda je soubor čistý, nebezpečný nebo neznámý (**Nalezena hrozba** / **Žádná hrozba nenalezena** / **Nepodporované**). Tento sloupec se zobrazí pouze tehdy, když zvolíte hlášení pro zobrazení všech analyzovaných souborů.

  K zobrazení kompletního seznamu typů souborů a přípon podporovaných Sandbox Analyzer přejděte do „Podporované typy souborů a přípony pro ruční odesílání“ (str. 570).
- Typ hrozby, jako je adware, rootkit, downloader, exploit, modifikátor hostitele, škodlivé nástroje, krádeže hesel, ransomware, spam nebo trojský kůň.
- Datum a čas detekce, které můžete filtrovat podle hlášeného období.
- Jméno hostitele nebo IP koncového bodu, na kterém byl soubor nalezen.
- Názvy souborů, pokud byly podány jednotlivě, nebo počet analyzovaných souborů v případě hromadného podání. Klikněte na název souboru nebo na odkaz k balíku souborů pro zobrazení detailů a přijatých opatření.
- Stav nápravných opatření pro podané soubory (**Částečné**, **Neúspěšné**, **Pouze nahlášené**, **Úspěšné**).
- Jméno společnosti.
- Více informací o vlastnostech analyzovaného souboru je k dispozici kliknutím na tlačítko **Číst dále** ve sloupci **Výsledek analýzy**. Zde uvidíte vhledy do zabezpečení a podrobná hlášení na příkladovém chování.

Sandbox Analyzer zachycuje následující behaviorální události:

- Psaní / odstraňování / přesouvání / kopírování / nahrazování souborů v systému a na vyměnitelných jednotkách.
- Spuštění nově vytvořených souborů.
- Změny v systému souborů.
- Změny provedené na aplikacích spuštěných uvnitř virtuálního stroje.
- Změny na hlavním panelu systému Windows a Start menu.

- Tvorba / ukončení / zavedení procesů.
- Psaní / odstranění klíčů registru.
- Tvorba mutex objektů
- Tvorba / spuštění / zastavení / upravování / dotazování / odstraňování služeb.
- Změna bezpečnostních nastavení prohlížeče.
- Změna nastavení zobrazení Průzkumníku Windows.
- Přidání souborů na seznam výjimek firewallu.
- Změna nastavení sítě
- Povolení spuštění při startu systému.
- Připojení ke vzdálenému hostiteli.
- Přístup k určitým doménám.
- Přenos dat z a na určité domény.
- Přístup k URL, IP a portům skrze různé komunikační protokoly.
- Kontrolování indikátorů virtuálního prostředí.
- Kontrola indikátorů monitorovacích nástrojů.
- Tvorba snímků.
- SSDT, IDT, IRP hooks.
- Paměťové skládky pro podezřelé procesy.
- Volání funkcí Windows API.
- Být neaktivní během určitého časového úseku pro pozdržení spuštění.
- Tvorba souborů s akcemi, které mají být spouštěny v určitých časových intervalech.

V okně **Výsledek analýzy** klikněte na tlačítko **Stáhnout** pro uložení obsahu Shrnutí chování na váš počítač v těchto formátech: XML, HTML, JSON, PDF.

Tato zpráva bude i nadále podporována po omezenou dobu. Doporučuje se, abyste předložili podklady pro shromažďování potřebných informací o analyzovaných vzorcích. Karty podání jsou k dispozici v sekci **Sandbox Analyzer** v hlavní nabídce Control Center.

Bezpečnostní Audit

Poskytuje informace o bezpečnostních událostech, ke kterým došlo na zvoleném cíli. Informace se týkají následujících událostí:

- Malwarová detekce
- Blokovaná aplikace
- Blokované skenování portu
- Blokovaný provoz
- Blokovaná webová stránka

- Blokovat zařízení
- Blokovaný email
- Blokovaný proces
- Události HVI
- Pokročilé Anti-Exploit události
- Network Attack Defense události
- Detekce ransomwaru

Stav Security Server

Pomáhá vám ve zhodnocení stavu zvolených Security Serverů. S pomocí různých stavových ukazatelů můžete rozpoznat problémy, které by se mohly na každém ze Security Serverů vyskytovat, jako například:

- **Stav** : ukazuje celkový stav Security Serverů.
- **Stav stroje**: informuje, která zařízení Security Server jsou pozastavena.
- **Stav AV**: Poukazuje na to, zda je modul Antimalware zapnutý nebo vypnutý.
- **Stav aktualizací**: ukazuje, zda jsou zařízení Security Server aktuální, nebo jsou na nich aktualizace vypnuty.
- **Stav zatížení**: ukazuje úroveň zatížení skenování Security Serveru, jak je popsáno níže:
  - **Nezatížený**, když je využito méně než 5% jeho skenovací kapacity.
  - **Normální**, když je zatížení skenu v rovnováze.
  - **Přetížený**, když zatížení skenu přesáhne 90% své kapacity. V takovém případě zkontrolujte bezpečnostní pravidla. Pokud jsou všechy alokované Security Servery v rámci politiky a přetížené, tak potřebujete přidat další Security Server do seznamu. V jiném případě, si vyberte síťové připojení mezi klienty a Security Servery, kde nejsou problémy s přetížením.
- **HVI chráněné VS**: informuje vás o virtuálních strojích, které jsou monitorované a chráněné modulem HVI.
- **Stav HVI**: ukazuje, zda je modul HVI povolený nebo vypnutý. HVI je povolený, pokud má host nainstalovaný jak Security Server, tak Doplňkový balíček.
- **Připojená úložná zařízení (Connected Storage Devices)**: vás informuje o tom kolik ICAP-compatibilních úložných zařízení (storage devices) je připojeno k Security Serveru. Kliknutím na toto číslo se vám zobrazí seznam

úložných zařízení, s detaily pro každého z nich: jméno, IP adresy, druh, datum a čas posledního připojení.

- **Stav skenování úložiště (Storage Scanning Status)**: ukazuje jestli je služba Security for Storage zapnutá nebo vypnutá.

Můžete také prohlížet počet agentů připojených k Security Serveru. Dále, kliknutím na počet připojených klientů zobrazíte seznam koncových bodů. Pokud má Security Server problémy, tyto koncové body mohou být zranitelné.

Top 10 odhaleného malwaru

Ukáže vám 10 malwarových hrozeb, odhalených během určitého časového období na zvolených koncových bodech.

> **Poznámka**
> V tabulce s podrobnostmi se zobrazují všechny koncové body, které byly nakaženy malwarem z Top 10.

Top 10 infikovaných koncových bodů

Ukazuje 10 nejvíce nakažených koncových bodů podle počtu celkových detekcí na zvolených koncových bodech během určitého období.

> **Poznámka**
> Tabulka s podrobnostmi zobrazuje všechen malware odhalený na Top 10 infikovaných koncových bodech.

Stav aktualizací

Ukáže vám stav aktualizací bezpečnostního agenta nebo Security Serveru nainstalovaného na vybraných cílech. Stav aktualizace se týká verzí obsahu produktu a zabezpečení.

Pomocí dostupných filtrů můžete snadno zjistit, kteří klienti byli za posledních 24 hodin aktualizováni, a kteří ne.

V tomto hlášení můžete agenty rychle aktualizovat na nejnovější verzi. Toto provedete kliknutím na tlačítko **Aktualizovat** v akčním panelu nástrojů nad tabulkou s údaji.

Stav aktualizací

Ukáže vám bezpečnostní agenty nainstalované na zvolených cílech, a zda je k dispozici aktuálnější řešení.

Na koncové body se zastaralým bezpečnostním agentem můžete rychle nainstalovat nejnovějšího podporovaného bezpečnostního agenta kliknutím na tlačítko **Aktualizovat**.

Poznámka
Toto hlášení je dostupné pouze po provedení aktualizace GravityZone.

Stav zabezpečení sítě virtuálních zařízení

Informuje vás o pokrytí ochrany Bitdefender ve vašem virtualizovaném prostředí. Pro každé ze zvolených zařízení si můžete prohlédnout, který z komponentů řeší bezpečnostní potíže:

- Security Server, pro zavedení bez agenta v prostředích VMware NSX a vShield a pro HVI
- Bezpečnostní agent, v jakékoli jiné situaci

Činnost HVI

Informuje vás o všech útocích, které moduly HVI zjistily na zvolených strojích během určitého časového úseku.

Hlášení obsahuje také informace o datu a času naposledy odhaleného problému, jehož součástí byl monitorovaný proces, konečný stav opatření uplatněného proti útoku, uživatele, pod kterým proces začal, a cílové zařízení.

V závislosti na uplatněném opatření může být ten samý proces nahlášen několikrát. Například, pokud byl proces v jednom případě zničen, a v druhém případě mu byl odepřen přístup, uvidíte v tabulce s hlášením dvě položky.

Pro každý proces, když kliknete na datum poslední detekce, se zobrazí oddělený protokol obsahující všechny problémy zjištěné od chvíle zahájení procesu. Protokol poskytuje důležité informace, jako je typ incidentu a jeho popis, zdroj a cíl útoku a opatření, která byla uplatněna pro jeho nápravu.

V tomto hlášení můžete rychle navést ochranný modul, aby ignoroval určité události, které považujete za legitimní. Toto provedete kliknutím na tlačítko **Přidat výjimku** v akčním panelu nástrojů nad tabulkou s údaji.

Poznámka
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

HVI Stav narušení třetí stranou

Nabízí vám podrobný popis stavu každého spuštěného zavedení na cílových koncových zařízeních. Informace zahrnují:

- Název koncového bodu.
- Název zavedeného nástroje.
- IP adresa koncového bodu.
- Hostitelský operační systém.
- Spoušť. Toto může být narušení paměti, vyžádaná úloha nebo plánované spuštění.
- Počet úspěšných spuštění. Kliknutím na číslo se otevře okno s cestou k protokolům a časovým záznamem pro každé spuštění nástroje. Kliknutím na ikonu před umístěním cesty ji zkopírujete do schránky.
- Počet neúspěšných spuštění. Kliknutím na číslo se otevře okno, ve kterém uvidíte důvod selhání a časový záznam.
- Poslední úspěšné zavedení.

Zavádění jsou seskupena podle cílových koncových bodů. Můžete filtrovat hlášení tak, aby se zobrazily pouze údaje týkající se konkrétního nástroje, pomocí možností filtrování v záhlaví tabulky.

Poznámka
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Aktivita Ransomware

Informuje vás o útocích na ransomware, které GravityZone zjistila na koncových bodech, které spravujete, a poskytuje vám nástroje potřebné k obnovení souborů postižených během útoků.

Zpráva je k dispozici jako stránka v Control Center, odlišná od ostatních zpráv, přístupná přímo z hlavní nabídky GravityZone.

Stránka **Aktivita ransomwaru** se skládá z tabulky, která pro každý útok ransomware uvádí následující:

- Název, IP adresa a FQDN koncového bodu, na kterém došlo k útoku
- Společnost, které koncový bod patří

- Jméno uživatele, který byl při útoku přihlášen
- Typ útoku, respektive lokální nebo vzdálený
- Proces, při kterém ransomware běžel pro lokální útoky, nebo IP adresa, ze které byl útok zahájen pro vzdálené
- Datum a čas detekce
- Počet šifrovaných souborů, dokud nebyl útok blokován
- Stav akce obnovení pro všechny soubory v cílovém koncovém bodě

Některé podrobnosti jsou ve výchozím nastavení skryty. Kliknutím na tlačítko **Zobrazit/skrýt sloupce** v pravé horní části stránky nakonfigurujete podrobnosti, které chcete v mřížce zobrazit. Pokud máte v mřížce mnoho položek, můžete filtry skrýt pomocí tlačítka **Zobrazit/Skrýt filtry** v pravé horní části stránky.

Další informace získáte kliknutím na číslo souboru. Můžete zobrazit seznam s úplnou cestou k původním a obnoveným souborům a se stavem obnovení všech souborů zapojených do vybraného útoku ransomwarem.

Důležité
Záložní kopie jsou k dispozici maximálně 30 dní. Nezapomeňte na datum a čas, dokud nebude možné soubory obnovit.

Obnovení souborů z ransomwaru:

1. Vyberte požadované útoky v tabulce.
2. Klikněte na tlačítko **Obnovit soubory** . Zobrazí se potvrzovací okno.

   Probíhá vytváření úlohy obnovení. Jeho stav můžete zkontrolovat na stránce **Úkoly** , stejně jako u jiných úkolů v GravityZone.

Pokud jsou detekce výsledkem legitimních procesů, postupujte takto:

1. Vyberte záznamy v tabulce.
2. Klikněte na tlačítko **Přidat výjimku** .
3. V novém okně vyberte zásady, na které se musí výjimky vztahovat.
4. Klikněte na tlačítko **Přidat**.

   použije všechny možné výjimky: na složku, na proces a na IP adresu.

   Můžete je zkontrolovat nebo upravit v sekci zásad **Antimalware a Nastavení - Vlastní vyloučení** .

Poznámka
Aktivita Ransomware udržuje záznamy o událostech po dobu dvou let.

10.1.2. Hlášení Exchange Serverů

Toto jsou dostupné typy hlášení pro Exchange Servery:

Exchange - Blokovaný obsah a přílohy
Poskytuje vám informace o emailech nebo přílohách, které Kontrola obsahu odstranila ze zvolených serverů během určitého období. Informace zahrnují:

- Emailové adresy odesílatele a adresátů.

  Když má email více adresátů, v hlášení je místo emailových adres uveden počet adresátů s odkazem k oknu, které obsahuje seznam emailových adres.
- Předmět emailu.
- Typ detekce, ukazující na to, který filtr Kontroly obsahu hrozbu odhalil.
- Opatření, která byla provedena na detekci.
- Server, na kterém byla hrozba odhalena.

Exchange - Blokované neskenovatelné přílohy
Poskytuje vám informace o emailech, které obsahují neskenovatelné přílohy (nadměrně komprimované, chráněné heslem, atd.), blokovaných na mailových serverech Exchange během určitého období. Informace odkazují k:

- Emailové adresy odesílatele a adresátů.

  Když je email odeslán více adresátům, v hlášení je místo emailových adres uveden počet adresátů s odkazem k oknu, které obsahuje seznam emailových adres.
- Předmět emailu.
- Opatření provedená pro odstranění neskenovatelných příloh:
  - **Odstraněný email**, což znamená, že byl celý email smazán.
  - **Odstraněné přílohy**, obecné jméno pro všechna opatření, která odstraňují přílohy z emailových zpráv, jako je smazání přílohy, přesunutí do karantény nebo nahrazení přílohy upozorněním.

  Kliknutím na odkaz ve sloupci **Akce** můžete prohlížet podrobnosti o každé blokované příloze a příslušné přijaté opatření.
- Datum a čas detekce.

- Server, na kterém byl email odhalen.

Exchange - Aktivita Skenu Emailu

Ukazuje statistiky opatření přijatých modulem Exchange Protection za určité období.

Opatření jsou seskupena podle typu detekce (malware, spam, zakázaná příloha a zakázaný obsah) a podle typu serveru.

Statistika odkazuje k následujícím stavům emailů:

- **V karanténě.** Tyto emaily byly přesunuty do složky Karanténa.
- **Odstraněné/Odmítnuté.** Tyto emaily byly smazány nebo odmítnuty serverem.
- **Přesměrované.** Tyto emaily byly přesměrovány na emailovou adresu zadanou v pravidle.
- **Vyčištěné a doručené.** Hrozby z těchto emailů byly odstraněny a emaily prošly filtrováním.

  Email je považován za čistý, když jsou všechny nalezené přílohy vydezinfikovány, přesunuty do karantény, odstraněny, nebo nahrazeny textem.
- **Změněné a doručené.** K hlavičkám emailů byly přidány informace o skenování a emaily prošly filtrováním.
- **Doručené bez jiného opatření.** Tyto emaily Exchange Protection ignorovala a prošly filtrováním.

Exchange - Malwarová činnost

Poskytuje vám informace o emailech obsahujících malwarovou hrozbu, zjištěných na zvolených mailových serverech Exchange během určitého období. Informace odkazují k:

- Emailové adresy odesílatele a adresátů.

  Když je email odeslán více adresátům, v hlášení je místo emailových adres uveden počet adresátů s odkazem k oknu, které obsahuje seznam emailových adres.
- Předmět emailu.
- Stav emailů po antimalwarovém skenování.

  Kliknutím na odkaz stavu zobrazíte podrobnosti o nalezeném malwaru a o přijatých opatřeních.

- Datum a čas detekce.
- Server, na kterém byla hrozba odhalena.

Exchange - Top 10 odhaleného malwaru

Informuje vás o top 10 nejčastěji se vyskytujících malwarových hrozbách v emailových přílohách. Můžete vygenerovat dvě zobrazení s různými statistikami. V jednom zobrazení uvidíte počet detekcí od postižených adresátů, a v druhém od odesílatelů.

Například, GravityZone odhalila jeden email s infikovanou přílohou, odeslaný pěti příjemcům.

- V prohlížení adresátů:
  - Hlášení ukazuje pět detekcí.
  - V detailech hlášení jsou zobrazeni pouze adresáti, nikoli odesílatelé.
- V prohlížení odesílatelů:
  - Hlášení ukazuje jednu detekci.
  - V detailech hlášení jsou zobrazeni pouze odesílatelé, nikoli adresáti.

Kromě jmen odesílatele/adresátů a malwaru, hlášení vám poskytne také následující podrobnosti:

- Typ malwaru (vir, spyware, PUA atd.)
- Server, na kterém byla hrozba odhalena.
- Opatření, která antimalwarový produkt provedl.
- Datum a čas poslední detekce.

Exchange - Top 10 malwarových příjemců

Ukáže vám top 10 emailových příjemců, kteří byli nejčastějším cílem malwaru během určeného období.

Detaily hlášení vám dodají kompletní seznam malwaru, kterým byli tito příjemci nakaženi, spolu s přijatými opatřenými.

Exchange - Top 10 malwarových příjemců

Ukáže vám top 10 emailových příjemců podle množství spamu nebo phishingových emailů odhalených během určitého období. Hlášení poskytuje také informace o akcích provedených na jednotlivých emailech.

10.1.3. Hlášení o mobilních zařízeních

Poznámka
Ochrana proti malware a podobná hlášení jsou dostupná pouze pro zařízení Android.

Toto je seznam dostupných typů hlášení pro mobilní zařízení:

Stav malwaru
Pomáhá vám zjistit, kolik a která z vybraných mobilních zařízení bylo ovlivněno malwarovou aktivitou v určitém čase, a jakým způsobem byly hrozby vyřešeny. Mobilní zařízení jsou seskupena na základě následujících kritérií:

- Mobilní zařízení bez detekcí (během určené doby nebyly zjištěny žádné malwarové hrozby)
- Mobilní zařízení s vyřešeným malwarem (všechny odhalené soubory byly odstraněny)
- Mobilní zařízení s přítomným malwarem (některé z odhalených souborů nebyly odstraněny)

Top 10 infikovaných zařízení
Zobrazí top 10 nejvíce infikovaných mobilních zařízení ze všech cílových zařízení během určitého období.

Poznámka
Tabulka s podrobnostmi zobrazuje všechen malware odhalený na top 10 infikovaných mobilních zařízeních.

Top 10 odhaleného malwaru
Ukáže vám top 10 malwarových hrozeb, odhalených během určitého časového období na zvolených mobilních zařízeních.

Poznámka
V tabulce s podrobnostmi se zobrazují všechna mobilní zařízení, která byla nakažena malwarem z top 10.

Soulad zařízení
Informuje vás o stavu souladu cílových mobilních zařízení. Můžete nastavit název zařízení, stav, operační systém a důvod nesouladu.

Pro více informací ohledně podmínek pro soulad se prosím podívejte na „Kritéria pro nesoulad“ (str. 387).

Synchronizace zařízení

Informuje vás o stavu synchronizace cílových mobilních zařízení. Můžete prohlížet název zařízení, uživatele, ke kterému je přiřazeno, dále stav synchronizace, operační systém a čas, kdy bylo zařízení naposledy viděno online.

Další informace viz „Kontrolování Stavu mobilních zařízení“ (str. 167).

Zablokované webové stránky

Informuje vás o počtu pokusů cílových zařízení k přístupu k internetovým stránkám, které jsou blokovány pravidly **Přístupu k webu**, za určité období.

Pro každé zařízení s detekcemi klikněte na číslo v sloupci **Blokované webové stránky** pro zobrazení podrobných informací o každé blokované webové stránce, jako jsou:

- Adresa
- Součást politiky, která provedla činnost
- Počet zablokovaných pokusů
- Kdy byla stránka naposledy blokována

pro více informací o nastavení politiky přístupu k webům, se obraťte na „Profily“ (str. 392).

Činnost Ochrany webu

Informuje vás o počtu pokusů cílových mobilních zařízení k přístupu k internetovým stránkám s bezpečnostními hrozbami (phishing, podvody, malware nebo nedůvěryhodné stránky) během určitého období. Pro každé zařízení s detekcemi klikněte na číslo v sloupci Blokované webové stránky pro zobrazení podrobných informací o každé blokované webové stránce, jako jsou:

- Adresa
- Typ hrozby (phishing, malware, podvod, nedůvěryhodné)
- Počet zablokovaných pokusů
- Kdy byla stránka naposledy blokována

Web Security je součástí politiky, která detekuje a zablokuje stránky s bezpečnostní chybou. Pro více informací o nastavení pravidel síťové bezpečnosti se odkažte na „Zabezpečení“ (str. 382).

10.2. Vytváření hlášení

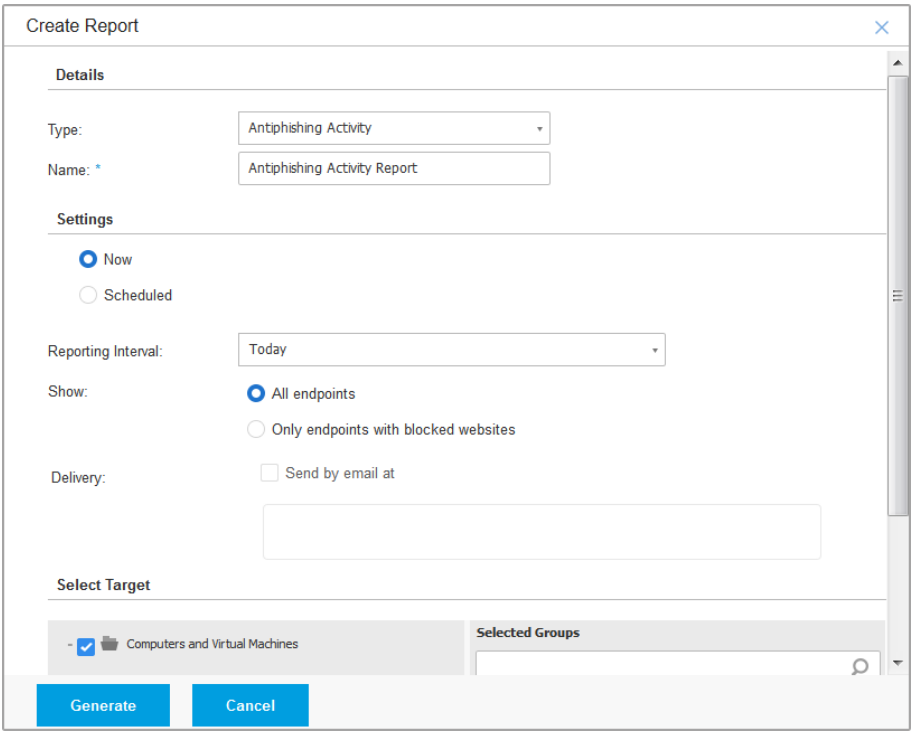
Můžete vytvářet dvě skupiny hlášení:

- **Okamžitá hlášení.** Okamžitá hlášení se zobrazují automaticky po vytvoření.
- **Plánovaná hlášení.** Plánovaná hlášení mohou být nastavena pro pravidelné spuštění, v konkrétní čas a datum. Seznam všech plánovaných hlášení je zobrazen na stránce **Hlášení**.

Důležité
Okamžitá hlášení jsou automaticky mazána, když zavřete stránku s hlášením. Plánovaná hlášení jsou uložena a zobrazena na stránce **Hlášení**.

Pro vytvoření hlášení:

1. Přejděte na stránku **Hlášení**.
2. Vyberte typ síťových objektů z nastavení zobrazení.
3. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.



Možnosti hlášení pro počítače a virtuální zařízení

4. Z nabídky zvolte požadovaný typ hlášení. Další informace viz „Typy hlášení“ (str. 477)
5. Zvolte pro hlášení definující jméno. Při vybírání jména vezměte v úvahu typ hlášení a cíl, případně nastavení hlášení.
6. Nastavte opakování hlášení:
   - Vyberte **Teď** pro vytvoření okamžitého hlášení.
   - Vyberte **Plánované** pro nastavení hlášení tak, aby byla generována automaticky v časových intervalech, které zvolíte:
     – Každou hodinu, v určeném úseku mezi hodinami.

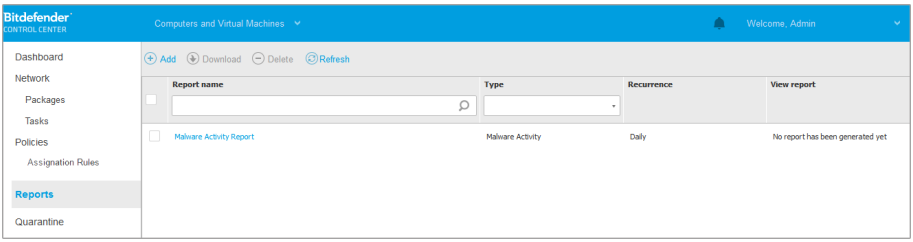
- Denně. V tomto případě můžete nastavit také počáteční čas (hodinu a minuty).
- Každý týden, v konkrétní dny a ve zvolený počáteční čas (hodina a minuty).
- Každý měsíc, v každý určený den v měsíci a ve zvolený počáteční čas (hodina a minuty).

7. Pro většinu typů hlášení musíte určit časový interval, ke kterému se zahrnuté údaje mají odkazovat. Hlášení bude obsahovat pouze údaje za zvolené období.
8. Několik typů hlášení poskytuje možnosti filtrování, které vám pomáhají najít informace, které vás zajímají. Použijte možnosti filtrování pod sekcí **Zobrazit**, abyste získali pouze vaše požadované informace.

   Například, pro hlášení **Stav aktualizací** si můžete vybrat prohlížení pouze seznamu objektů v síti, které se neaktualizovaly, nebo takových, které potřebují restartovat pro dokončení aktualizace.
9. **Doručení**. Pro obdržení plánovaného hlášení emailem označte odpovídající pole. Zadejte požadované emailové adresy do pole níže. Ve výchozím nastavení email obsahuje archiv s oběma typy hlášení (PDF a CSV). Použijte zaškrtávací pole v sekci **Připojit soubory** pro nastavení, které soubory a jak je odeslat emailem.
10. **Zvolte cíl**. Posuňte se dolů pro nastavení cíle hlášení. Vyberte jednu nebo více skupin koncových bodů, které chcete zahrnout v hlášení.
11. V závislosti na zvoleném typu opakování klikněte buď na **Vytvořit** pro vytvoření okamžitého hlášení, nebo na **Uložit** pro vytvoření plánovaného hlášení.
    - Okamžité hlášení se zobrazí automaticky poté, co kliknete na **Vytvořit**. Čas potřebný pro vytvoření hlášení se může lišit podle počtu spravovaných objektů v síti. Počkejte prosím na vytvoření požadovaného hlášení.
    - Plánované hlášení se zobrazí na stránce **Hlášení**. Jakmile je hlášení vytvořeno, můžete si ho prohlédnout kliknutím na odpovídající odkaz ve sloupci **Zobrazit hlášení** na stránce **Hlášení**.

10.3. Prohlížení a správa Plánovaných hlášení

Pro prohlížení a správu plánovaných hlášení přejděte na stránku **Hlášení**.



Stránka s Hlášení

Všechna plánovaná hlášení uvidíte v tabulce spolu s užitečnými informacemi o nich:

- Jméno a typ hlášení
- Report opakování
- Poslední vytvořené hlášení.

Poznámka
Plánovaná hlášení jsou dostupná pouze pro uživatele, který je vytvořil.

Pro seřazení hlášení podle konkrétního sloupce jednoduše klikněte na hlavičku toho sloupce. Pro otočení pořadí řazení klikněte znovu na hlavičku sloupce.

Pro rychlé nalezení toho, co hledáte, použijte vyhledávací pole, nebo na možnosti filtrování pod hlavičkami sloupců.

Pro vyčištění vyhledávacího pole nad něj posuňte kurzor a klikněte na ikonu × **Smazat**.

Ujistěte se, že se zobrazují ty nejnovější informace kliknutím na tlačítko **Obnovit** v horní části tabulky.

10.3.1. Prohlížení hlášení

Pro zobrazení hlášení:

1. Přejděte na stránku **Hlášení**.
2. Seřaďte hlášení podle jména, typu nebo opakování pro snadné nalezení hlášení, které hledáte.
3. Pro zobrazení hlášení klikněte na odpovídající odkaz ve sloupci **Zobrazit hlášení**. Zobrazí se nejnovější verze hlášení.

Pro zobrazení všech edicí hlášení se odkažte na„Ukládání hlášení“ (str. 503)

Všechna hlášení sestávají ze shrnutí (v horní části stránky s hlášeními), a ze sekce s podrobnostmi (v dolní části stránky s hlášeními).

- Část se shrnutím vám poskytne statistické údaje (koláčové grafy a grafická znázornění) pro všechny cílové síťové objekty a také obecné informace o hlášení, jako je hlášené období (případné), cíl hlášení atd.
- Sekce podrobností vám poskytne informace o každém cílovém síťovém objektu.

Poznámka

- Pro konfiguraci informací zobrazených v tabulce, klikněte na položky legendy pro zobrazení nebo schování vybraných údajů.
- Klikněte na oblast v grafice (část koláče, sloupec), která vás zajímá, pro zobrazení souvisejících podrobností v tabulce.

10.3.2. Úprava Plánovaných hlášení

Poznámka
Když upravujete plánované hlášení, všechny aktualizace budou uplatněny počínaje jeho dalším vydáním. Dříve vytvořená hlášení nebudou ovlivněna úpravami.

Pro změnu nastavení plánovaného hlášení:

1. Přejděte na stránku **Hlášení**.
2. Klikněte na jméno hlášení.
3. Upravte nastavení hlášení dle potřeby. Můžete změnit následující:
   - **Jméno hlášení.** Zvolte pro hlášení definující jméno pro usnadnění identifikace, o jaké hlášení se jedná. Při vybírání jména vezměte v úvahu typ hlášení a cíl, případně nastavení hlášení. Hlášení vytvořena podle plánovaného hlášení se jmenují podle něj.
   - **Opakování hlášení (plán).** Můžete naplánovat automatické generování hlášení každou hodinu (v určitém hodinovém intervalu), každý den (zahájené v určitý čas), každý týden (v určitý den v týdnu a čase zahájení), nebo každý měsíc (v určitý den v měsíci a čase zahájení). V závislosti na zvoleném plánu bude hlášení obsahovat pouze údaje buď za poslední den, týden nebo měsíc.
   - **Nastavení**

- Můžete naplánovat automatické generování hlášení každou hodinu (v určitém hodinovém intervalu), každý den (zahájené v určitý čas), každý týden (v určitý den v týdnu a čase zahájení), nebo každý měsíc (v určitý den v měsíci a čase zahájení). V závislosti na zvoleném plánu bude hlášení obsahovat pouze údaje buď za poslední den, týden nebo měsíc.
- Hlášení bude obsahovat pouze údaje za zvolené období. Interval můžete změnit počínaje příštím opakováním.
- Většina hlášení poskytuje možnosti filtrování, které vám pomáhají najít informace, které vás zajímají. Při prohlížení hlášení v konzoli jsou k dispozici všechny informace, nehledě na zvolené možnosti. Pokud ale hlášení odešlete emailem, v PDF souboru bude zahrnuto pouze shrnutí hlášení a zvolené informace. Podrobnosti hlášení budou k dispozici pouze ve formátu CSV.
- Můžete si vybrat obdržení hlášení emailem.

- **Zvolit cíl.** Zvolená možnost ukazuje typ současného cíle hlášení (buď skupiny, nebo jednotlivé objekty v síti). Klikněte na odpovídající odkaz pro zobrazení současného cíle hlášení. Pro jeho změnu zvolte skupiny nebo objekty v síti, které mají být zahrnuty v hlášení.

4. Kliknutím na tlačítko **Uložit** aplikujete změny.

10.3.3. Mazání plánovaných hlášení

Když plánované hlášení již nepotřebujete, je nejlepší ho odstranit. Vymazání plánovaného hlášení odstraní všechna jeho vydání, která byla do této chvíle automaticky generována.

Pro odstranění plánovaného hlášení:

1. Přejděte na stránku **Hlášení**.
2. Vyberte hlášení, které chcete odstranit.
3. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky.

10.4. Přijímání opatření na základě hlášení

Zatímco většina hlášení pouze upozorní na problémy ve vaší síti, některá z nich vám nabídnou několik možností opravy zjištěných problémů pouhým stisknutím tlačítka.

Pro opravení problémů zobrazených v hlášení klikněte na příslušné tlačítko v Akčním panelu nástrojů nad tabulkou s údaji.

Poznámka
Pro provedení těchto akcí potřebujete oprávnění pro **Správu sítě**.

Toto jsou dostupné možnosti pro každé hlášení:

Blokované aplikace

- **Přidat výjimku**. Přidá do pravidla výjimku, aby ochranné moduly příště již nemohly aplikaci zablokovat.
- **Přidat pravidlo**. Definuje pravidlo pro aplikaci nebo proces v Kontrole aplikací.

Činnost HVI

- **Přidat výjimku**. Přidá do pravidla výjimku, aby ochranný modul příště již nemohl incident nahlásit.

  Poznámka
  Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Stav malwaru

- **Skenování infikovaných cílů**. Spustí přednastavený Kompletní sken na cílech, které se stále zobrazují jako infikované.

Stav aktualizací

- **Aktualizace**. Aktualizuje cílové klienty na jejich nejnovější dostupnou verzi.

Stav aktualizací

- **Aktualizace**. Nahradí staré klienty na koncových bodech nejnovější generací dostupných produktů.

10.5. Ukládání hlášení

Ve výchozím nastavení se všechna plánovaná hlášení automaticky ukládají do Control Center.

Pokud potřebujete mít hlášení k dipozici po delší dobu, můžete si je uložit do počítače. Shrnutí hlášení bude dostupné ve formátu PDF, s tím, že podrobnosti hlášení budou dostupné pouze ve formátu CSV.

Máte dvě možnosti, jak ukládat hlášení:

- Export
- Stahování

10.5.1. Exportování hlášení

Pro exportování hlášení na váš počítač:

1. Vyberte formát a klikněte na **Export CSV** nebo **Export PDF** .
2. Podle nastavení vašeho prohlížeče může být soubor stažen automaticky do výchozího umístění pro stažené soubory, nebo se zobrazí okno pro stahování, ve kterém musíte určit cílovou složku.

10.5.2. Stahování hlášení

Archiv hlášení obsahuje jak shrnutí, tak podrobnosti hlášení.

Pro stažení archivu s hlášením:

1. Přejděte na stránku **Hlášení**.
2. Vyberte hlášení, které chcete zobrazit.
3. Klikněte na tlačítko **Stáhnout** a zvolte buď **Poslední verze** pro stažení naposledy generovaného hlášení, nebo **Plný archiv** pro stažení archivu obsahujícího všechny verze hlášení.

   Podle nastavení vašeho prohlížeče může být soubor stažen automaticky do výchozího umístění pro stažené soubory, nebo se zobrazí okno pro stahování, ve kterém musíte určit cílovou složku.

10.6. Hlášení na email

Hlášení můžete odesílat emailem podle následujících kroků:

1. Chcete-li e-mailem zobrazený přehled, klikněte na tlačítko **E-mail** . Hlášení bude odesláno na emailovou adresu přiřazenou k vašemu účtu.
2. Pro nastavení požadovaného odesílání plánovaných hlášení na email:
   a. Přejděte na stránku **Hlášení**.

b. Klikněte na jméno požadovaného hlášení.
c. Pod **Nastavení > Doručení** vyberte **Odeslat emailem na**.
d. Do pole níže zadejte požadovanou emailovou adresu. Můžete přidat libovolný počet emailových adres.
e. Klikněte na tlačítko **Save**.

> **Poznámka**
> PDF soubor odeslaný na email bude obsahovat pouze shrnutí hlášení a graf. Podrobnosti hlášení jsou k dispozici v CSV souboru.

Hlášení jsou odesílána na emaily jako .zip archivy.

10.7. Tisk hlášení

Control Center v současnosti nepodporuje funkci tlačítka pro tisk. Pro tisk hlášení ho musíte nejprve uložit na váš počítač.

11. KARANTÉNA

Karanténa je šifrovaná složka, obsahující potenciálně škodlivé soubory, jako jsou soubory podezřelé na malware, infikované malwarem, nebo jiné nežádoucí soubory. Virus nebo jiná forma malwaru v karanténě nemůže způsobit žádnou škodu, protože ho nelze spustit ani přečíst.

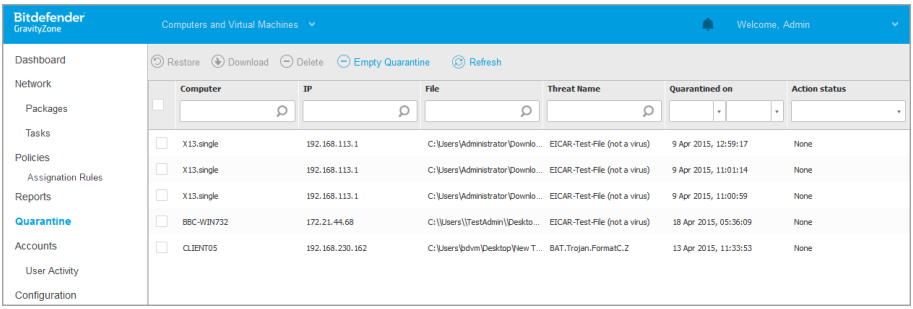
GravityZone přesouvá soubory do karantény v souladu s pravidly přiřazenými ke koncovým bodům. Ve výchozím stavu jsou do karantény ukládány soubory, které nelze vydezinfikovat.

Karanténa je uložena lokálně na každém koncovém bodě, kromě VMware vCenter Serveru integrovaného s vShield Endpoint a s NSX, pro který se ukládá na Security Server.

Důležité
Karanténa je nedostupná pro mobilní zařízení.

11.1. Prohlížení Karantény

Stránka **Karanténa** poskytuje podrobné informace ohledně souborů v karanténě na všech vašich spravovaných koncových bodech.



Stránka Karanténa

Stránka Karanténa sestává ze dvou zobrazení:

- Počítače a virtuální stroje, pro soubory nalezené přímo v systému souborů na koncových bodech.
- Exchange Servery, pro emaily a přílohy emailů odhalené na mailových serverech Exchange.

Výběr zobrazení v horní části stránky vám umožňuje střídání mezi těmito dvěma zobrazeními.

Informace o souborech v karanténě jsou zobrazeny v tabulce. Podle počtu spravovaných koncových bodů a úrovně nakažení, tabulka Karantény dokáže zahrnout velké množství záznamů. Tabulka může mít rozsah na několik stran (ve výchozím stavu je zobrazených 20 záznamů na stránku).

Pro pohyb mezi stránkami použijte navigační tlačítka ve spodní části tabulky. Můžete změnit počet položek zobrazených na stránku tak, že vyberete nějakou z menu umístěného vedle navigačních tlačítek.

Pro lepší viditelnost údajů, které vás zajímají, můžete použít vyhledávací pole v záhlaví sloupců pro filtrování zobrazených údajů. Například, můžete vyhledat konkrétní hrozbu nalezenou v síti, nebo konkrétní síťový objekt. Můžete také kliknout na hlavičku sloupců pro seřazení údajů podle určitého sloupce.

Ujistěte se, že se zobrazují ty nejnovější informace kliknutím na tlačítko **Obnovit** v horní části tabulky. Toto může být potřeba, když na stránce strávíte více času.

11.2. Karanténa pro počítače a virtuální stroje

Ve výchozím stavu jsou soubory z karantény automaticky odesílány do laboratoří společnosti Bitdefender, aby je analyzovali pracovníci výzkumu malwaru společnosti Bitdefender. Pokud je přítomnost malwaru potvrzena, je vydána signatura umožňující odstranění malwaru. Navíc, soubory v karanténě jsou skenovány po každé aktualizaci malwarových signatur. Vyčištěné soubory budou automaticky vráceny do původního umístění. Tyto funkce odpovídají každému bezpečnostnímu pravidlu na stránce **Zásady**, a můžete si vybrat, zda je ponechat nebo deaktivovat. Další informace viz „Karanténa“ (str. 278).

11.2.1. Zobrazení detailů Karantény

V tabulce Karanténa jsou uvedeny následující informace:

- Jméno koncového bodu, na kterém byla hrozba odhalena.
- IP koncového bodu, na kterém byla hrozba odhalena.
- Cesta k nakaženému nebo podezřelému souboru na koncovém bodě, na kterém byl zjištěn.
- Název, který malwarové hrozbě přidělili pracovníci výzkumu zabezpečení Bitdefender.
- Datum a čas, kdy byl soubor vložen do karantény.
- Stav opatření, jehož uplatnění bylo vyžádáno pro soubor v karanténě.

11.2.2. Správa souborů v Karanténě

Chování karantény se liší podle jednotlivých prostředí:

- **Security for Endpoints** uchovává soubory z karanténě na každém spravovaném počítači. Pomocí Control Center máte možnost buď odstranit, nebo obnovit určité soubory z karantény.
- **Security for Virtualized Environments (Multi-Platform)** ukládá soubory v karanténě na každém spravovaném virtuálním stroji. Pomocí Control Center máte možnost buď odstranit, nebo obnovit určité soubory z karantény.
- **Security for Virtualized Environments (integrované s VMware vShield Endpoint nebo NSX)** ukládá soubory z karantény na zařízení Security Server. Pomocí Control Center můžete mít možnost smazat soubory v karanténě nebo je stáhnout na místo kam chcete.

Obnovení souborů z karantény

V některých případech můžete potřebovat obnovit soubory z karantény buď do jejich původního, nebo jiného umístění. Jeden z takových případů může nastat, když chcete obnovit důležité soubory uložené v nakaženém archivu, který byl přesunut do karantény.

Poznámka
Obnovení souboru z karantény je možné pouze v prostředích, která jsou spravována prostřednictvím Security for Endpoints a Security for Virtualized Environments (Multi-Platform).

Pro obnovení jednoho nebo více souborů z karantény:

1. Přejděte na stránku **Karanténa**.
2. Zvolte **Počítače a virtuální stroje** z výběru zobrazení dostupného v horní části stránky.
3. Označte pole příslušící k souborům v karanténě, které chcete obnovit.
4. Klikněte na tlačítko **Obnovit** v horní části tabulky.
5. Zvolte umístění, do kterého chcete obnovit zvolené soubory (buď původní, nebo vlastní umístění na zvoleném počítači).

   Pokud se rozhodnete soubory obnovit do vlastního umístění, musíte zadat kompletní cestu do příslušného pole.
6. Zvolte **Automaticky přidat výjimku do pravidla** pro vyjmutí souborů, které mají být obnoveny, z budoucích skenování. Výjimka platí pro všechna pravidla platná pro zvolené soubory, kromě výchozích zásad, které nemohou být změněny.

7. Klikněte na **Uložit** pro zadání požadavku o obnovení. Ve sloupci **Akce** si můžete povšimnout stavu čekání.
8. Požadovaná akce je odeslána na cílové koncové body okamžitě, nebo hned poté, co jsou znovu online.

   Detaily ohledně stavu akce můžete prohlížet na stránce **Úlohy**. Jakmile je soubor obnoven, odpovídající záznam zmizí z tabulky Karanténa.

Stahovnání souborů v karanténě

Ve virtualizovaných prostředích VMware integrovaných s vShield Endpoint nebo NSX se karanténa ukládá na Security Server. Pokud si chcete prohlédnout nebo obnovit data ze souborů v karanténě, musíte je stáhnout z Security Server pomocí Control Center. Soubory z karantény jsou stahovány jako šifrované, heslem chráněné archivy ZIP, pro zabránění nepředvídané malwarové infekci.

Pro otevření archivu a extrahování jeho obsahu musíte použít nástroj Karanténa, samostatnou aplikaci Bitdefender, která nevyžaduje aplikaci.

Nástroj Karanténa je k dispozici pro tyto operační systémy:

- Windows 7 nebo novější
- Většina distribucí Linux 32-bit s grafickým uživatelským rozhraním (GUI).

Poznámka
Prosím poznamenejte si že Quarantine Tool nemá příkazový řádek.

Varování
Při extrahování souborů z karantény buďte opatrní, protože mohou infikovat váš systém. Doporučujeme extrahovat a analyzovat soubory z karantény na testovacím nebo izolovaném systému, nejlépe na bázi Linux. Na Linux jsou malwarové infekce snadněji izolovatelné.

Stažení souborů karantény do vašeho počítače:

1. Přejděte na stránku **Karanténa**.
2. Zvolte **Počítače a virtuální stroje** z výběru zobrazení dostupného v horní části stránky.
3. Filtrujte údaje v tabulce zadáním jména hostitele Security Server nebo jeho IP adresy do příslušného pole v záhlaví tabulky.

   Pokud je karanténa rozsáhlá, možná budete muset použít přídatné filtry nebo zvýšit počet souborů zobrazených na stránku, abyste si mohli prohlédnout právě ty soubory, které vás zajímají.

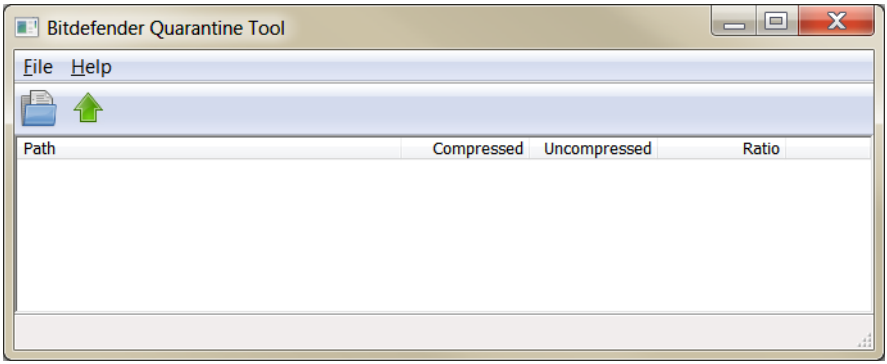
4. Vyberte zaškrtávací pole odpovídajícího souboru, který chcete stáhnout.
5. Klikněte na tlačítko **Stáhnout** v horní části tabulky. Podle toho jaký prohlížeč používáte, se vás zeptá kam chcete uložit soubory, nebo soubory budou staženy automaticky do výchozí složky pro stažené soubory.

Pro přístup k obnoveným souborům:

1. Stáhněte odpovídající Quarantine Tool pro váš operační systém ze stránky **Help & Support** nebo z následují adresy:
   - Nástroj Karanténa pro Windows
   - Nástroj Karanténa pro Linux

   Poznámka
   Nástroj Karanténa pro Linux je archivován v souboru `tar`.

2. Zapněte spustitelný soubor Nástroje Karanténa.



Nástroj Karanténa

3. V nabídce **Soubor** klikněte na **Otevřít** (CTRL+O), nebo klikněte na tlačítko **Otevřít** pro načtení archivu do nástroje.

   Soubory jsou v archivu organizovány podle virtuálního zařízení, na kterém byly nalezeny, a zachovávají svou původní cestu.
4. Pokud je v systému zapnuté antimalwarové skenování při přístupu, ujistěte se, že ho před extrahováním archivovaných souborů vypnete nebo nastavíte výjimku ze skenování pro umístění, do kterého budete soubory extrahovat. V opačném případě, váš antimalwarový program detekuje a provede akci na extraktovaných souborech.

5. Vyberte soubory k extrakci.
6. V menu **File**, klikněte **Extract** (CTRL+E) nebo klikněte na tlačítko **Extract**.
7. Vyberte cílovou složku. Soubory budou extrahovány do vybraného umístění, se zachováním původní struktury složky.

Automatické odstranění souborů v karanténě

Ve výchozím stavu se soubory v karanténě starší než 30 dní automaticky odstraní. Toto nastavení může být změněno upravením pravidla přiřazeného ke spravovaným koncovým bodům.

Pro změnu intervalu automatického odstranění souborů v karanténě:

1. Jděte na záložku **Práva**
2. Vyhledejte pravidlo přiřazené ke koncovým bodům, na kterých chcete změnit nastavení, a klikněte na jeho jméno.
3. Přejděte na stránku **Antimalware > Nastavení**.
4. V sekci **Karanténa** vyberte počet dní, po kterém budou soubory odstraněny.
5. Kliknutím na tlačítko **Uložit** aplikujete změny.

Ruční odstranění souborů z karantény

Pokud chcete ručně odstranit soubory v karanténě, měli byste se nejprve ujistit, že vybrané soubory nepotřebujete.

Sám soubor může být malware. Pokud zjistíte, že jste v takové situaci, můžete prohledat karanténu na specifickou hrozbu a odstranit ji z karantény.

Pro odstranění jednoho nebo více souborů z karantény:

1. Přejděte na stránku **Karanténa**.
2. Zvolte **Počítače a virtuální stroje** z výběru zobrazení dostupného v horní části stránky.
3. Označte pole příslušící k souborům v karanténě, které chcete odstranit.
4. Klikněte na tlačítko **Smazat** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

   Ve sloupci **Akce** si můžete povšimnout stavu čekání.

   Požadovaná akce je odeslána na cílové koncové body okamžitě, nebo hned poté, co jsou znovu online. Jakmile je soubor odstraněn, odpovídající záznam zmizí z tabulky Karanténa.

Vyprázdnění karantény.

Pro vymazání všech objektů v karanténě:

1. Přejděte na stránku **Karanténa**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Klikněte na tlačítko **Vyprázdnění Karantény (Empty Quarantine)**.

   Je nutné potvrdit kliknutím na **Ano**.

Všechny záznamy budou z karantény smazány. Požadovaná akce je odeslána na cílové koncové body okamžitě, nebo hned poté, co jsou znovu online.

11.3. Karanténa Exchange Serverů

Karanténa Exchange obsahuje emaily a přílohy. Modul Antimalware ukládá do karantény přílohy emailů, zatímco Antispam, Filtrování obsahu a Filtrování příloh uloží do karantény celý email.

Poznámka
Mějte prosím na paměti, že karanténa pro Exchange servery vyžaduje na oddílu, na kterém je nainstalovaný bezpečnostní agent, místo na pevném disku navíc. Velikost karantény závisí na počtu uložených položek a jejich velikosti.

11.3.1. Zobrazení detailů Karantény

Stránka **Karanténa** vám nabízí podrobné informace o souborech v karanténě ze všech Exchange Serverů ve vaší organizaci. Informace jsou dostupné v tabulce Karanténa a v okně s podrobnostmi o každé položce.

V tabulce Karanténa jsou uvedeny následující informace:

- **Předmět.** Předmět emailu uloženého do karantény.
- **Odesílatel.** Emailová adresa odesílatele tak, jak je zobrazena v poli **Od** v hlavičce emailu.
- **Adresáti.** Seznam adresátů tak, jak jsou uvedeni v hlavičce emailu v polích **Pro** a **Cc**.
- **Skuteční adresáti.** Seznam emailových adres jednotlivých uživatelů, na které měl být email odeslán předtím, než byl uložen do karantény.

- **Stav.** Stav objektu poté, co byl oskenován. Stav ukazuje, zda email označený jako spam obsahuje nežádaný obsah, nebo jestli je jeho příloha nakažená malwarem, podezřelá z nákazy, nežádaná, nebo neskenovatelná.
- **Jméno malwaru.** Název, který malwarové hrozbě přidělili pracovníci výzkumu zabezpečení Bitdefender.
- **Jméno serveru.** Jméno hostitele serveru, na kterém byla hrozba odhalena.
- **Vloženo do karantény v.** Datum a čas, kdy byl objekt vložen do karantény.
- **Stav opatření.** Stav opatření, které bylo přijato pro soubor v karanténě. Tímto způsobem můžete rychle zjistit, zda je opatření stále ve frontě, nebo bylo neúspěšné.

Poznámka

- Ve výchozím zobrazení jsou sloupce **Skuteční adresáti**, **Jméno malwaru** a **Jméno serveru** skryty.
- Když je více příloh z toho samého emailu uložených do karantény, v tabulce Karanténa se každá příloha zobrazí jako samostatný záznam.

Pro úpravu podrobností o karanténě zobrazených v tabulce:

1. Klikněte na tlačítko **Columns** na pravé straně záhlaví tabulky.
2. Vyberte sloupce, které chcete zobrazit.

   Pro obnovení výchozího zobrazení sloupců klikněte na tlačítko **Obnovit**.

Více informací získáte kliknutím na odkaz **Předmět** odpovídající každé položce. Zobrazí se okno **Podrobnosti objektu**, které vám poskytne následující informace:

- **Objekt v karanténě.** Typ objektu v karanténě, což může být buď email, nebo příloha.
- **Vloženo do karantény v.** Datum a čas, kdy byl objekt vložen do karantény.
- **Stav.** Stav objektu poté, co byl oskenován. Stav ukazuje, zda email označený jako spam obsahuje nežádaný obsah, nebo jestli je jeho příloha nakažená malwarem, podezřelá z nákazy, nežádaná, nebo neskenovatelná.
- **Jméno přílohy.** Název souboru přílohy odhalené moduly Antimalwarové filtrování nebo Filtrování příloh.

- **Jméno malwaru.** Název, který malwarové hrozbě přidělili pracovníci výzkumu zabezpečení Bitdefender. Tyto informace jsou dostupné pouze v případě, že byl objekt infikovaný,
- **Bod detekce.** Objekt je detekován buď na úrovni přenosu, nebo v emailové schránce nebo ve veřejné složce z Exchange Store.
- **Shodné pravidlo.** Pravidlo ze zásad, se kterým byla hrozba spárována.
- **Server.** Jméno hostitele serveru, na kterém byla hrozba odhalena.
- **IP odesílatele.** IP adresa odesílatele.
- **Odesílatel (Od).** Emailová adresa odesílatele tak, jak je zobrazena v poli **Od** v hlavičce emailu.
- **Adresáti.** Seznam adresátů tak, jak jsou uvedeni v hlavičce emailu v polích **Pro** a **Cc**.
- **Skuteční adresáti.** Seznam emailových adres jednotlivých uživatelů, na které měl být email odeslán předtím, než byl uložen do karantény.
- **Předmět.** Předmět emailu uloženého do karantény.

Poznámka
Symbol pro elipsu na konci textu značí, že část textu byla vynechána. V tomto případě přesuňte kurzor myši nad text pro jeho zobrazení v nápovědě.

11.3.2. Soubory v karanténě

Emaily a soubory uložené do karantény modulem Exchange Protection jsou uloženy na serveru lokálně jako šifrované soubory. Pomocí Kontrolního centra máte možnost obnovit emaily z karantény a také možnost odstranit nebo uložit jakékoli soubory a emaily v karanténě.

Obnovení emailů z karantény

Pokud se rozhodnete, že email z karantény nepředstavuje hrozbu, můžete ho z karantény propustit. Pomocí služeb Exchange Web Services, Exchange Protection posílá emaily z karantény jejich zamýšleným příjemcům jako přílohu notifikačního emailu Bitdefender.

Poznámka
Obnovit můžete pouze emaily. Pro obnovení přílohy z karantény ji musíte uložit do místní složky na Exchange serveru.

Pro obnovení jednoho nebo více emailů:

1. Přejděte na stránku **Karanténa**.
2. Z výběru zobrazení v horní části stránky zvolte **Exchange**.
3. Označte pole odpovídající emailům, které chcete obnovit.
4. Klikněte na tlačítko **Obnovit** v horní části tabulky. Zobrazí se okno **Obnovení poverení**.
5. Vyberte pověření uživetele Exchange s oprávněním posílat emaily na obnovu. Pokud jsou pověření, která chcete použít, nová, musíte je nejprve přidat do Správce pověření.

   Pro přidání požadovaných oprávnění:

   a. Zadejte potřebné informace do odpovídajících polí v hlavičce tabulky:
      - Uživatelské jméno a heslo uživatele Exchange.

        Poznámka
        Uživatelské jméno musí obsahovat jméno domény, jako v `user@domain` nebo `domain\user`.

      - Emailovou adresu uživatele Exchange, která je nezbytná pouze v případě, že se liší od uživatelského jména.
      - URL služeb Exchange Web Services (EWS), nezbytné pro případ, že Exchange Autodiscovery nefunguje. To se obvykle stává u serverů Edge Transport v DMZ.

   b. Klikněte na tlačítko **Přidat** v pravé části tabulky. Nová sada pověření je přidána do tabulky.
6. Klikněte na tlačítko **Obnovit**. Zobrazí se potvrzovací okno.

   Požadovaná akce je okamžitě odeslána na cílové servery. Jakmile je email obnoven, je také vymazán z karantény, takže z tabulky Karanténa zmizí jemu odpovídající záznam.

   Stav obnovovací akce můžete kontrolovat na kterémkoli z těchto míst:

   - Sloupec **Stav opatření** v tabulce Karanténa.
   - Stránka **Síť > Úlohy**.

Ukládání souborů v karanténě

Pokud chcete vyšetřit nebo obnovit data ze souborů v karanténě, můžete tyto soubory uložit do lokální složky na Exchange Serveru. Bitdefender Endpoint Security Tools soubory dešifruje a uloží je do specifikovaného umístění.

Pro uložení jednoho nebo více souborů z karantény:

1. Přejděte na stránku **Karanténa**.
2. Z výběru zobrazení v horní části stránky zvolte **Exchange**.
3. Filtrujte údaje v tabulce pro zobrazení všech souborů, které chcete uložit, tak, že zadáte termíny pro vyhledávání do polí v hlavičce tabulky.
4. Označte pole příslušící k souborům v karanténě, které chcete obnovit.
5. Klikněte na tlačítko **Uložit** v horní části tabulky.
6. Zadejte cestu k cílové složce na Exchange Serveru. Pokud složka na serveru neexistuje, bude vytvořena.

   Důležité
   Tuto složku musíte vynechat ze skenování na systémové úrovni, nebo budou soubory přesunuty do Karantény počítačů a virtuálních strojů. Další informace viz „Výjimky“ (str. 280).

7. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Ve sloupci **Stav opatření** si můžete povšimnout stavu čekání. Stav akce můžete prohlížet také na stránce **Síť > Úlohy**.

Automatické odstranění souborů v karanténě

Ve výchozím stavu, se soubory v karanténě starší než 30 dní jsou automaticky smazány. Toto nastavení můžete změnit upravením pravidel přiřazených ke spravovanému Exchange Serveru.

Pro změnu intervalu automatického odstranění souborů v karanténě:

1. Jděte na záložku **Práva**
2. Klikněte na jméno pravidla přiřazeného k Exchange Serveru, který vás zajímá.
3. Přejděte na stránku **Exchange Protection > Obecné**.
4. V sekci **Nastavení** vyberte počet dní, po kterém budou soubory odstraněny.

5. Kliknutím na tlačítko **Uložit** aplikujete změny.

Ruční odstranění souborů z karantény

Pro odstranění jednoho nebo více souborů z karantény:

1. Přejděte na stránku **Karanténa**.
2. Ve výběru zobrazení vyberte **Exchange**.
3. Označte pole odpovídající souborům, které chcete odstranit.
4. Klikněte na tlačítko ⊖ **Smazat** v horní části tabulky. Je nutné potvrdit kliknutím na **Ano**.

   Ve sloupci **Stav opatření** si můžete povšimnout stavu čekání.

   Požadovaná akce je okamžitě odeslána na cílové servery. Jakmile je soubor odstraněn, odpovídající záznam zmizí z tabulky Karanténa.

Vyprázdnění karantény.

Pro vymazání všech objektů v karanténě:

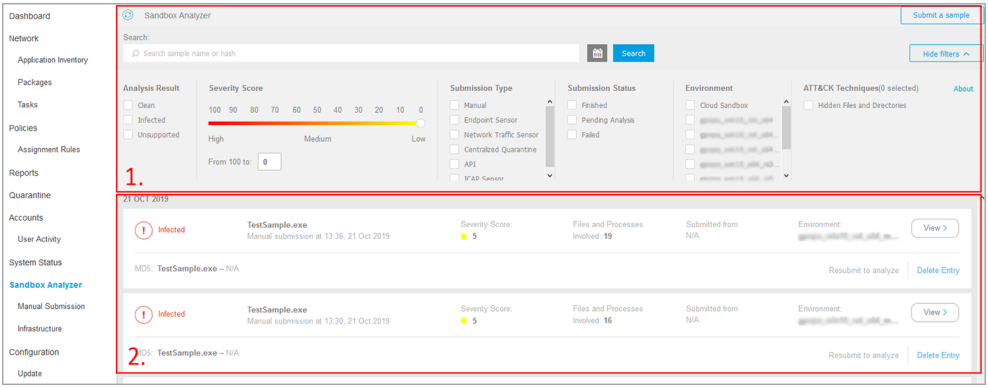
1. Přejděte na stránku **Karanténa**.
2. Vyberte **Exchange** z výběru náhledu.
3. Klikněte na tlačítko **Vyprázdnění Karantény (Empty Quarantine)**.

   Je nutné potvrdit kliknutím na **Ano**.

Všechny záznamy budou z karantény smazány. Požadovaná akce je poslána okamžitě na cílový objekt v síti.

12. POUŽITÍ SANDBOX ANALYZER

Stránka **Sandbox Analyzer** poskytuje unifikované jednotné rozhraní pro porhlížení , filtrování a vyhledávání automatických a manuálních podání do prostředí sandboxu. Stránka **Sandbox Analyzer** se skládá ze dvou oblastí:



Stránka Sandbox Analyzer

1. **oblast filtrování** umožňuje vyhledávat a filtrovat příspěvky podle různých kritérií: jméno, hash, datum, výsledek analýzy, status, detonační prostředí a techniky MITRE's ATT&CK
2. V části **submission cards area** jsou zobrazeny všechny příspěvky v kompaktním formátu s podrobnými informacemi o každém z nich.

Na záložce Sandbox Analyzer můžete provádět následující akce:

- Filtrování karet podaných vzorků
- Prohlédněte si seznam podaných vzorků a podrobnosti analýzy
- Smazání karet podaných vzorků
- Proveďte manuální podání

12.1. Filtrování karet podaných vzorků

Tohle můžete dělat v oblasti filtrů:

- Filtrujte příspěvky podle různých kritérií. Stránka se automaticky aktualizuje a načítá pouze karty bezpečnostních událostí odpovídající vybraným kritériím.
- Vypněte filtry klepnutím na tlačítko **Vymazat filtry**.
- Vypněte filtry klepnutím na tlačítko **Vymazat filtry** Skryté možnosti můžete znovu zobrazit klepnutím na tlačítko **Zobrazit filtry**.

Můžete filtrovat vzorky v Sandbox Analyzeru pomocí následujících kritérií:

- **Ukázkový název a hash (MD5)**. Do vyhledávacího pole zadejte část nebo celé jméno nebo hash vzorku, který hledáte, a klikněte na tlačítko **Hledat** na pravé straně.
- **Datum**. Pro filtrování podle datumu:
  1. Klikněte na ikonu kalendáře pro konfiguraci časového úseku.
  2. Definujte interval. Klepnutím na tlačítka **Od** a **K** v horní části kalendáře vyberte data určující časový interval. Můžete také vybrat přednastavené období z pravé strany seznamu voleb, relativně k aktuálnímu času (například posledních 30 dnů).

     Můžete si také vyspecifikovat hodinu a minutu pro každý datum časového intervalu, použitím volby pod kalendářem.
  3. Klepnutím na tlačítko **OK** se aplikuje filtr.
- **Výsledky Analýzy**. Vyberte jednu nebo více z následujících možností:
  - **Čistý (Clean)** – vzorek je bezpečný.
  - **Infikovaný (Infected)** – vzorek je nebezpečný.
  - **Nepodporovaný (Unsupported)** – vzorek má formát který Sandbox Analyzer nemohl detonovat. Pro zobrazení kompletního seznamu souborů podporovanýchSandbox Analyzerem, se podívejte na„Podporované typy souborů a přípony pro ruční odesílání“ (str. 570).
- **Skóre závažnosti**. Hodnota označuje, jak nebezpečný je vzorek na stupnici od 100 do 0 (nula). Čím vyšší je skóre, tím nebezpečnější je vzorek. Skóre závažnosti se týká všech odeslaných vzorků, včetně těch, které mají stav **Čistý** nebo **Nepodporovaný**.
- **Typ podání**. Vyberte jednu nebo více z následujících možností:
  - **Ruční**. Sandbox Analyzer obdržel vzorek přes možnosti **Ručního odeslání** .

  - **Senzor na koncovém bodě**. Bitdefender Endpoint Security Tools poslal vzorek do Sandbox Analyzer na základě nastavení politik.
  - **Senzor síťového provozu** . Síťový senzor poslal vzorek místní instanci Sandbox Analyzer na základě nastavení zásad.
  - **Centralizovaná karanténa** . GravityZone poslal vzorek místní instanci Sandbox Analyzer na základě nastavení zásad.
  - **API**. Vzorek byl odeslán do místní instance Sandbox Analyzer pomocí metod API.
  - **ICAP sensor**. Security Server odeslal vzorek do místní instance Sandbox Analyzer po naskenování serveru ICAP.
- **Stav podání**. Zaškrtněte jedno nebo více z následujících políček:
  - **Dokončeno** - Sandbox Analyzer dodal výsledek analýzy
  - **Čekající analýza** – Sandbox Analyzer spouští/odpaluje vzorek.
  - **Selhalo** – Sandbox Analyzer nemohl spustit/odpálit vzorek.
- **Prostředí** . Jsou zde uvedeny virtuální stroje dostupné pro detonaci, včetně Sandbox Analyzer umístěného u společností Bitdefender .. Zaškrtnutím jednoho nebo více políček zobrazíte, u jakých vzorků došlo k detonaci v různých prostředích
- **ATT&CK techniques**. Pokud je to relevantní, tak tato možnost filtrování umožňuje integraci s MITRE's ATT&CK znalostní databází. Hodnoty ATT&CK technik se dynamicky mění na základě bezpečnostních událostí.

  Klikněte na **O (About)** pro otevření ATT&CK Matrix v novém štítku.

12.2. Zobrazení podrobností analýzy

Stránka **Sandbox Analyzer** zobrazuje karty podání (submission cards) podle dnů, v opačném chronologickém pořadí. Karty k odeslání obsahují následující údaje:

- Výsledky Analýzy
- Název vzorku
- Typ podání
- Skóre závažnosti
- Spojené soubory a procesy
- Detonační prostředí
- Hash hodnota (MD5)

- ATT&CK techniques
- Stav odeslání, pokud není výsledek k dispozici

Každá předložená karta obsahuje odkaz na podrobnou zprávu o analýze HTML, pokud je k dispozici. Chcete-li přehled otevřít, klepněte na tlačítko **Zobrazit** na pravé straně karty.

Zpráva HTML poskytuje rozsáhlé informace uspořádané na několika úrovní, s popisem, grafikou a obrazovkami, které ilustrují chování vzorku v detonačním prostředí. To je to, co se můžete naučit z HTML zprávy Sandbox Analyzer:

- Obecné údaje o analyzovaném vzorku, například: název a klasifikace malwaru, podrobnosti o zaslání (název souboru, typ a velikost, hash, doba odeslání a doba trvání analýzy).
- Výsledky behaviorální analýzy, které zahrnují všechny bezpečnostní události zachycené během detonace, jsou uspořádány do sekcí. Bezpečnostní události se týkají:
  - Psaní / odstraňování / přesouvání / kopírování / nahrazování souborů v systému a na vyměnitelných jednotkách.
  - Spuštění nově vytvořených souborů.
  - Změny v systému souborů.
  - Změny provedené na aplikacích spuštěných uvnitř virtuálního stroje.
  - Změny na hlavním panelu systému Windows a Start menu.
  - Tvorba / ukončení / zavedení procesů.
  - Psaní / odstranění klíčů registru.
  - Tvorba mutex objektů
  - Tvorba / spuštění / zastavení / upravování / dotazování / odstraňování služeb.
  - Změna bezpečnostních nastavení prohlížeče.
  - Změna nastavení zobrazení Průzkumníku Windows.
  - Přidání souborů na seznam výjimek firewallu.
  - Změna nastavení sítě
  - Povolení spuštění při startu systému.
  - Připojení ke vzdálenému hostiteli.
  - Přístup k určitým doménám.
  - Přenos dat z a na určité domény.
  - Přístup k URL, IP a portům skrze různé komunikační protokoly.
  - Kontrolování indikátorů virtuálního prostředí.
  - Kontrola indikátorů monitorovacích nástrojů.
  - Tvorba snímků.

- SSDT, IDT, IRP hooks.
- Paměťové skládky pro podezřelé procesy.
- Volání funkcí Windows API.
- Být neaktivní během určitého časového úseku pro pozdržení spuštění.
- Tvorba souborů s akcemi, které mají být spouštěny v určitých časových intervalech.

Důležité
Hlášení HTML jsou k dispozici pouze v angličtině, bez ohledu na jazyk, který používáte v GravityZone Control Center.

12.3. Opakované odeslání vzorku

V oblasti odeslaných karet můžete již odeslané vzorky odeslat znovu místní instanci Sandbox Analyzer, aniž byste je museli znovu nahrávat. Můžete to udělat pro vzorky dříve odeslané do místní instance Sandbox Analyzer pomocí jakéhokoli senzoru nebo metody, automaticky, ručně nebo prostřednictvím API.

K znovuodeslání vzorku:

1. Na odesílací kartě klikněte na **Znovu odeslat k analýze** .
2. V konfiguračním okně ponechte nastavení z předchozího zadání nebo je změňte následovně:
   a. V části **Správa obrazů** vyberte obraz virtuálního počítače, který chcete použít k detonaci.
   b. V části **Nastavení detonace** nakonfigurujte následující nastavení:
      i. **Časový limit pro detonace vzorků (minuty)**. Přidělte přesnou délku času v minutách pro provedení kompletní analýzy vzorku. Výchozí hodnota je 4 minuty, ale někdy může analýza trvat déle. Na konci nakonfigurovaného intervalu Sandbox Analyzer přeruší analýzu a vygeneruje zprávu založenou na datech shromážděných do tohoto okamžiku. Pokud je analýza přerušena před dokončením, může obsahovat nepřesné výsledky.
      ii. **Povolený počet znovuspuštění**. V případě neočekávaných chyb, se pokusí Sandbox Analyzer detonovat vzorek tolikrát, kolikrát jak je zde nastaveno dokud nedokončí analýzu. Standartní hodnota je 2. To znamená, že Sandbox Analyzer se bude v případě chyby ještě dvakrát pokoušet o odpálení/spuštění vzorku.

iii. **Předfiltrování**. Tuto možnost vyberte, chcete-li vyloučit vzorky detonace, které již byly analyzovány.

iv. **Přístup do internetu během detonace**. Během analýzy některé vzorky vyžadují připojení k internetu, aby se dokončila analýza. Pro dosažení nejlepšího výsledku doporučujeme ponechat tuto možnost zapnutou.

c. V části **Detonační profil** můžete upravit úroveň složitosti analýzy chování a zároveň ovlivnit propustnost Sandbox Analyzer. Pokud je například nastaveno na **Vysoká**, Sandbox Analyzer provede přesnější analýzu na menším počtu vzorků ve stejném intervalu než na **Střední** nebo **Nízká**.

3. Klikněte na **Znovu odeslat** .

Po opětovném odeslání se na stránce **Sandbox Analyzer** zobrazí nová karta a retence dat pro tento vzorek se odpovídajícím způsobem prodlouží.

Poznámka
Možnost **Znovu odeslat k analýze** je k dispozici pro vzorky stále přítomné v datovém úložišti Sandbox Analyzer. Zkontrolujte, zda je uchovávání dat nakonfigurováno na stránce **Sandbox Analyzer > Sandbox Manager** nastavení zásad.

12.4. Smazání karet podaných vzorků

Chcete-li odstranit kartu odeslání, kterou již nepotřebujete:

1. Přejděte na kartu, kterou chcete odstranit.
2. Klikněte na možnost **Smazat položku** na levé straně karty.
3. Klikněte na **Ano (Yes)** pro potvrzení úlohy.

Poznámka
Pokud budete následovat tyto kroky, tak smažete pouze kartu podání (submission card). Informace ohledně podání budou nadále dostupné v reportu **Sandbox Analyzer (Odmítnuté)**. Tato zpráva bude i nadále podporována po omezenou dobu.

12.5. Ruční odeslání

Z **Sandbox Analyzer > Manuální podání (Manual Submission)**, můžete zaslat vzorky podezdřelých objektů do Sandbox Analyzeru, za účelem zjištění zda jsou to hrozby nebo neškodné soubory. Na sekci **Ruční odeslání** se dostanete také kliknutím na tlačítko **Vložte vzorek** v pravé horní části oblasti v sekci filtrování v Sandbox Analyzer.

Poznámka
Sandbox Analyzer manuální zaslání je kompatibilní s všemi webovými prohlížeči požadovanými pro Control Center, s vyjímkou Internet Explorer 9. Pro zaslání objektu do Sandbox Analyzer, se zalogujte do Control Center použitím kteréhokoliv podporovaného prohlížeče zmíněném v „Připojování se k Control Center“ (str. 19).

Sandbox Analyzer > Ruční odeslání

Odeslání vzorků do Sandbox Analyzer:

1. Na stránce **Upload** v části **Samples** vyberte typ objektu:
   a. **Soubory**. Klepnutím na tlačítko **Procházet** vyberte objekty, které chcete odeslat pro analýzu chování. V případě archivů chráněných heslem můžete definovat jedno heslo pro každé nahrání relace ve vyhrazeném poli. Během procesu analýzy Sandbox Analyzer aplikuje zadané heslo na všechny odeslané archivy.
   b. **URL**. Vyplňte odpovídající pole libovolnou adresou URL, kterou chcete analyzovat. Za každou relaci můžete odeslat pouze jednu adresu URL.
2. V části **Nastavení detonace** nakonfigurujte parametry analýzy pro aktuální relaci:
   - Instance Sandbox Analyzer, kterou chcete použít. Můžete vybrat Cloud nebo Sandbox Analyzer mistní instanci

     Pokud se rozhodnete použít lokálníSandbox Analyzer, můžete vybrat více virtuálních strojů, kam můžete poslat vzorky najednou.
   - **Argumenty příkazového řádku**. Argumenty v příkazovém řádku můžete libovolně přidávat pro upravu chování určitých programů, například spustitelných souborů. Argumenty příkazového řádku platí pro všechny předložené vzorky během analýzy.
   - **Spouštět vzorky individuálně**. Zaškrtněte políčko, chcete-li analyzovat soubory ze svazku jeden po druhém.
3. V části **Detonační profil** můžete upravit úroveň složitosti analýzy chování a zároveň ovlivnit propustnost Sandbox Analyzer. Pokud je například nastaveno na **Vysoká**, Sandbox Analyzer provede přesnější analýzu na menším počtu vzorků ve stejném intervalu než na **Střední** nebo **Nízká**.
4. Na stránce **Obecná nastavení** můžete provádět konfigurace, které se vztahují na všechny ruční odesílání, bez ohledu na relaci:

a. **Časový limit pro detonace vzorků (minuty)**. Přidělte přesnou délku času v minutách pro provedení kompletní analýzy vzorku. Výchozí hodnota je 4 minuty, ale někdy může analýza trvat déle. Na konci nakonfigurovaného intervalu Sandbox Analyzer přeruší analýzu a vygeneruje zprávu založenou na datech shromážděných do tohoto okamžiku. Pokud je analýza přerušena před dokončením, může obsahovat nepřesné výsledky.

b. **Povolený počet znovuspuštění**. V případě neočekávaných chyb, se pokusí Sandbox Analyzer detonovat vzorek tolikrát, kolikrát jak je zde nastaveno dokud nedokončí analýzu. Standartní hodnota je 2. To znamená, že Sandbox Analyzer se bude v případě chyby ještě dvakrát pokoušet o odpálení/spuštění vzorku.

c. **Předfiltrování**. Tuto možnost vyberte, chcete-li vyloučit vzorky detonace, které již byly analyzovány.

d. **Přístup do internetu během detonace**. Během analýzy některé vzorky vyžadují připojení k internetu, aby se dokončila analýza. Pro dosažení nejlepšího výsledku doporučujeme ponechat tuto možnost zapnutou.

e. Kliknutím na tlačítko **Uložit** aplikujete změny.

5. Přejděte zpět na stránku **Upload**.
6. Klikněte na tlačítko **ODESLAT**. Indikátor průběhu označuje stav odeslání.

   Po odeslání se na stránce zobrazí nová karta.**Sandbox Analyzer** Po dokončení analýzy karta poskytne souhrn informací včetně podrobností

Poznámka
Pro ruční odeslání vzorků do Sandbox Analyzer musíte mít oprávnění **Spravovat sítě**.

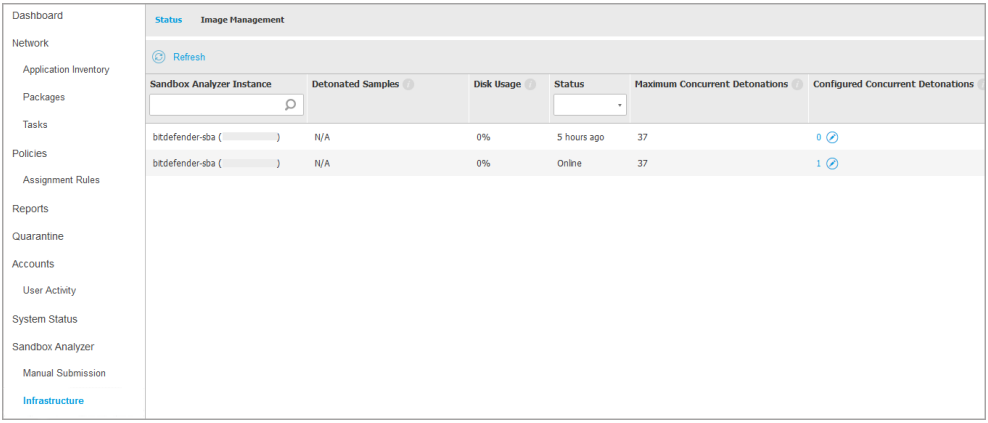
12.6. Správa infrastruktury Sandbox Analyzer

V sekci **Sandbox Analyzer > Infrastruktura** můžete provádět následující akce související s lokálně nainstalovanou instancí Sandbox Analyzer:

- Zkontrolujte stav instance Sandbox Analyzer
- Konfigurace souběžných detonací
- Zkontrolujte stav obrazů(images) virtuálního stroje
- Konfigurace a správa obrazů(image) virtuálních strojů

12.6.1. Kontrola stavu Sandbox Analyzer

Po nasazení a konfiguraci virtuálního zařízení Sandbox Analyzer na hypervizoru ESXi můžete získat informace o místní instanci Sandbox Analyzer ze stránky **Status** .



Sandbox Analyzer > Infrastructure > Status

Tabulka poskytuje následující podrobnosti:

- **Sandbox Analyzer jméno instance** . Každé jméno odpovídá instanci Sandbox Analyzer nainstalované na jednom hypervizoru ESXi. Sandbox Analyzer můžete nainstalovat na více hypervizorů ESXi.
- **Detonované vzorky** . Hodnota označuje počet vzorků analyzovaných od doby, kdy byla instance Sandbox Analyzer licencována poprvé.
- **Využití disku**. Procento označuje množství místa na disku spotřebovaného v datovém úložišti Sandbox Analyzer.
- **Status**. V tomto sloupci uvidíte, zda je instance Sandbox Analyzer online, offline, není nainstalována, probíhá instalace nebo instalace selhala.
- **Maximální souběžné detonace** . Hodnota představuje maximální počet virtuálních počítačů, které může Sandbox Analyzer vytvořit pro detonaci vzorků. V daném čase může jeden virtuální stroj provést jednu detonaci. Počet virtuálních počítačů je určen množstvím hardwarových prostředků dostupných na ESXi.

- **Konfigurované souběžné detonace**. Toto je skutečný počet virtuálních počítačů vytvořených na základě dostupné licence.
- **Použít proxy** . Klepnutím na přepínač Zapnuto/Vypnuto povolíte nebo zakážete komunikaci mezi instancemi GravityZone Control Center a Sandbox Analyzer prostřednictvím serveru proxy. Chcete-li nastavit proxy, přejděte na **Nastavení a Proxy** v hlavní nabídce Control Center. Pokud není nastaven žádný proxy server, Control Center tuto možnost ignoruje.

  Podrobnosti o konfiguraci serveru proxy naleznete v **Instalace ochrany GravityZone, Instalace a nastavení, Konfigurovat Nastavení Control Center, Proxy** v instalační příručce GravityZone.

  Poznámka
  Control Center používá tento proxy pouze ke komunikaci s instancemi Sandbox Analyzer On-Premises. Ke komunikaci s cloudovou instancí Sandbox Analyzer používá Control Center proxy server nakonfigurovaný na stránce Sandbox Analyzer nastavení zásad.
  Tento server proxy se také liší od serveru nakonfigurovaného na stránce **Obecná nastavení** nastavení zásad, která zajišťuje komunikaci mezi koncovými body a komponentami GravityZone.

Sloupce můžete vyhledávat a filtrovat podle názvu a stavu instance Sandbox Analyzer. Pomocí tlačítek v pravém horním rohu tabulky obnovte stránku a zobrazte a skryjte filtry a sloupce.

12.6.2. Konfigurace souběžných detonací

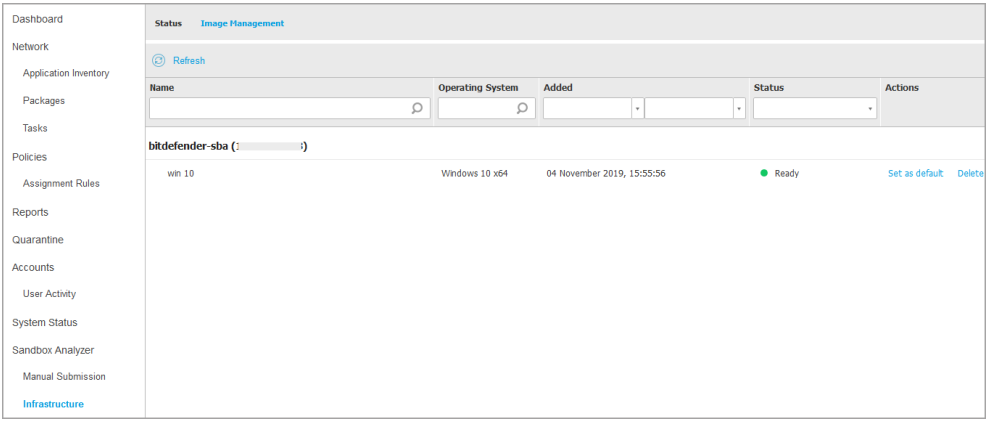
Na stránce **Status** můžete nakonfigurovat souběžné detonace představující počet virtuálních strojů, které mohou současně spouštět a detonovat vzorky v instanci Sandbox Analyzer. Počet souběžných detonací závisí na hardwarových prostředcích a distribuci licenčních slotů ve více instancích Sandbox Analyzer.

K nastavení souběžných detonací:

1. Klikněte na číslo nebo na ikonu **Upravit** ve sloupci **Konfigurované souběžné detonace** .
2. V novém okně zadejte v odpovídajícím poli počet souběžných detonací, které chcete přiřadit instanci Sandbox Analyzer.
3. Klikněte na tlačítko **Save**.

12.6.3. Kontrola stavu obrazů(images) VM

Sandbox Analyzer používá obrazy virtuálních strojů jako prostředí detonace k provádění behaviorální analýzy na odeslaných vzorcích. Stav virtuálních strojů můžete zkontrolovat na stránce **Správa obrazů(images)** .



Sandbox Analyzer > Infrastructure > Image Management

V tabulce jsou uvedeny následující podrobnosti:

- **Název** dostupných obrazů virtuálních strojů, jak je uvedeno v konzole zařízení Sandbox Analyzer. Více obrazů virtuálních strojů je seskupeno do stejné instance Sandbox analyzátoru.
- **Operační systém** , jak je uvedeno v konzole zařízení Sandbox Analyzer.
- Čas přidání obrazu virtuálního stroje.
- **Status**. V tomto sloupci zjistíte, zda je obraz virtuálního stroje nový a lze jej připravit k detonaci, zda je připraven k detonaci nebo proces přípravy selhal.
- **Akce**. V tomto sloupci se dozvíte, co můžete s obrazy virtuálních strojů dělat, v závislosti na jejich stavu: vytváření obrazů pro detonaci, jejich nastavení jako výchozího detonačního prostředí nebo jejich odstranění.

12.6.4. Konfigurace a správa obrazů VM

Budování detonačních virtuálních strojů

Chcete-li detonovat vzorky pomocí místní instance Sandbox Analyzeru , musíte vytvořit vyhrazené virtuální stroje. Stránka **Správa obrazů** umožňuje vytvářet detonační virtuální stroje za předpokladu, že jste do konzoly zařízení Sandbox Analyzer přidali obrazy VM.

Poznámka
Informace o tom, jak přidat obrazy VM do konzoly zařízení Sandbox Analyzer, naleznete v kapitole **Instalace Sandbox Analyzer Virtual Appliance** v Instalační příručce GravityZone.

Chcete-li vytvořit detonační virtuální stroje, ve sloupci **Akce** klikněte na možnost **Sestavit obraz** pro obrazy VM se stavem: **Nový - Vyžaduje sestavení** . Vytvoření virtuálního počítače obvykle vyžaduje 15 až 30 minut v závislosti na jeho velikosti. Po dokončení sestavení se stav virtuálních strojů změní na **Připraveno** .

Konfigurace výchozího virtuálního počítače

V instanci Sandbox Analyzer může být nainstalováno a nakonfigurováno více obrazů(images) jako detonační virtuální stroje. V případě automatického odeslání Sandbox Analyzer použije první sestavený obraz(image) VM k detonaci vzorků.

Toto chování můžete změnit nakonfigurováním výchozího obrazu(image) VM. Chcete-li to provést, klikněte na možnost **Nastavit jako výchozí** u preferovaného obrazu(image) VM.

Odstranění virtuálních počítačů

Chcete-li odstranit obraz(image) virtuálního počítače ze stránky **Image Management** , klikněte na **Delete** v sloupci **Akce** . V potvrzovacím okně klikněte na **Odstranit obraz** .

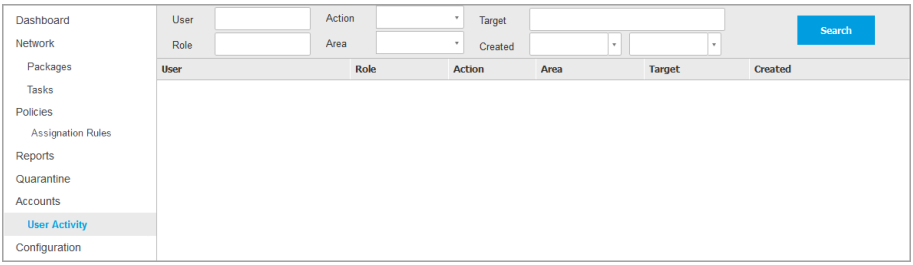
13. PROTOKOL AKTIVITY UŽIVATELE

Control Center zaznamenává všechny operace a akce prováděné uživateli. Záznam aktivity uživatele zahrnuje následující události, v souladu s úrovní vašich oprávnění správce:

- Přihlašování a odhlašování
- Tvorba, úprava, přejmenování a mazání hlášení
- Přidávání a odebírání portletů ovládací desky
- Tvorba, úprava a mazání pověření
- Tvorba, úprava, stahování a mazání síťových balíčků
- Vytváření síťových úloh
- Spuštění, ukončení, zrušení a zastavení procesů odstraňování problémů na postižených počítačích
- Tvorba, úprava, přejmenování a mazání uživatelských účtů
- Mazání nebo přemisťování cílových bodů mezi skupinami
- Tvorba, přemisťování, přejmenování a mazání skupin
- Odstranění a obnovení souborů z karantény
- Tvorba, úprava a mazání uživatelských účtů
- Vytváření, editace a mazání pravidel práv přístupu.
- Tvorba, úprava, přejmenování, přiřazení a mazání pravidel
- Úpravy nastavení ověřování pro účty GravityZone.
- Vytváření, editování, synchronizace a mazání Amazon EC2 integrací
- Vytváření, editování, synchronizace a mazání Microsoft Azure integrací
- Aktualizování zařízení GravityZone .

Pro prohlídku záznamů o činnostech uživatele přejděte na stránku **Účty > Aktivita uživatele** a zvolte požadované zobrazení sítě z nastavení zobrazení.

Pro prohlídku záznamů o činnostech uživatele přejděte na stránku **Aktivita uživatele** a zvolte požadované zobrazení sítě z výběr zobrazení.



Stránka Aktivity uživatele

Pro zobrazení zaznamenaných událostí, které vás zajímají, musíte definovat vyhledávání. Vyplňte do prázdných polí kritéria vyhledávání a klikněte na tlačítko **Hledat**. V tabulce se zobrazí všechny záznamy, které se shodují s kritérii vašeho vyhledávání.

Sloupce tabulky vám poskytují užitečné informace o zaznamenaných událostech:

- Uživatelské jméno toho, kdo akci provedl.
- Roli uživatele.
- Akce, která způsobila událost.
- Typ objektu konzole, který byl akcí ovlivněn.
- Konkrétní objekt konzole, který byl akcí ovlivněn.
- Čas, kdy k události došlo.

Pro seřazení událostí podle konkrétního sloupce jednoduše klikněte na hlavičku toho sloupce. Pro otočení pořadí řazení klikněte znovu na hlavičku sloupce.

Pro zobrazení podrobných informací o události, vyberte ji a podívejte se do sekce pod tabulkou.

14. POUŽÍVÁNÍ NÁSTROJŮ

14.1. Zavedení vlastních nástrojů s HVI

Bitdefender HVI vás osvobodí od zátěže s nahlašováním problémů, sbíráním forenzních údajů nebo prováděním pravidelných údržbářských prací na virtuálních strojích ve vašem prostředí Citrix tím, že vám umožní vložení nástrojů od třetí strany do hostujících operačních systémů. Tyto operace jsou prováděny skrze API Direct inspect (připojení TCP/IP není nutné), aniž by rušily koncové uživatele. Pro tento účel je nutné, aby nástroje mohly pracovat tiše.

GravityZone vám poskytne 3 GB místa, ve kterém můžete držet své nástroje v bezpečí a odkud je můžete vložit ho hostujících operačních systémů.

Pro nahrání nástrojových sad do GravityZone:

1. Stáhněte si nejnovější verzi nástrojové sady na váš počítač.
2. Archivujte sadu do souboru ZIP.
3. Přejděte na GravityZone Control Center a klikněte na menu **Nástroje** v levé spodní části stránky. Zobrazí se stránka **Centrum správy nástrojů**.
4. Klikněte na příslušné nahrávací tlačítko v horní části tabulky, podle cílového operačního systému: **Nahrát nástroj pro Windows** nebo **Nahrát nástroj pro Linux**.
5. Pokud je nástroj pro Windows, musíte zvolit také příslušnou počítačovou architekturu z rozbalovací nabídky.
6. Najděte soubor ZIP, vyberte ho a poté klikněte na **Otevřít**.

   V případě velkých souborů se může stát, že nahrávání zabere několik minut. Jakmile se dokončí, nástroj bude přidán do tabulky, a ukazatel průběhu nad ní aktualizuje informace o zbývajícím volném místě pro budoucí nahrávání.

Společně s názvem nástroje, tabulka zobrazuje další užitečné detaily, jako například:

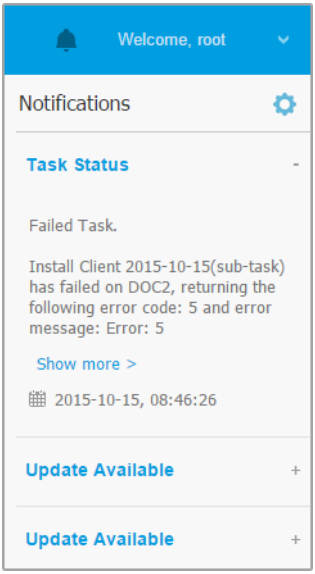
- Operační systém a platforma, na které nástroj pracuje.
- Stručný popis nástroje. Toto pole můžete upravit kdykoli se vám bude chtít.
- Jméno uživatele, který nahrál nástroj.
- Stav nahrávání. Zkontrolujte toto pole a ujistěte se, že byl nástroj úspěšně nahrán.
- Datum a čas nahrání.

Příště můžete prostřednictvím pravidel naplánovat, kdy nástroje zavést, nebo je můžete zavést kdykoli tím, že spustíte úlohy na stránce **Síť**.

Když už nástroje nevyužíváte, zvolte je a poté klikněte na tlačítko **Odstranit** v horní části tabulky , čímž je smažete. Je nutné potvrdit kliknutím na **Ano**.

15. UPOZORNĚNÍ

V závislosti na událostech, které se mohou dít napříč vaší sítí, bude Control Center zobrazovat nejrůznější upozornění, aby vás informovala o stavu zabezpečení vašeho prostředí. Oznámení se zobrazují v **Oznamovací oblasti** umístěné na pravé straně Control Center.



Oznamovací oblast

Když jsou v síti zjištěny nové události, ikona 11 v pravé horní části Control Center ukazuje počet nově zjištěných událostí. Kliknutím na ikonu zobrazíte Oznamovací oblast, kde najdete seznam zjištěných událostí.

15.1. Typy oznámení

Toto je seznam dostupných typů hlášení:

Malwarová epidemie

Toto upozornění je odesláno uživatelům, z jejichž celkového počtu spravovaných síťových objektů je alespoň 5% nakažených tím samým malwarem.

Práh malwarové epidemie můžete nastavit dle svých potřeb v okně **Nastavení oznámení**. Další informace viz „Konfigurace Nastavení upozornění“ (str. 545).

Hrozby detekované HyperDetectem jsou mimo rozsah tohoto upozornění.

Vypršení licence

Toto upozornění je zasíláno 30, 7 a 1 den před vypršením licence.

Pro prohlížení tohoto upozornění musíte mít oprávnění **Spravovat firmu**.

Dostupný Syslog format: JSON, CEF

Byl dosažen limit užívání licence

Toto upozornění je zasíláno, když byly všechny dostupné licence již využity.

Dostupný Syslog format: JSON, CEF

Brzy bude dosažen limit užívání licence

Toto upozornění je zasíláno, když bylo využito 90% dostupných licencí.

Pro prohlížení tohoto upozornění musíte mít oprávnění **Spravovat firmu**.

Dostupný Syslog format: JSON, CEF

Byl dosažen limit pro využití licencí serverů

Toto oznámení se odešle, když počet chráněných serverů dosáhne limitu uvedeného v licenčním klíči.

Pro prohlížení tohoto upozornění musíte mít oprávnění **Spravovat firmu**.

Dostupný Syslog format: JSON, CEF

Limit licencí pro servery je téměř dosažen

Toto oznámení je zasláno, v případě dosažení 90% dostupných licenčních míst pro servery.

Pro prohlížení tohoto upozornění musíte mít oprávnění **Spravovat firmu**.

Dostupný Syslog format: JSON, CEF

Byl dosažen limit užívání licence Exchange

Toto upozornění je vyvoláno pokaždé, když počet chráněných emailových schránek z vašich Exchange serverů dosáhne limitu určeného na vašem licenčním klíči.

Pro prohlížení tohoto upozornění musíte mít oprávnění **Spravovat firmu**.

Dostupný Syslog format: JSON, CEF

Neplatné přihlašovací údaje uživatele Exchange

Toto upozornění je zasíláno, když na cílovém Exchange serveru nemohlo být zahájeno skenování na vyžádání kvůli neplatným přihlašovací údaje uživatele Exchange.

Dostupný Syslog format: JSON, CEF

Stav aktualizací

Toto upozornění je vyvoláno každý týden, pokud jsou ve vaší síti nalezeny starší verze produktu.

Dostupný Syslog format: JSON, CEF

Aktualizace k dispozici

Toto upozornění vás informuje o dostupnosti nového GravityZone, nového balíčku nebo aktualizaci produktu.

Dostupný Syslog format: JSON, CEF

Internetové připojení

Toto upozornění je vyvoláno v případě, že jeden z následujících procesů zjistí změny v připojení k internetu:

- Validace licence
- Získání Požadavku na podpis certifikátu společnosti Apple
- Komunikace s mobilními zařízeními Apple a Android
- Přístup k účtu MyBitdefender

Dostupný Syslog format: JSON, CEF

Připojení SMTP

Toto upozornění je odesláno pokaždé, když Bitdefender GravityZone zjistí změny týkající se připojení poštovního serveru.

Dostupný Syslog format: JSON, CEF

Uživatelé mobilních zařízení bez emailové adresy

Toto upozornění je odesláno po přidání mobilních zařízení k více uživatelům, a jeden nebo několik z těchto uživatelů nemá žádnou emailovou adresu přiřazenou ke svému účtu. Toto upozornění vás má varovat, že uživatelé bez žádné zadané emailové adresy nemohou přidávat svá přiřazená zařízení, protože podrobnosti o aktivaci jsou automaticky zasílány přes email.

Pro více podrobností o přidávání mobilních zařízení k několika uživatelům se podívejte do Průvodce instalací GravityZone.

Dostupný Syslog format: JSON, CEF

Záloha databáze

Toto upozornění vás informuje o stavu plánovaného zálohování databáze, ať už úspěšného či neúspěšného. Pokud se databázi nepodařilo zálohovat, ve zprávě s upozorněním najdete také důvod selhání.

Pro podrobnosti o konfiguraci záloh databáze GravityZone se podívejte do Průvodce instalací GravityZone.

Dostupný Syslog format: JSON, CEF

Zjištěn malware na Exchange

Tato notifikace vás informuje, že byl detekován malware na Exchamge Serveru ve vaší síti.

Dostupný Syslog format: JSON, CEF

Pokročilý Anti-Exploit

Toto oznámení informuje, že Advanced Anti- Exploit zjistil pokus o zneužití ve vaší síti.

Dostupný Syslog format: JSON, CEF

Antimalwarová událost

Toto upozornění vás informuje při zjištění přítomnosti malwaru na koncovém zařízení ve vaší síti. Toto oznámení je vytvořeno pro každou detekci malwaru a poskytuje podrobnosti o infikovaném koncovém bodu (jméno, IP, nainstalovaný agent), typ kontroly, detekovaný malware, verzi podpisu, dobu detekce a typ skenovacího stroje.

Dostupný Syslog format: JSON, CEF

Mimo synchronizaci Integrace

Tato notifikace je zaslána jakmile se existující integrace virtuální platformy nemůže synchronizovat s GravityZone. V nastaveních notifikací si můžete vybrat integrace, pro které chcete být notifikováni, jakmile se objeví synchronizační chyby. Můžete si zjistit více informací o stavech synchronizace v detailech notifikací (hlášení).

Dostupný Syslog format: JSON, CEF

Antiphishingová událost

Toto upozornění vás informuje pokaždé, když agent na koncovém bodě zablokuje přístup na známou phishingovou stránku. V tomto upozornění naleznete také podrobnosti, jako je koncový bod, který se pokusil o přístup k

nebezpečné stránce (jméno a IP), instalovaného agenta nebo zablokovanou URL.

Dostupný Syslog format: JSON, CEF

Událost Firewallu

Toto upozornění vás informuje pokaždé, když modul firewall nainstalovaného agenta zablokuje skenování portu nebo přístup aplikace k síti, v souladu s platnými pravidly.

Dostupný Syslog format: JSON, CEF

Událost ATC/IDS

Toto upozornění je odesláno pokaždé, když je na koncovém bodě ve vaší síti zjištěna a zablokována potenciálně nebezpečná aplikace. Naleznete podrobnosti o typu aplikace, názvu a cestě, stejně jako ID nadřazeného procesu a cestu a příkazový řádek, který proces zahájil, pokud se jedná o tento případ.

Dostupný Syslog format: JSON, CEF

Událost Kontroly uživatele

Toto upozornění je vyvoláno pokaždé, když klient na koncovém bodě zablokuje činnost uživatele, jako je prohlížení webu nebo aplikace softwaru, v souladu s platnými pravidly.

Dostupný Syslog format: JSON, CEF

Událost Ochrany dat

Toto upozornění je odesláno pokaždé, když je na koncovém bodě zablokován přenos dat v souladu s pravidly ochrany dat.

Dostupný Syslog format: JSON, CEF

Událost produktových modulů

Toto upozornění je odesláno při každém zapnutí nebo vypnutí bezpečnostního modulu nainstalovaného agenta.

Dostupný Syslog format: JSON, CEF

Událost stavu Security Serveru

Tento typ upozornění obsahuje informace o změnách stavu určitého Security Serveru nainstalovaného ve vaší síti. Změny stavu Security Serveru odkazují k následujícím událostem: vypnutý / zapnutý, aktualizace produktu, aktualizace signatur a požadovaný restart.

Dostupný Syslog format: JSON, CEF

Událost přetíženého Security Serveru

Toto upozornění je odesláno, když zatížení skenování na Security Serveru ve vaší síti překročí určený práh.

Dostupný Syslog format: JSON, CEF

Událost registrace produktu

Toto upozornění vás informuje, když se změní registrační stav agenta nainstalovaného ve vaší síti.

Dostupný Syslog format: JSON, CEF

Kontrola autentizace

Toto upozornění vás informuje, když byl použit jiný učet GravityZone, než je váš, k přihlášení se do Control Center pomocí nerozpoznaného zařízení.

Dostupný Syslog format: JSON, CEF

Přihlášení se z nového zařízení

Toto upozornění vás informuje, že váš účet GravityZone byl použit pro přihlášení se do Control Center ze zařízení, které jste k tomuto účelu nikdy dřív nepoužili. Upozornění je automaticky nastaveno tak, aby bylo viditelné v Control Center i emailu, a prohlížet ho můžete jen vy.

Dostupný Syslog format: JSON, CEF

Certifikát vyprší

Toto upozornění vás informuje o tom, že platnost bezpečnostního certifikátu vyprší. Upozornění je odesíláno 30, sedm a jeden den před datem vypršení lhůty.

Dostupný Syslog format: JSON, CEF

Stav úloh

Toto upozornění vás informuje při každé změně stavu úlohy, nebo pouze při dokončení úlohy, podle vašich preferencí.

Dostupný Syslog format: JSON, CEF

Zastaralý aktualizační server

Toto oznámení se odešle, když má aktualizační server ve vaší síti zastaralý bezpečnostní obsah.

Dostupnost formátu Syslog: JSON, CEF

Síťové události

Toto oznámení se odešle pokaždé, když modul Network Attack Defense zjistí pokus o útok ve vaší síti. Toto upozornění vás také informuje, zda byl pokus o útok proveden z venčí nebo z kompromitovaného koncového bodu uvnitř sítě. Mezi další podrobnosti patří data o koncovém bodu, technika útoku, IP adresa útočníka a provedené akce Network Attack Defense.

Dostupný Syslog format: JSON, CEF

Zjištěné narušení paměti

Toto upozornění vás informuje, když HVI zjistí útok, který narušuje paměť chráněných virtuálních strojů v prostředí Citrix Xen. Hlášení vám poskytne důležité detaily, jako například název a IP nakaženého stroje, popis incidentu, zdroj a cíl útoku, opatření provedená pro odstranění hrozby, a čas detekce.

Upozornění se tvoří pro následující incidenty:

- Pokusy o využití paměťové oblasti jinak, než zamýšlel hypervizor, skrze Rozšířené tabulky stránek (EPT).
- Pokusy o zavedení kódu do jiných procesů.
- Pokusy o změnu adres procesů v překladových tabulkách.
- Pokusy o změnu Modelově specifických registrů (MSR).
- Pokusy o změnu obsahu specifických položek ovladače nebo tabulky deskriptorů přerušení (IDT).
- Pokusy o načtení konkrétních Kontrolních registrů (CR) s neplatnými hodnotami.
- Pokusy o načtení konkrétních Rozšířených kontrolních registrů (XCR) s neplatnými hodnotami.
- Pokusy o změnu Globálního nebo Tabulek deskriptorů přerušení.

Poznámka
Funkce HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Dostupný Syslog format: JSON, CEF

Nová aplikace v inventáři aplikací

Toto upozornění vás informuje, když Kontrola aplikací zjistí novou aplikaci nainstalovanou na monitorovaných koncových bodech.

Dostupný Syslog format: JSON, CEF

Detekce Sandbox Analyzeru

Toto oznámení vás upozorní vždy, když Sandbox Analyzer zjistí novou hrozbu mezi odeslanými vzorky. Zobrazí se vám podrobnosti, jako je název hostitele nebo IP koncového bodu, čas a datum detekce, typ hrozby, path, název, velikost souborů a provedená akce u každého z nich.

> **Poznámka**
> O čistých analyzovaných souborech vám nebudou zasílána upozornění. Informace o všech odeslaných vzorech jsou k dispozici v přehledu **Sandbox Analyzer Výsledky (Neschválené)** a v přehledu **Sandbox Analyzer** V hlavní nabídce Control Center.

Dostupný Syslog format: JSON, CEF

Činnost HyperDetectu

Toto upozornění vás informuje, když HyperDetect nalezne v síti jakékoli antimalwarové nebo neblokované události. Toto upozornění je odesláno při každé události v HyperDetect a poskytuje následující informace:

- Informace o zasaženém koncovém bodě (název, IP, instalovaný agent).
- Typ a název malwaru
- Infikovaná cesta k souboru. V případě bezsouborových útoků je mu poskytnuto jméno spustitelného souboru použitého při útoku.
- Stav infekce
- SHA256 hash malwarového spustitelného souboru
- Typu zamýšleného útoku (cílený útok, grayware, exploity, ransomware, podezřelé soubory a síťový přenos)
- Úroveň detekce (tolerantní, normální, agresivní)
- Čas a datum detekce

Dostupný Syslog format: JSON, CEF
Můžete si prohlédnout podrobnosti o infekci a provést hlubší vyšetření problémů tak, že vytvoříte hlášení **Činnost HyperDetectu** přímo na stránce **Upozornění**. K tomu, aby jste to provedli:

1. V Control Center, klikněte na tlačítko **Upozornění (Notification)** pro zobrazení oblasti upozorněni (Notification Area).

2. Klikněte na odkaz **Zobrazit více** na konci upozornění pro otevření stránky **Upozornění**.
3. V detailech hlášení klikněte na tlačítko **Zobrazit hlášení**. Tímto se otevře konfigurační okno.
4. Pokud je třeba, upravte hlášení. Další informace viz „Vytváření hlášení“ (str. 497).
5. Klikněte na tlačítko **Vytvořit**.

Poznámka
Pro vyhnutí se spamování vám bude zasíláno vždy maximálně jedno upozornění za hodinu.

Mimo synchronizaci Integrace
Toto oznámení vás informuje o problémech spojených s integrací a synchronizací. K tomu může dojít z různých důvodů, jako jsou například podrobnosti o integraci, které se změnily, nebo dočasná nedostupnost serveru.

Dostupný Syslog format: JSON, CEF

Problém chybějící opravy
K tomuto upozornění dochází, když koncovým bodům ve vaší síti chybí jeden nebo více balíčků.

GravityZone automaticky zasílá oznámení obsahující všechna zjištění za posledních 24 hodin do data oznámení.

Můžete se podívat, které koncové body jsou v této situaci tak, že kliknete na tlačítko **Zobrazit hlášení** v detailech upozornění.

Ve výchozím stavu se upozornění týká bezpečnostních balíčků, ale můžete ho nastavit tak, aby vás informovalo i o s bezpečností nesouvisejících balíčcích.

Dostupný Syslog format: JSON, CEF

Nový Incident
Toto oznámení vás informuje, když dojde k nové události. Po povolení se oznámení vygeneruje pokaždé, když se v Řídicím centru v sekci **Incidenty** zobrazí nový incident. Odpovídající událost syslog obsahuje seznam relevantních položek extrahovaných z podrobností o incidentu, které můžete použít k obohacení korelací řízených bezpečnostními informacemi a správou událostí (SIEM). Další informace zobrazíte kliknutím na **Název incidentu** .

Dostupný Syslog format: JSON, CEF

Detekce Ransomware

Toto oznámení vás informuje, když GravityZone zjistí útok ransomwaru ve vaší síti. Jsou vám poskytnuty podrobnosti týkající se cíleného koncového bodu, uživatele, který byl přihlášen, zdroje útoku, počtu šifrovaných souborů a času a data útoku.

V době, kdy obdržíte oznámení, je útok již blokován.

Odkaz v oznámení vás přesměruje na stránku **Aktivita ransomwaru** , kde můžete zobrazit seznam šifrovaných souborů a v případě potřeby je obnovit.

Dostupný Syslog format: JSON, CEF

Antimalwarové Úložiště

Upozornění je zasláno jakmile je na ICAP-kompatibilním úložném zařízení (storage device) škodlivý kód detekován. Toto upozornění je vytvořeno pro každou detekci škodlivého kódu, obsahující detailní informace o infikovaném úložním zařízení (Jméno, IP adresa, druh), detekovaném škodlivém kódu (malware) a času detekce.

Dostupný Syslog format: JSON, CEF

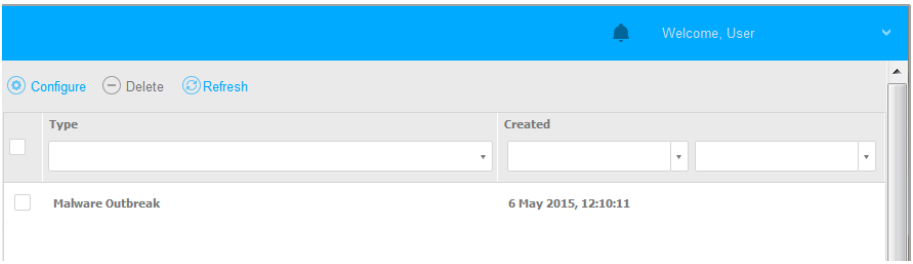
Blokovaná zařízení

Toto oznámení se spustí, když se k koncovému bodu připojí blokované zařízení nebo zařízení s oprávněním jen pro čtení. Pokud se stejné zařízení připojí vícekrát za hodinu, během tohoto intervalu se odešle pouze jedno oznámení. Pokud se zařízení po jedné hodině znovu připojí, spustí se nové oznámení.

Dostupný Syslog format: JSON, CEF

15.2. Prohlížení upozornění

Pro zobrazení upozornění klikněte na tlačítko **Upozornění** a poté klikněte na **Zobrazit všechna upozornění**. Zobrazí se tabulka se všemi hlášeními.



Stránka Upozornění

V závislosti na počtu upozornění může tabulka zabrat několik stran (ve výchozím stavu je zobrazeno pouze 20 objektů na stránku).

Pro pohyb mezi stránkami použijte navigační tlačítka ve spodní části tabulky.

Můžete změnit počet položek zobrazených na stránku tak, že vyberete nějakou z menu umístěného vedle navigačních tlačítek.

Pokud je záznamů příliš mnoho, můžete použít vyhledávací pole pod hlavičkami sloupců nebo filtrovací menu navrchu stránky pro filtrování zobrazených údajů.

- Pro filtrování upozornění zvolte požadovaný typ upozornění, která chcete prohlížet, z nabídky **Typ**. Nebo můžete zvolit časový interval, během kterého bylo upozornění vytvořeno, a snížit tak počet záznamů v tabulce, zvláště pro případ velkého množství vygenerovaných upozornění.
- Pro zobrazení detailů upozornění klikněte na jeho název v tabulce. Pod tabulkou se zobrazí sekce **Detaily**, kde můžete vidět událost, která upozornění vytvořila.

15.3. Mazání upozornění

Pro odstranění upozornění:

1. Klikněte na tlačítko **Oznamovací oblast** na pravé straně panelu nabídky a poté klikněte na **Zobrazit všechna upozornění**. Zobrazí se tabulka se všemi hlášeními.
2. Vyberte upozornění, která chcete odstranit.
3. Klikněte na tlačítko **Smazat** v horní části tabulky.

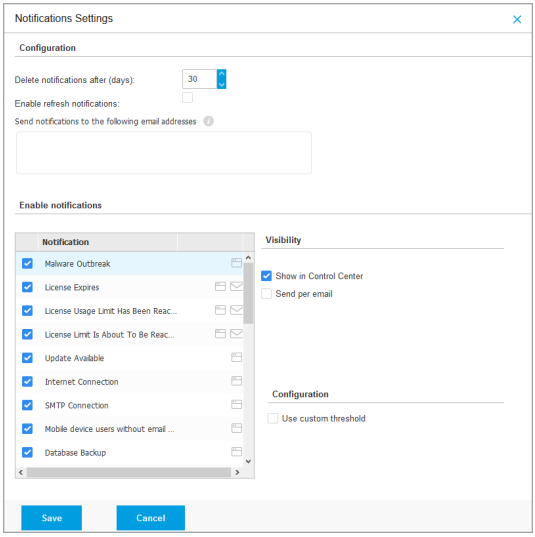
Můžete také nastavit upozornění tak, aby se mazala automaticky po určeném počtu dní. Další informace viz „Konfigurace Nastavení upozornění“ (str. 545).

15.4. Konfigurace Nastavení upozornění

Všechny typy upozornění k odeslání a emailové adresy, na které jsou odeslány, lze nastavit pro každého uživatele.

Pro nastavení parametrů upozornění:

1. Klikněte na tlačítko **Oznamovací oblast** na pravé straně panelu nabídky a poté klikněte na **Zobrazit všechna upozornění**. Zobrazí se tabulka se všemi hlášeními.
2. Klikněte na tlačítko **Nastavit** v horní části tabulky. Zobrazí se okno **Nastavení upozornění**.



Nastavení oznámení

Poznámka
K oknu **Nastavení upozornění** můžete přistupovat také přímo pomocí ikony **Nastavit** z pravého horního rohu okna **Oznamovací oblasti**.

3. V sekci **Konfigurace** můžete definovat následující parametry:
   - Automatické mazání upozornění po určitém časovém období. Nastavte libovolné číslo mezi 0 a 365 do pole **Odstranit upozornění po (dnech)**.

- Označte pole **Povolit obnovení upozornění**, pokud chcete, aby se oznamovací oblast automaticky aktualizovala každých 60 sekund.
- Navíc můžete posílat upozornění emailem konkrétním příjemcům. Zadejte emailové adresy do určeného pole a po každé z nich stiskněte `Enter`.

4. V sekci **Povolit upozornění** si můžete zvolit typ upozornění, který chcete přijímat od GravityZone. Můžete nastavit také viditelnost a možnosti odesílání jednotlivě pro každý typ oznámení.

   Ze seznamu vyberte požadovaný typ oznámení. Další informace viz „Typy oznámení“ (str. 534). Zatímco typ upozornění je vybraný, můžete nastavit jeho konkrétní možnosti (pokud dostupné) v oblasti na pravé straně:

Viditelnost

- **Zobrazit v Control Center** určuje, že se tento typ události zobrazí v Control Center, prostřednictvím tlačítka **Oznámení (Notifications)**.
- **Přihlásit se k serveru** určuje, že tento typ události je posílán také do souboru `syslog`, pokud je syslog nastaven.

  Pro postup při konfiguraci syslog serverů se podívejte do Průvodce instalací GravityZone.
- **Odeslat přes email** určuje, že tento typ události je také zasílán na určité emailové adresy. V tomto případě musíte zadat emailové adresy do příslušného pole a po zadání každé z nich stisknout `Enter`.

Konfigurace

- **Použít vlastní práh** - vám umožní definovat práh pro dějící se události, ze kterých je odesláno upozornění.

  Například, upozornění o Malwarové infekci je ve výchozím nastavení odesláno uživatelům, z jejichž všech spravovaných síťových objektů je alespoň 5% nakažených tím samým malwarem. Pro změnu hodnotu prahu malwarové infekce, povolte možnost **Použít vlastní práh** a zadejte požadovanou hodnotu do pole **Práh malwarové infekce**.
- Pro upozornění **Zálohování databáze** si můžete zvolit možnost obdržet upozornění pouze v případě, že zálohování databáze selhalo. Nechte tuto

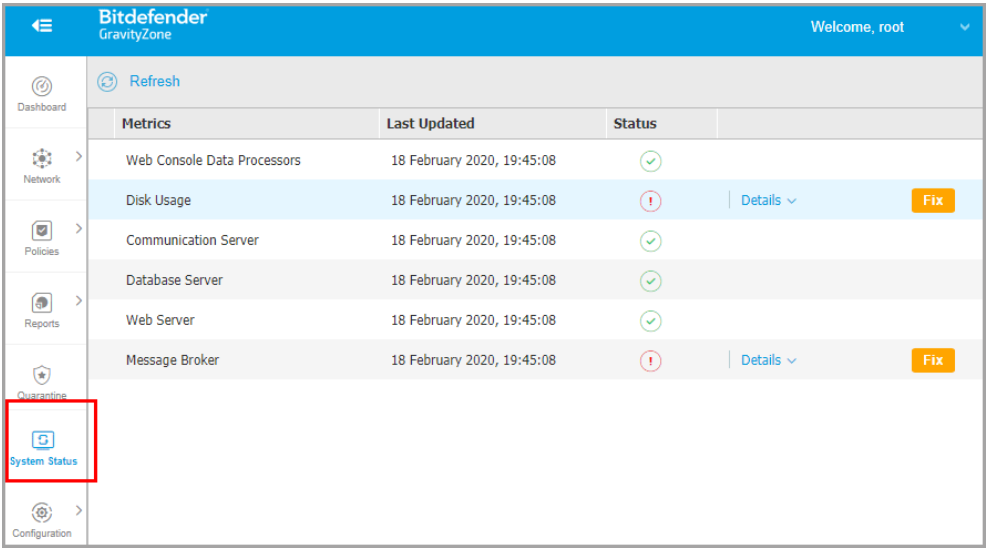
možnost neoznačenou, pokud chcete být upozorňováni na všechny události týkající se zálohování databáze.

- Pro **Stavovou událost Security Server** můžete vybrat události Security Serveru, které vyvolají tento typ upozornění:
  - **Zastaralý** - upozorní vás pokaždé, když je Security Server ve vaší síti zastaralý.
  - **Powered off** - informuje pokaždé Security Server ve vaší síti, že byl vypnut.
  - **Vyžaduje restart** - upozorní vás pokaždé, když Security Server ve vaší síti potřebuje restartovat.
- Pro **Stav úlohy** můžete vybrat typ stavu, který vyvolá tento typ upozornění:
  - **Jakýkoli stav** - upozorní při každém odeslání úlohy z Control Center v jakémkoli stavu.
  - **Pouze nezdařené** - upozorní vás pokaždé, když úloha odeslaná z Control Center selže.

5. Klikněte na tlačítko **Save**.

16. STAV SYSTÉMU

Stránka **Stav systému** zobrazuje informace o stavu nasazení GravityZone, takže Vám usnadňuje prohlížení, když se něco pokazí. Stránka poskytuje systémové metriky, jejich stav a datum, kdy byly naposledy aktualizovány, všechny zobrazené v tabulce.



Stránka stavu systému

Sloupec **Metriky** zobrazuje všechny indikátory sledované pomocí GravityZone Control Center. Další podrobnosti o všech metrikách a stavových zprávách naleznete v „Datové procesory“ (str. 572).

Sloupec **Poslední aktualizace** zobrazuje datum a čas poslední kontroly stavu metriky.

Sloupec **Stav** zobrazuje stav každé metriky: **OK** nebo **Pozor**. **Stav** metriky je aktualizován každých 15 minut nebo pokaždé, když kliknete na tlačítko **Refresh**.

16.1. OK Status

Stav OK znamená, že se metrika chová normálně. V tomto případě se nezobrazí žádné další podrobnosti.

16.2. Stav pozornosti

Stav označuje, že metrika nefunguje v rámci normálních parametrů.

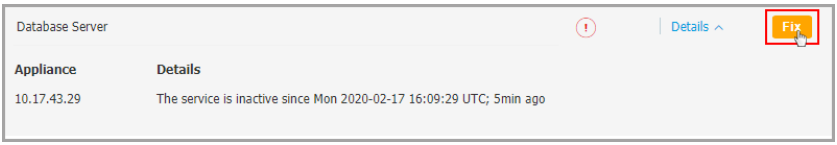
V tomto případě je třeba dále prozkoumat, co se stalo, a vyřešit aktuální problémy:

1. Kliknutím na tlačítko **Detaily** rozbalte další informace týkající se metriky pod kontrolou.

Detaily metriky

- V části **Appliance** najdete IP adresy dotčených počítačů
- V části **Podrobnosti** můžete zobrazit informace specifické pro každou metriku.

2. Kliknutím na **Oprava** opravíte metriku a o zbytek se postará GravityZone.



Detaily metriky

Stav metriky se jednou změní zpět na **OK** v případě že bylo opraveno.

Poznámka
V případě jakýchkoli dalších problémů souvisejících s metrikami kontaktujte tým technické podpory .

16.3. Metriky

Stránka **System Status** obsahuje podrobnosti o následujících metrikách:

- Webová Console Procesorů dat
- Používání disku
- Komunikační server
- Databázový Server
- Webový Server
- Zprostředkovatel zpráv

Webová Console Procesorů dat

Tato metrika sleduje stav datových procesorů, které se používají pro kompilaci dat zobrazených v Control Center.

pozor zpráva o stavu	Podrobnosti
`Procesory, které na tomto zařízení selhaly: <pole datových procesorů> .`	Jeden nebo více datových procesorů je zastaveno.
`Virtuální appliance je mimo provoz`	Virtuální appliance využívající služby webové konzole je vypnuto.

Úplný seznam procesorů používaných Control Center viz „Datové procesory“ (str. 572).

Používání disku

Tato metrika sleduje množství místa na disku použitého v každé virtuální applianci, kolik volného místa zbývá, stejně jako celkový prostor na disku. Pokud je některý z disků použit nad 80%, metrika zobrazí ! **Pozor** status.

pozor zpráva o stavu	Podrobnosti
`Využité místo na disku (název disku)`	Jeden nebo více disků se používá nad 80% jejich maximální kapacity.
`Virtuální appliance je mimo provoz`	Hlášené virtuální zařízení je vypnuté.

Komunikační server

Tato metrika sleduje propojení mezi agenty zabezpečení nainstalovanými na vašich koncových bodech a databázovém serveru.

pozor zpráva o stavu	Podrobnosti
`Služba je od této doby neaktivní <timestamp>`	Služba se zastavila.

Databázový Server

Tato metrika sleduje stav databáze GravityZone.

pozor zpráva o stavu	Podrobnosti
`Služba je od této doby neaktivní <timestamp>`	Služba se na jednom z virtuálních strojů(appliances) zastavila.
`Virtuální appliance je mimo provoz`	Virtuální zařízení používající databázový server je vypnuto.

Webový Server

Tato metrika sleduje stav webového serveru, který je hostitelem GravityZone Control Center.

pozor zpráva o stavu	Podrobnosti
`Služba je od této doby neaktivní <timestamp>`	Server se na jednom z virtualních zařízení zastavil.
`Virtuální appliance je mimo provoz`	Virtuální zařízení používající tento server je vypnuto.

Zprostředkovatel zpráv

Tato metrika sleduje stav služby zprostředkovatele zpráv na zařízeních s rolemi webové konzole a komunikačního serveru.

pozor zpráva o stavu	Podrobnosti
Na těchto zařízeních je služba zprostředkovatele zpráv vypnutá	Služba se na jednom z virtuálních strojů(appliances) zastavila.
Síťové připojení mezi zařízeními selhalo	Spojení mezi dvěma virtualnímy stroji je přerušeno.
Virtuální appliance je mimo provoz	Virtuální zařízení používající tuto službu je vypnuto.

17. ODBORNÁ POMOC

Bitdefender poskytuje svým zákazníkům bezkonkurenčně rychlou a přesnou podporu. Pokud se setkáte s jakýmkoli problémem nebo máte dotaz ohledně čehokoli na vašem produktu Bitdefender, přejděte na naše online Centrum podpory. Dodá vám několik zdrojů, kde můžete rychle najít řešení nebo odpověď. Nebo, pokud vám to tak vyhovuje lépe, můžete kontaktovat Tým péče o zákazníky Bitdefender. Naši zástupci podpory pohotově zodpoví vaše dotazy a poskytnou vám potřebnou pomoc.

Poznámka
Informace o našich poskytovaných službách podpory a zásadách podpory naleznete v Centru podpory.

17.1. Bitdefender Centrum Podpory

Bitdefender Centrum podpory je místo, kde naleznete všechnu pomoc s vaším produktem Bitdefender, kterou potřebujete.

Můžete použít několik zdrojů pro rychlé nalezení řešení nebo odpovědi:

- Články Knowledge Base
- Bitdefender Fórum Podpory
- Dokumentace produktu

Můžete také použít svůj oblíbený vyhledávač k nalezení dalších informací o počítačovém zabezpečení, produktech Bitdefender a společnosti.

Články Knowledge Base

Bitdefender Knowledge Base je online úložiště informací o produktech Bitdefender. Uchovává v snadno přístupném formátu zprávy o výsledcích probíhající technické podpory a činnostech opravy chyb týmů podpory a vývoje produktu Bitdefender, spolu s obecnějšími články o virové prevenci, správě řešení produktů Bitdefender s podrobnými vysvětleními a mnoha dalšími články.

Bitdefender Knowledge Base je přístupná veřejnosti a lze ji volně prohledávat. Rozsáhlé informace, které obsahuje, jsou dalším prostředkem poskytování potřebných technických znalostí zákazníkům produktu Bitdefender. Všechny platné žádosti o informace nebo hlášení chyb od klientů produktu Bitdefender se časem dostanou do Bitdefender Knowledge Base jako hlášení o opravách chyb, taháky

pro obcházení problémů nebo informativní články doplňující soubory nápovědy produktu.

Bitdefender Knowledge Base pro obchodní produkty je kdykoli dostupná na http://support.bitdef.cz/.

Bitdefender Fórum Podpory

Fórum podpory produktu Bitdefender poskytuje uživatelům produktu Bitdefender snadný způsob, jak získat pomoc a pomoci ostatním. Můžete vložit jakýkoliv problém nebo otázku ohledně vašeho produktu Bitdefender.

Technici podpory produktu Bitdefender sledují nové příspěvky a fóru, aby vám pomohli. Odpověď nebo řešení můžete rovněž získat od zkušenějšího uživatele produktu Bitdefender.

Před zveřejněním problému nebo otázky prohledejte fórum, jestli se na něm nenachází podobné nebo související téma.

Fórum podpory produktu Bitdefender je k dispozici na adrese https://forum.bitdefender.com v 5 různých jazycích: v angličtině, němčině, francouzštině, španělštině a rumunštině. Klikněte na odkaz **Business Protection** pro přístup k sekci věnované obchodním produktům.

Dokumentace produktu

Dokumentace produktu je ten nejkompletnější zdroj informací o vašem produktu.

Nejsnadnější způsob získání dokumentace je na stránce **Pomoc & Podpora** v Control Center. Klikněte na své uživatelské jméno v pravém horním rohu konzole, zvolte **Pomoc & Podpora** a poté odkaz průvodce, který vás zajímá. Průvodce se otevře v nové kartě vašeho prohlížeče.

17.2. Žádost o podporu

Můžete požádat o podporu pomocí online supportniho centra. Vyplňte Kontaktní formulář (contact form) a potvrďte zaslání.

17.3. Používání Nástroje podpory

Nástroj podpory GravityZone je navržen pro pomáhání uživatelům a podporujícím technikům ve snadném získání informací potřebných k odstraňování problémů. Spusťte Nástroj podpory na postižených počítačích a odešlete výsledný archiv s informacemi o odstraňování problémů zástupci podpory společnosti Bitdefender

17.3.1. Používání Nástroje podpory na operačních systémech Windows

Spuštění aplikace Nástroj podpory

Chcete-li vygenerovat protokol o postižených počítačích, použijte jednu z těchto metod:

- Příkazový Řádek

  V případě problémů s BEST nainstalovaným v počítači.

- Problém s instalací

  Pro situace, kdy BEST není v počítači nainstalována a instalace selže.

Metoda příkazového řádku

Pomocí příkazového řádku můžete sbírat protokoly přímo z postiženého počítače. Tato metoda je užitečná v situacích, kdy nemáte přístup do GravityZone Control Center nebo počítač nekomunikuje s konzolí.

1. Otevřete příkazový řádek s oprávněními pro správu.
2. Přejděte do složky pro instalaci produktu. Výchozí cesta je:

   `C:\Program Files\Bitdefender\Endpoint Security`

3. Zhromažďujte a ukládejte protokoly spuštěním tohoto příkazu:

   ```
   Product.Support.Tool.exe collect
   ```

   Protokoly jsou uloženy ve výchozím nastavení v `C:\Windows\Temp`.

   Volitelné, pokud chcete protokol nástrojů podpory uložit do vlastního umístění, zadejte vlastní cestu :

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Například:

   ```
   Product.Support.Tool.exe collect path="D:\Test"
   ```

Během provádění příkazu můžete na obrazovce sledovat průběh. Po dokončení procesu se na výstupu zobrazí název archivu obsahujícího protokoly a jeho umístění.

Chcete-li protokoly odeslat do Bitdefender Enterprise Support `C:\Windows\Temp` nebo vlastního umístění a najděte soubor archivu s názvem `ST_[název_počítače]_[aktuální datum]` . Připojte archiv k vašemu supportnímu ticketu pro další odstranění problémů.

Problém s instalací

1. Chcete-li stáhnout nástroj BEST Support Tool, klikněte zde .
2. Spusťte spustitelný soubor jako správce. Zobrazí se okno.
3. Vyberte umístění pro uložení archivu protokolů.

   Během shromažďování protokolů si na obrazovce všimnete ukazatele průběhu. Po dokončení procesu zobrazí výstup název archivu a jeho umístění.

Chcete-li protokoly odeslat na podporu společnosti Bitdefender Enterprise Support, přejděte do vybraného umístění a najděte soubor archivu s názvem `ST_[computername]_[currentdate]`. Připojte archiv k vašemu supportnímu ticketu pro další odstranění problémů.

17.3.2. Používání Nástroje podpory na operačních systémech Linux

Pro operační systémy Linux je Nástroj podpory integrovaný s bezpečnostním agentem Bitdefender.

Pro sbírání systémových informací Linux pomocí Nástroje podpory, zadejte následující příkaz:

```
# /opt/BitDefender/bin/bdconfigure
```

pomocí těchto dostupných možností:

- `--help` pro seznam všech příkazů Nástroje podpory
- `enablelogs` pro zapnutí protokolů produktu a komunikačních modulů (všechny služby se automaticky restartují)

- `disablelogs` pro zakázání protokolů produktu a komunikačních modulů (všechny služby se automaticky restartují)
- `deliverall` pro vytvoření:
  - Archiv obsahující protokoly produktu a komunikačního modulu, doručený do složky `/tmp` v následujícím formátu `bitdefender_machineName_timeStamp.tar.gz`.

    Poté, co je archiv vytvořen:

    1. Budete dotázáni, zda si přejete zakázat protokoly. Pokud je třeba, služby se automaticky restartují.
    2. Budete dotázáni, zda si přejete odstranit protokoly.
- `deliverall -default` doručí ty samé informace jako předchozí možnost, ale na protokolech budou provedena výchozí opatření bez dotazování se uživatele (protokoly budou vypnuty a odstraněny).

Můžete spustit také příkaz `/bdconfigure` přímo z balíčku BEST (plný nebo downloader), aniž byste měli produkt nainstalovaný.

Pro nahlášení problému s GravityZone, který ovlivňuje vaše systémy Linux, postupujte dle následujících kroků pomocí dříve popsaných možností:

1. Povolte protokoly produktu a komunikačního modulu.
2. Pokusit se o opětovné vyvolání problému.
3. Zakázat protokoly.
4. Vytvořte protokolový archiv.
5. Otevřete emailový lístek podpory pomocí formuláře dostupného na stránce **Pomoc & Podpora** v Control Center s popisem problému a připojeným protokolovým archivem.

Nástroj podpory pro Linux poskytuje následující informace:

- Složky `etc`, `var/log`, `/var/crash` (pokud dostupná) a `var/epag` z `/opt/BitDefender`, obsahující protokoly a nastavení Bitdefender.
- Soubor `/var/log/BitDefender/bdinstall.log`, obsahující instalační informace
- Soubor `network.txt`, ve kterém jsou uvedeny informace o nastavení sítě / připojení stroje

- Soubor `product.txt`, včetně obsahu všech souborů `update.txt` z `/opt/BitDefender/var/lib/scan` a kompletní rekurzivní seznam všech souborů z `/opt/BitDefender`
- Soubor `system.txt`, obsahující obecné systémové informace (distribuce a kernelové verze, dostupná RAM a volné místo na pevném disku)
- Soubor `users.txt` s uživatelskými informacemi
- Další informace ohledně produktu související se systémem, jako jsou externí připojení procesů a využití CPU
- Systémové protokoly

17.3.3. Používání Nástroje podpory na operačních systémech Mac

Při posílání žádosti Týmu technické podpory Bitdefender je nutné uvést následující:

- Podrobný popis problému, se kterým jste se setkali.
- Screenshot (pokud proveditelný) přesně té chybové zprávy, která se vám zobrazuje.
- Protokol Nástroje podpory.

Pro sběr systémových informací Mac pomocí Nástroje podpory:

1. Stáhněte ZIP archiv obsahující Nástroj podpory.
2. Z archivu extrahujte soubor **BDProfiler.tool**.
3. Otevřete okno Terminálu.
4. Přejděte do umístění souboru **BDProfiler.tool**.
   Například:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. K souboru přidejte práva pro spuštění:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Spusťte nástroj.

   Například:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Až budete vyzváni k zadání hesla administrátora, stiskněte `Y` a zadejte heslo.

   Počkejte pár minut, než nástroj dokončí generování protokolu. Výsledný soubor archivu (**Bitdefenderprofile_output.zip**) naleznete na své Ploše.

17.4. Kontaktní informace

Účinná komunikace je klíčem k úspěšnému obchodu. Za uplynulých 18 let si Bitdefender vybudoval nezpochybnitelnou pověst díky neustálému usilování o lepší komunikaci s cílem překonat očekávání našich klientů a partnerů. V případě dotazů nás bez váhání kontaktujte.

17.4.1. Webové adresy

Prodejní oddělení: enterprisesales@bitdefender.com
Centrum podpory:http://support.bitdef.cz/
Dokumentace: gravityzone-docs@bitdefender.com
Lokální distributoři :http://www.bitdefender.com/partners
Partner Program: partners@bitdefender.com
Mediální vztahy: pr@bitdefender.com
Viry: virus_submission@bitdefender.com
Spam: spam_submission@bitdefender.com
Oznámení zneužívání produktu: abuse@bitdefender.com
Webová stránka: http://www.bitdefender.com

17.4.2. Lokální distributoři

Lokální distributoři produktu Bitdefender jsou připraveni zodpovědět jakékoli dotazy ohledně své oblasti působnosti jak v komerčních, tak v obecných záležitostech.

Chcete-li najít distributora produktu Bitdefender ve vaší zemi:

1. Přejděte na web http://www.bitdefender.com/partners.
2. Jděte na **Partner Locator**.

3. Informace o kontaktech na lokální Bitdefender distributory by se měla automaticky zobrazit. Pokud se tak nestane, vyberte zemi ve které se nacházíte a zobrazte si informace.
4. Pokud nenajdete distributora produktu Bitdefender ve vaší zemi, kontaktujte nás emailem na adrese enterprisesales@bitdefender.com.

17.4.3. Bitdefender Kanceláře

Pobočky produktu Bitdefender jsou připraveny zodpovědět jakékoli dotazy ohledně své oblasti působnosti jak v komerčních, tak v obecných záležitostech. Jejich příslušné adresy a kontakty jsou uvedeny níže.

Spojené státy

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (prodej&technická podpora): 1-954-776-6262
Prodej: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrum podpory: http://www.bitdefender.com/support/business.html

Francie

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
Email: b2b@bitdefender.fr
Web: http://www.bitdefender.fr
Centrum podpory: http://www.bitdefender.fr/support/business.html

Španělsko

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España

Fax: (+34) 93 217 91 28
Telefon (pobočka a prodej): (+34) 93 218 96 15
Telefon (technická podpora): (+34) 93 502 69 10
Prodej: comercial@bitdefender.es
Web: http://www.bitdefender.es
Centrum podpory: http://www.bitdefender.es/support/business.html

Německo

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (pobočka a prodej): +49 (0) 2304 94 51 60
Telefon (technická podpora): +49 (0) 2304 99 93 004
Prodej: firmenkunden@bitdefender.de
Web: http://www.bitdefender.de
Centrum podpory: http://www.bitdefender.de/support/business.html

Velká Británie a Irsko

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (prodej&technická podpora): (+44) 203 695 3415
Email: info@bitdefender.co.uk
Prodej: sales@bitdefender.co.uk
Web: http://www.bitdefender.co.uk
Centrum podpory: http://www.bitdefender.co.uk/support/business.html

Rumunsko

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (prodej&technická podpora): +40 21 2063470

Prodej: sales@bitdefender.ro
Web: http://www.bitdefender.ro
Centrum podpory: http://www.bitdefender.ro/support/business.html

Spojené arabské emiráty

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (prodej&technická podpora): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Prodej: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrum podpory: http://www.bitdefender.com/support/business.html

A. Dodatky

A.1. Podporované typy souborů

Antimalwarové skenovací nástroje obsažené v bezpečnostních řešeních společnosti Bitdefender jsou schopné skenovat všechny typy souborů, které by mohly obsahovat hrozby. Seznamy níže zahrnují nejběžnější typy souborů, které jsou analyzovány.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

```
xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo
```

A.2. Typy a stavy síťových souborů

A.2.1. Typy síťových objektů

Každý typ objektu dostupného na stránce **Síť** je označen určitou ikonou.

V tabulce níže najdete ikonu a popis pro všechny dostupné typy objektů.

Ikona	Typ
	Síťová skupina
	Počítač
	Relay počítač
	Počítač Exchange Server
	Relay Exchange Server počítač
	Virtuální stroj
	Relay virtual počítač
	Zlatý obraz
	Exchange Server virtualní počítač
	Relay Exchange Server virtualní počítač
	Virtuální stroj s vShield
	Relay virtuální stroj s vShield
	Nutanix inventář
	Nutanix Prism
	Nutanix cluster
	VMware inventář
	VMware vCenter
	Datové centrum VMware
	Zdrojový fond VMware
	VMware Klastr

Ikona	Typ
	Citrix inventář
	XenServer
	Xen Pool
	Amazon EC2 inventář (inventory)
	Integrace s Amazon EC2
	Amazon EC2 / Microsoft Azure Region
	Amazon EC2 / Microsoft Azure zóny dostupnosti
	Microsoft Azure inventář
	Microsoft Azure integrace
	Security Server
	Security Server se vShield
	Hostitel bez Security Server
	Host s Security Server
	VMware vApp
	Uživatel mobilního zařízení
	Mobilní zařízení

A.2.2. Stavy síťových objektů

Každý síťový objekt může mít různý stav ohledně stavu správy, bezpečnostních problémů, připojení a tak dále. V další tabulce najdete všechny dostupné stavové ikony a jejich popis.

Poznámka
Tabulka níže obsahuje několik typických příkladů stavu. Ty samé stavy mohou platit, jednotlivě nebo dohromady, pro všechny typy síťových objektů, jako jsou síťové skupiny, počítače a tak dále.

Ikona	Stav
	Hostitel bez Security Serveru, Odpojený
	Virtuální stroj, offline, nespravovaný

Ikona	Stav
	Virtuální stroj, online, nespravovaný
	Virtuální stroj, online, spravovaný
	Virtuální stroj, online, spravovaný, s problémy
	Virtuální stroj, čekání na restart
	Virtuální stroj, pozastaven
	Virtuální stroj, odstraněn

A.3. Typy souborů aplikací

Nástroje antimalwarového skenování obsažené v bezpečnostních řešeních Bitdefender lze nastavit tak, aby omezily skenování pouze na soubory aplikací (nebo programů). Programové soubory jsou daleko zranitelnější malwarovými útoky než ostatní druhy souborů.

Tato kategorie zahrnuje soubory s těmito příponami:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt;
accdu; acl; acr; action; ade; adp; air; app; as; asd; asp;
awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl;
csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm;
dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv;
hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu;
jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat;
mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms;
msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm;
potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf;
prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx;
rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm;
sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url;
vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk;
ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb;
xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

A.4. Typy souborů Filtrování příloh

Modul Kontrola obsahu nabízený Security for Exchange může filtrovat emailové přílohy podle typu souboru. Typy dostupné v Control Center zahrnují následující souborové přípony:

Spustitelné soubory

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Obrázky

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimédia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archivy

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Tabulky

fm3; ods; wk1; wk3; wks; xls; xlsx

Prezentace

odp; pps; ppt; pptx

Dokumenty

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Systémové proměnné

Některá z nastavení dostupných v konzoli vyžadují určení cesty na cílových počítačích. Pro jistotu, že je cesta platná na všech cílových počítačích, doporučujeme používat systémové proměnné (tam, kde je to vhodné).

Zde je seznam přednastavených systémových proměnných:

`%ALLUSERSPROFILE%`
Složka profilu Všichni uživatelé Typická cesta:

`C:\Documents and Settings\All Users`

`%APPDATA%`
Složka Application Data přihlášeného uživatele. Typická cesta:

`C:\Users\{username}\AppData\Roaming`

`%LOCALAPPDATA%`
Dočasné soubory nebo aplikace. Typická cesta:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`
Složka Program Files. Typická cesta je `C:\Program Files`.

`%PROGRAMFILES(X86)%`
Složka Program Files pro 32-bitové aplikace (na 64-bitových systémech). Typická cesta:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`
Složka Common Files. Typická cesta:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`
Složka Common Files pro 32-bitové aplikace (na 64-bitových systémech). Typická cesta:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`
Adresář Windows nebo SYSROOT. Typická cesta je `C:\Windows`.

`%USERPROFILE%`
Cesta k složce uživatelského profilu. Typická cesta:

`C:\Users\{username}`

V systému MacOS odpovídá složka profilu uživatele domovské složce. Při konfiguraci výjimek použijte `$HOME` nebo `~`.

A.6. Nástroje Kontroly aplikací

Pro nastavení pravidel Kontroly aplikací na základě hashe spustitelného souboru nebo certifikátu otisku palce, je nutné stáhnout následující nástroje:

- **Otisk prstu** pro obdržení vlastní hodnoty hashe.
- **Otisk palce** pro obdržení vlastních hodnot certifikátu otisku palce.

Otisk prstu

Klikněte zde pro stažení spustitelného souboru Otisk prstu, nebo přejděte na http://download.bitdefender.com/business/tools/ApplicationControl/

Pro získání hashe aplikace:

1. Otevřete okno **Příkazového řádku**.
2. Přejděte na umístění nástroje Otisk prstu. Například:

```
cd/users/fingerprint.exe
```

3. Pro zobrazení hashové hodnoty aplikace, zadejte tento příkaz:

```
fingerprint <application_full_path>
```

4. Vraťte se do Control Center a nastavte pravidlo na základě obdržené hodnoty. Další informace viz „Kontrola aplikací“ (str. 329).

Otisk palce

Klikněte zde pro stažení spustitelného souboru Otisk palce, nebo přejděte na http://download.bitdefender.com/business/tools/ApplicationControl/

Pro obdržení certifikátu otisku palce:

1. Spusťte **Příkazový řádek** jako administrátor.
2. Přejděte na umístění nástroje Otisk palce. Například:

```
cd/users/thumbprint.exe
```

3. Pro zobrazení certifikátu otisku palce, zadejte následující příkaz:

```
thumbprint <application_full_path>
```

4. Vraťte se do Control Center a nastavte pravidlo na základě obdržené hodnoty. Další informace viz „Kontrola aplikací“ (str. 329).

A.7. Objekty Sandbox Analyzeru

A.7.1. Podporované typy souborů a přípony pro ruční odesílání

Následující přípony souborů jsou podporovány a mohou být ručně spuštěny v Sandbox Analyzer:

`Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archiv), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, soubory MZ/PE (spustitelné), PDF, PEF (spustitelné), PIF (spustitelné), RTF, SCR, URL (binární), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.`.

Sandbox Analyzer dokáže rozpoznat výše zmíněné typy souborů také, když jsou součástí archivů těchto typů: `7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, komprimovaný archiv LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (vícesvazkový), ZOO, XZ.`

A.7.2. Typy souborů podporované předfiltrováním obsahu při automatickém odesílání

Předběžné filtrování obsahu určí konkrétní typ souboru kombinací, která zahrnuje obsah a příponu objektu. To znamená, že spustitelný soubor, který má příponu `.tmp`, bude rozpoznán jako aplikace a pokud bude shledán podezřelým, bude odeslán do Sandbox Analyzer.

- Aplikace - soubory ve formátu PE32, včetně, ale bez omezení na následující přípony: `exe, dll, com`.
- Dokumenty - soubory ve formátu dokumentu, včetně následujících přípon: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm , dotm, potm, potx,`

ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf.

- Skripty: ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- Archivy: zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- E-maily (uložené v systému souborů): eml, tnef.

A.7.3. Výchozí vyloučení při automatickém odesílání

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.

A.7.4. Doporučené použití pro detonační VMs

Sandbox Analyzer On-Premises vyžaduje, aby byly na detonační virtuální stroje nainstalovány určité aplikace, aby otevřely odeslané vzorky.

Aplikace	Soubory
Microsoft Office suite	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Výchozí nastavení systému Windows	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Datové procesory

Jméno	Podrobnosti
Processor Request Forwarder	Předává žádosti o procesor v distribuovaných prostředích
VMware Hypervision Integrátor	Synchronizuje VMware inventář a další informace s GravityZone
Citrix Hypervisor Integrator	Synchronizuje inventář Xenu a další informace s GravityZone
Generic Virtualization Integrator	Synchronizuje inventář Nutanix, Amazon EC2 a Azure s GravityZone
NTSA Integrator	Synchronizuje Network Traffic Security Analytics (NTSA) stav integrace a odešle aktualizace licence do zařízení NTSA
Synchronizátor počítačového inventáře služby Active Directory	Synchronizuje inventář počítače služby Active Directory s GravityZone
Synchronizátor inventáře skupin Active Directory	Synchronizuje inventář skupin Active Directory s GravityZone
Synchronizátor importu uživatelů služby Active Directory	Synchronizuje účty uživatelů služby Active Directory s GravityZone (používá se k propojení účtů AD s účty GravityZone)
Szchronizátor inventáře uživatelů služby Active Directory	Synchronizuje inventář uživatelů služby Active Directory s GravityZone
Processor emailů	E-maily ve frontě pro odeslání z GravityZone
Processor reportů	Zpracovává sestavy a portlety
Windows bezpečnostní agent deployer	Nasadí agenta zabezpečení Bitdefender do zařízení Windows
Bezpečnostní server Deployer	Nasazuje bezpečnostní virtuální zařízení
Správa Licencí	Spravuje licence nainstalovaných koncových bodů
Mobilní notifikační procesor	Odesílá oznámení do chráněných mobilních zařízení

Jméno	Podrobnosti
Linux and macOS bezpečnostní agent Deployer	Nasazuje agenta Bitdefender GravityZone Enterprise Security pro virtualizovaná prostředí (SVE) na zařízeních Linux a macOS
Soupravy koncových bodů a aktualizace produktu	Stáhne a zveřejní soupravy koncových bodů společnosti Bitdefender a aktualizace produktů
GravityZone Updater	Automaticky aktualizuje GravityZone, když je nakonfigurován. Aktualizuje verzi virtuálních zařízení GravityZone
Čistič balíčků	Vyčistí nepoužívané soubory balíčku
Procesor problémů se zabezpečením	Zpracovává bezpečnostní problémy u položek v části Síť
Backup Processor	Provádí zálohy databáze GravityZone
Procesor oznámení	Odesílá oznámení uživatelům
Procesor systémových událostí	Zpracovává události z infrastruktury (Application Control, Sandbox Analyzer, Serenity, SVA) nebo integrace (Exchange, Nutanix, NSX)
HVI Deployer Doplňkových balíčků	Zpracovává instalaci, aktualizaci a odebrání doplňkového balíčku HVI pro hostitele XEN
Procesor restartu úlohy HVI	Spravuje úlohy pro restart na hostitelích HVI
Power a Online Status Procesor	Vypočítá stav napájení a stav připojení počítačů a virtuálních strojů
Procesor čištění strojů offline	Vyčistí offline stroje ze sítě
Spouštěč úloh na pozadí	Zpracovává a spouští úkoly a procesy na pozadí

Významový slovník

Adware

Adware je často spojen s hostitelskou aplikací, která je zdarma poskytována tak dlouho, dokud uživatel adware akceptuje. Protože je adware instalován většinou až po odsouhlasení licenčních podmínek, které stanovují účel aplikace, nejedná se o trestný čin.

Přesto mohou být vyskakovací reklamy obtěžující a v některých případech snižují výkon systému. Také informace shromažďované některými aplikacemi mohou znamenat bezpečností riziko pro uživatele, kteří nejsou plně seznámeni s podmínkami licenční smlouvy.

Aktualizace

Nová verze softwarového nebo hardwarového produktu vyvinutá za účelem nahradit starší verzi téhož produktu. Navíc se při instalaci aktualizací často zjišťuje, zda již je ve vašem počítači nainstalovaná starší verze, a pokud ne, nemůžete aktualizaci instalovat.

Bitdefender má svůj vlastní modul pro aktualizace, který Vám umožňuje aktualizace produktu kontrolovat ručně nebo produkt nechat aktualizovat automaticky.

Antimalwarové bouře

Intenzivní využití systémových zdrojů, ke kterému dochází, když antivirový software skenuje více virtuálních zařízení současně na jednom fyzickém hostiteli.

Archiv

Disk, páska nebo adresář obsahující soubory, které byly zálohovány.

Soubor, který obsahuje jeden nebo více souborů v komprimovaném formátu.

Boot vir

Virus, který infikuje spouštěcí sektor pevného disku nebo diskety. Pokus o spuštění z diskety infikované boot virem zapříčiní, že se virus v paměti aktivuje. Pokaždé, když zavedete systém z tohoto místa, budete mít aktivní virus v paměti.

Bootkit

Bootkit je škodlivý program, který dokáže infikovat hlavní spouštěcí záznam (MBR), záznam spouštěcí hlasitosti (VBR) nebo spouštěcí sektory. Bootkit zůstává aktivní i po obnovení systému.

Červ

Program, který se sám šíří po síti a přitom se reprodukuje. Neumí se sám připojit k jiným programům.

Cílené útoky

Kybernetické útoky, jejichž cílem jsou především finanční výhody nebo očernění pověsti. Cílem může být jedinec, společnost, software nebo systém, který je před provedením útoku důkladně prostudován. Tyto útoky probíhají dlouhodobě a ve fázích, za použití jednoho nebo více infiltračních bodů. Těžko si jich všimnete, obvykle až když napáchají škody.

Cookie

V internetovém žargonu jsou cookie popisovány jako malé soubory, obsahující informace o jednotlivých počítačích, které mohou být analyzovány a použity inzerenty pro vysledování vašich internetových zájmů a zálib. V této oblasti se technologie cookie stále ještě rozvíjí se záměrem cílit reklamu přímo na zájmy, které jste uvedli. Na jednu stranu se pro mnoho lidí jedná o dvousečný meč, který je účinný a relevantní, protože vidíte pouze reklamy, o které se zajímáte. Na stranu druhou ve skutečnosti „stopuje“ a „pronásleduje“, kam chodíte a na co kliknete. Je pochopitelné, že to vyvolalo debatu o soukromí a mnoho lidí se cítí dotčeno představou, že je na ně nazíráno jako na „číslo SKU“ (určitě znáte čárový kód na zadní straně obalů, které jsou skenovány v obchodě u pokladny). Jakkoliv se může zdát tento názor extrémní, v některých případech odpovídá realitě.

Exploit

Exploit obecně označuje jakoukoli metodu použitou pro získání neoprávněného přístupu k počítačům nebo zranitelnosti v zabezpečení systému, která vystaví systém nebezpečí.

Falešná detekce

Objeví se, když sken rozpozná soubor jako infikovaný, ačkoliv ve skutečnosti není.

Grayware

Kategorie softwarových aplikací mezi legitimním softwarem a malwarem. Přestože nejsou tak škodlivé jako malware, který působí na integritu systému, jejich chování je přesto rušivé a vede k nežádoucím situacím, jako jsou krádeže dat a neoprávněné užívání, nežádoucí reklama. Nejobvyklejší grayware aplikace jsou spyware a adware.

Heuristika

Na pravidlech založená metoda identifikace nových virů. Tato metoda skenování je nezávislá na specifických virových signaturách. Výhodou heuristického skenování je, že se nenechá ošálit novou variantou existujícího viru. Nicméně občas se může stát, že ohlásí podezřelý kód u normálních programů – pak hovoříme o „falešné detekci“.

IP

Internetový protokol - směrovací protokol v sadě protokolů TCP/IP, který je zodpovědný za adresování v sítích IP, směrování a fragmentaci a skládání paketů IP.

Keylogger

Keylogger je aplikace, která zaznamenává vše, co napíšete.

Keyloggery jsou ze své povahy škodlivé. Lze je použít k legitimním účelům, jako sledování aktivity zaměstnanců nebo dětí. Stále častěji je však používají počítačoví piráti k zlomyslným účelům (např. ke shromažďování soukromých dat, jako přihlašovací údaje a čísla sociálního pojištění).

Makro virus

Druh počítačového viru, který je zakódovaný jako makro začleněné do dokumentu. Mnoho aplikací, jako např. Microsoft Word a Excel, podporuje výkonné jazyky maker.

Tyto aplikace umožňují vložit makro do dokumentu a nechat ho provést při každém otevření dokumentu.

Malware

Malware je obecný název pro software, který je navržen tak, aby škodil - zkratka pro 'malicious software' (škodlivý software). Ještě není používán univerzálně, ale jeho popularita jakožto označení pro viry, Trojské koně, červy a škodlivý mobilní kód stále vzrůstá.

Malwarová signatura

Malware signatury jsou úryvky kódu extrahované ze skutečných vzorků malwaru. Jsou používané antivirovými programy pro porovnání vzorků a detekci malwaru. Signatury jsou také používány pro odstranění malwarového kódu z infikovaných souborů.

Databáze malwarových signatur Bitdefender je sbírka malwarových signatur, kterou každou hodinu aktualizují výzkumní pracovníci pro malware společnosti Bitdefender.

Neheuristický

Tato metoda skenování je závislá na specifických virových signaturách. Výhodou neheuristického skenování je, že se nedá zmást domnělým virem a negeneruje falešné detekce.

Phishing

Jedná se o rozesílání podvržených emailových zpráv, které se tváří jako legitimní, s cílem, aby uživatel poskytl soukromé informace, které budou následně použity ke krádeži identity. Email obvykle nasměruje uživatele na webovou stránku, kde má aktualizovat své osobní informace, jako hesla, údaje o kreditní kartě, číslo sociálního pojištění a čísla bankovních účtů apod., která již legitimní organizace má. Webová stránka je však falešná a vytvořená s cílem zcizit informace uživatele.

Podezřelé soubory a síťový provoz

Podezřelé soubory jsou ty s pochybnou reputací. Toto hodnocení je dáno mnoha faktory, mezi které patří: existence digitální signatury, častost výskytu v počítačových sítích, užitý balič atd.. Síťový provoz je považován za podezřelý, když se odchýlí od vzoru. Například nedůvěryhodný zdroj, žádosti o připojení k neobvyklým portům, zvýšené využití šířky pásma, nahodilé časy připojení atd..

Polymorfní virus

Virus, který mění svoji formu v každém souboru, který infikuje. Jelikož takové viry nemají konzistentní binární vzorec, je těžké je identifikovat.

Port

Rozhraní v počítači, ke kterému můžete připojit zařízení. Osobní počítače mají různé druhy portů. Uvnitř je celá řada portů pro připojení diskových jednotek,

displejů a klávesnic. Vně mají osobní počítače porty pro připojení modemů, tiskáren, myší a dalších periferních zařízení.

V sítích TCP/IP a UDP je to konečný bod logického propojení. Číslo portu udává, o jaký typ portu jde. Např. port 80 je používán pro HTTP provoz.

Příkazový řádek

V rozhraní příkazového řádku píše uživatel příkazy do prostoru přímo na obrazovce s použitím jazyka příkazového řádku.

Přípona názvu souboru

Součást názvu souboru, nacházející se za tečkou, která indikuje druh dat uložených v souboru.

Mnohé operační systémy používají přípony názvů souborů, např. Unix, VMS a MS-DOS. Skládají se obvykle z 1-3 písmen (některé staré operační systémy nepodporují více než tři). Jako příklad poslouží „c“ jako zdrojový kód v jazyce C, „ps“ jako PostScript, „txt“ pro libovolný text.

Prohlížeč

Zkrácené označení pro webový prohlížeč, aplikaci používanou pro nalezení a zobrazení webových stránek.

Ransomware

Malware, který vám zabrání v přístupu k vašemu počítači nebo blokuje přístup k vašim souborům a aplikacím. Ransomware od vás bude vyžadovat uhrazení určitého poplatku (výkupného) za dešifrovací klíč, který vám umožní získat zpět přístup k vašemu počítači nebo souborům.

Rootkit

Rootkit je sada softwarových nástrojů, které nabízejí přístup k systému na úrovni správce. Termín byl poprvé použit pro UNIXové operační systémy a označoval překompilované nástroje, které vetřelci poskytovaly administrátorská práva, umožňující utajit jeho přítomnost i před samotnými správci systému.

Hlavní úlohou rootkitů je maskovat procesy, soubory, přihlašování a protokoly. Rovněž mohou zachytávat data z terminálů, síťových připojení nebo periferií, pokud se včlení do příslušného softwaru.

Rootkity nejsou ve skutečnosti nebezpečné. Například systémy a dokonce některé aplikace skrývají kritické soubory používající rootkity. Nicméně jsou většinou používány ke skrývání malwaru nebo maskování přítomnosti vetřelce

v systému. V kombinaci s malwarem představují rootkity velkou hrozbu pro integritu a bezpečnost systému. Mohou monitorovat síťový provoz, vytvořit zadní vrátka do systému, modifikovat soubory a protokoly, a zabránit tak své detekci.

Skript
Jiný termín pro makro nebo pro dávkový soubor; skript je seznam příkazů, které mohou být vykonány bez uživatelovy interakce.

Soubor se zprávou
Soubor, který obsahuje seznam akcí, ke kterým došlo. Bitdefender uchovává soubor se zprávou, ve které jsou uvedeny skenované cesty, složky, počet skenovaných archivů a souborů, počet nalezených infikovaných a podezřelých souborů.

Spam
Nevyžádaná pošta nebo nevyžádané příspěvky v diskuzních skupinách. Obecně jsou označovány jako nevyžádané emaily.

Spouštěcí sektor:
Sektor na začátku každého disku, který identifikuje architekturu disku (velikost sektoru, velikost clusteru atd.). U startovacích disků obsahuje spouštěcí sektor rovněž program, který načítá operační systém.

Spyware
Jakýkoli software, který tajně shromažďuje informace o uživateli prostřednictvím internetového připojení bez jeho vědomí, obvykle pro reklamní účely. Spywarové aplikace jsou většinou skrytou součástí freewarových nebo sharewarových programů, volně přístupných na Internetu; nicméně je třeba poznamenat, že většina freewarových a sharewarových aplikací spyware neobsahuje. Pokud je spyware nainstalován, monitoruje uživatelovu aktivitu na Internetu a na pozadí odesílá tyto informace někomu jinému. Spyware také může shromažďovat informace o emailových adresách a dokonce i hesla a čísla kreditních karet.

Podobnost spywaru a trojských koní tkví hlavně ve skutečnosti, že uživatelé ho instalují, když instalují něco jiného. Nejobvyklejším způsobem, jak se stát obětí spywaru, je stahování některých v současnosti dostupných produktů pro výměnu souborů metodou peer-to-peer.

Vedle otázky etiky a porušování soukromí spyware zabírá také paměťové prostředky počítače a přenosové pásmo, když odesílá informace zpět na svou domovskou základnu prostřednictvím internetového připojení uživatele. Protože spyware využívá paměť a systémové prostředky, aplikace běžící na pozadí mohou vést až k pádu systému a jeho obecné nestabilitě.

Systémová lišta

Systémová lišta, uvedená se systémem Windows 95, se nachází na hlavním panelu systému Windows (obvykle dole vedle hodin) a obsahuje miniaturní ikony pro snadný přístup k systémovým funkcím, jako je fax, tiskárna, modem, hlasitost atd. Dvojím kliknutím nebo kliknutím pravým tlačítkem na ikonu zobrazíte a získáte přístup k podrobnostem a ovládacím prvkům.

TCP/IP

Transmission Control Protocol/Internet Protocol - sada síťových protokolů široce používaných na Internetu, které zajišťují komunikaci mezi propojenými sítěmi počítačů s různorodou hardwarovou architekturou a rozličnými operačními systémy. Protokol TCP/IP obsahuje standardy pro komunikaci počítačů a konvence pro propojení sítí a směrování provozu.

Trójský kůň

Destruktivní program, který se maskuje jako neškodná aplikace. Narozdíl od virů se trojské koně samy nereplikují, ale přesto mohou být stejně destruktivní. Jedním z nejzákeřnějších typů trojského koně je program, který slibuje odstranění virů z vašeho počítače, ale namísto toho do počítače viry zavede.

Termín pochází z příběhu Homérovy Illiady, v němž Řekové darují obrovského dřevěného koně svému nepříteli, Trójanům, jako symbol míru. Jakmile však Trójané dovlečou koně dovnitř městských hradeb, řečtí vojáci vylezou z dutých útrob koně a otevřou městské brány, aby tak umožnili svým spolubojovníkům proniknout dovnitř a zmocnit se Tróje.

Události

Akce nebo událost odhalená programem. Událostmi mohou být aktivity uživatele, jako např. kliknutí tlačítkem myši nebo stisk klávesy, nebo systémové události, jako např. zaplnění paměti.

Virus

Program, nebo kus kódu, který je načten do Vašeho počítače bez vašeho vědomí a pracuje proti vaší vůli. Většina virů se může také replikovat. Všechny

počítačové viry jsou dílem člověka. Je relativně snadné vyrobit jednoduchý virus, který se neustále kopíruje. Dokonce i tak jednoduchý vir je nebezpečný, protože rychle spotřebuje veškerou dostupnou paměť a způsobí kolaps systému. Mnohem nebezpečnějším druhem virů jsou takové, které jsou schopné se přenášet po sítích a obcházet bezpečnostní systémy.

Vrstvy ochrany

GravityZone poskytuje ochranu prostřednictvím řady modulů a rolí, souhrnně označovaných jako ochranné vrstvy, které se dělí na ochranu koncových bodů (EPP) nebo ochranu jádra a různé doplňky. Ochrana koncových bodů zahrnuje Antimalware, Advanced Threat Control, Advanced Anti-Exploit, Firewall, Content Control, Device Control, Network Attack Defense, Power User a Relay. Doplňky zahrnují ochranné vrstvy, jako jsou Security for Exchange a Sandbox Analyzer.

Podrobnosti o ochranných vrstvách dostupných u vašeho řešení GravityZone najdete na stránce „Ochranné vrstvy GravityZone “ (str. 2).

Windows Downloader

Je to obecný název programu, jehož hlavní funkcí je stahování obsahu pro nežádoucí nebo škodlivé účely.

Zadní vrátka

Díra v zabezpečení systému, kterou návrháři nebo údržbáři úmyslně zanechali. Nemusí se vždy jednat o zlý úmysl; některé operační systémy, např. počítají s privilegovanými účty zamýšlenými pro používání terénními servisními techniky nebo programátory údržby dodavatele.

Zloděj hesel

Zloděj hesel shromažďuje útržky dat, které mohou být jména účtů a s nimi spojená hesla. Tyto ukradené přihlašovací údaje jsou poté použity k záškodným účelům, jako krádeže účtů.