Bitdefender

GravityZone

PRZEWODNIK ADMINISTRATORA

Bitdefender GravityZone
Przewodnik administratora

Data publikacji 2021.04.20

Notka prawna

Bitdefender

Spis treści

Wstęp

Przewodnik ten jest przeznaczony dla administratorów sieci zarządzających ochroną GravityZone wewnątrz organizacji.

Dokument ma na celu wyjaśnienie jak stosować i sprawdzać bezpieczeństwa na punktach końcowych sieci przy użyciu Control Center GravityZone. Dowiesz się jak przeglądać elementy sieci przy pomocy Control Center, jak tworzyć i stosować reguły zarządzania punktami końcowymi, generować raporty, zarządzać kwarantanną oraz jak korzystać z panelu nawigacyjnego.

1. Znaki umowne stosowane w przewodniku

Konwencje Typograficzne

Podręcznik ten wykorzystuje kilka stylów formatowania tekstu dla polepszonej czytelności. Dowiedz się o ich aspektach i znaczeniu z poniższej tabeli.

Wygląd	Opis
`wzorzec`	Nazwy i składnie poleceń liniowych, ścieżki i nazwy plików, dane wyjściowe plików konfiguracyjnych, tekst wejściowy są zapisane z użyciem czcionki `o stałej szerokości znaków`.
http://www.bitdefender.com	Link URL wskazuje na zewnętrzną lokalizację, na serwerach http lub ftp.
gravityzone-docs@bitdefender.com	W tekście umieszczono adresy e-mail w celu podania informacji kontaktowych.
„Wstęp” (p. viii)	To link wewnętrzny, do miejsca wewnątrz dokumentu.
opcja	Wszystkie opcje produktu są napisane z użyciem **pogrubionych** znaków.
słowo kluczowe	Ważne słowa kluczowe lub frazy są wyróżniane poprzez użycie **pogrubionych** znaków.

Uwagi

Uwagi to notatki tekstowe oznaczone graficznie wskazujące na dodatkowe informacje związane z bieżącym akapitem.

Notatka

Notatka jest tylko krótką informacją. Chociaż można by ją ominąć, jednak wskazówki zawierają użyteczne informacje, takie jak specyficzne działanie lub powiązania z podobnym tematem.

WAŻNE

Wymaga to Państwa uwagi i nie jest wskazane pomijanie tego. Zazwyczaj nie są to wiadomości krytyczne, ale znaczące.

Ostrzeżenie

To jest krytyczna informacja, którą należy traktować ze zwiększoną ostrożnością. Nic złego się nie stanie jeśli podążasz za tymi wskazówkami. Powinieneś to przeczytać i zrozumieć, ponieważ opisuje coś ekstremalnie ryzykowanego.

1. O GRAVITYZONE

GravityZone jest biznesowym rozwiązaniem bezpieczeństwa zaprojektowanym od podstaw z myślą o wirtualizacji, a chmura by dostarczać usługę ochrony dla fizycznych punktów końcowych, urządzeń mobilnych, maszyn wirtualnych opartych na prywatnej, publicznej chmurze oraz serwerów pocztowych Exchange.

GravityZone jest jednym produktem z ujednoliconą konsolą zarządzania dostępną w chmurze, której gospodarzem jest Bitdefender lub jednym wirtualnym urządzeniem instalowanym w siedzibie firmy i stanowi jeden punkt wdrażania, egzekwowania i zarządzania zasadami zabezpieczeń dla dowolnej liczby urządzeń końcowych i dowolnego typu w dowolnym miejscu.

GravityZone dostarcza wielowarstwową ochronę dla punktów końcowych, oraz dla serwerów poczty Microsoft Exchange: antymalware wraz z monitorowaniem zachowań, ochronę przed zagrożeniami dnia zero, kontrolę aplikacji, sandboxa, zaporę sieciowej, kontrolę urządzeń, kontrolę treści, antyphishing i antyspam.

2. GRAVITYZONE WARSTWY OCHRONNE

GravityZone udostępnia następujące warstwy ochrony:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- HyperDetect
- Zaawansowany Anty-Exploit
- Zapora Sieciowa
- Kontrola Zawartości
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne szyfrowanie dysku
- Security for Exchange
- Kontrola Aplikacji
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antymalware

Warstwa ochrony antymalware bazuje na skanowaniu sygnatur i analizie heurystycznej (B-HAVE, ATC) przeciwko: wirusom, robakom, Trojanom, spyware, adware, keyloggerom, rootkitom i innym rodzajom złośliwego oprogramowania.

Technologia skanowania antymalware Bitdefender opiera się na następujących warstwach ochrony:

- Po pierwsze, tradycyjna metoda skanowania jest wykorzystywana, gdzie zeskanowana treść jest dopasowana do bazy sygnatur. Baza sygnatur zawiera wzory bajtów charakterystycznych dla znanych zagrożeń i jest regularnie aktualizowana przez Bitdefender. Ta metoda skanowania jest skuteczna przeciwko potwierdzonym zagrożeniom, które były badane i udokumentowane. Jakkolwiek bez względu na to jak szybko baza sygnatur jest aktualizowana, zawsze istnieje luka pomiędzy czasem gdy nowe zagrożenie zostaje odkryte a tym kiedy zostaje wydana poprawka. .
- Przeciwko najnowszym, nieudokumentowanym zagrożeniom stosowana jest druga warstwa ochrony której dostarcza nam **B-HAVE**, heurystyczny silnik

Bitdefender. Algorytmy heurystyczne wykrywają szkodliwe oprogramowanie na podstawie cech behawioralnych. B-HAVE uruchamia podejrzany malware w środowisku wirtualnym, aby sprawdzić jego wpływ na system i upewnić się, że nie stanowi zagrożenia. Jeśli zagrożenie zostało wykryte, uniemożliwione jest uruchomienie programu.

Silniki Skanowania

Bitdefender GravityZone jest w stanie automatycznie ustawić silniki skanowania podczas tworzenia pakietów agentów bezpieczeństwa, zgodnie z konfiguracją punktu końcowego.

Administrator może również dostosować silniki skanowania wybierając pośród kilku technologii skanowania:

1. **Skanowanie Lokalne**, gdy skanowanie jest wykonywane na lokalnym punkcie końcowym. Tryb skanowania lokalnego jest odpowiedni dla potężnych maszyn, posiadających zawartość bezpieczeństwa przechowywaną lokalnie.
2. **Skanowanie hybrydowe za pomocą lekkich silników (chmura publiczna)** , o średnim zasięgu, z wykorzystaniem skanowania w chmurze i częściowo lokalnej zawartości zabezpieczeń. Ten tryb skanowania przynosi korzyści z lepszego wykorzystania zasobów oraz angażuje poza przesłankowe skanowanie.
3. **Centralne skanowanie w chmurze publicznej lub prywatnej** , z niewielkim rozmiarem wymagającym Security Server do skanowania. W takim przypadku żaden zestaw zawartości zabezpieczeń nie jest przechowywany lokalnie, a skanowanie jest odciążane na Security Server.

   Notatka
   Jest to minimalny zestaw silników przechowywanych lokalnie potrzebnych do rozpakowywania skompresowanych plików.

4. **Centralne skanowanie (skanowanie w chmurze publicznej lub prywatnej za pomocą Security Server) z powrotem * na skanowanie lokalne (pełne silniki)**
5. **Centralne skanowanie (skanowanie w chmurze publicznej lub prywatnej za pomocą Security Server) z powrotem * na Hybrid Scan (Publiczna Chmura z Lekkimi Silnikami**

* Podczas wykorzystania podwójnego silnika skanowania, gdy pierwszy silnik jest niedostępny, zostanie użyty silnik awaryjny. Zużycie zasobów oraz wykorzystanie sieci będzie zależało do użytych silników.

2.2. Zaawansowana Kontrola Zagrożeń

Dla zagrożeń, które wymykają się nawet silnikowi heurystycznemu, trzecia warstwa ochrony występuje w formie Zaawansowanej Kontroli Zagrożeń (ATC).

Zaawansowana Kontrola Zagrożeń stale monitoruje procesy i ocenia podejrzane zachowania, takie jak próby: ukrycia typu procesu, wykonanie kodu w innej przestrzeni procesowej (HJ pamięci procesu dla przekroczenia uprawnień), replikacji, upuszczenia plików, ukrycia aplikacji wyliczeń procesowych, itp. Każde podejrzane zachowanie podnosi rating procesu. Gdy próg zostanie osiągnięty, wyzwalany jest alarm.

2.3. HyperDetect

Bitdefender HyperDetect to dodatkowa warstwa zabezpieczeń zaprojektowana specjalnie do wykrywania zaawansowanych ataków i podejrzanych działań na etapie poprzedzającym wykonanie. HyperDetect zawiera modele uczenia maszynowego i technologię wykrywania ataków typu stealth przeciwko zagrożeniom takim jak: ataki zerowego dnia, zaawansowane trwałe zagrożenia (APT), ukryte malware, ataki bez plików (niewłaściwe użycie PowerShell, Windows Management Instrumentation itp.), kradzieży poświadczeń, ataki ukierunkowane, niestandardowe malware, ataki oparte na skryptach, exploity, narzędzia hakerskie, podejrzany ruch sieciowy, potencjalnie niepożądane aplikacje (PUA), oprogramowanie ransomware.

Notatka
Ten moduł jest dostępny jako dodatek z oddzielnym kluczem licencyjnym.

2.4. Zaawansowany Anty-Exploit

Zaawansowana technologia Anty-Exploit, oparta na uczeniu maszynowym, jest proaktywną technologią, która powstrzymuje ataki zerowe przeprowadzane przez nieuchwytne exploity. Zaawansowany Anti-Exploit przechwytuje najnowsze exploity w czasie rzeczywistym i łagodzi luki w zabezpieczeniach pamięci, które mogą ominąć inne rozwiązania bezpieczeństwa. Chroni najczęściej używane aplikacje, takie jak przeglądarki, Microsoft Office lub Adobe Reader, a także inne. Nadzoruje procesy systemowe i chroni przed naruszeniami bezpieczeństwa i przejmowaniem istniejących procesów.

2.5. Zapora Sieciowa

Firewall kontroluje dostęp aplikacji do sieci i do Internetu. Dostęp jest automatycznie dopuszczony do obszernej bazy danych znanych, uzasadnionych wniosków. Ponadto zapora sieciowa chroni system przed skanowaniem portów, ograniczeniami ICS i ostrzega gdy nowe węzły dokonują połączenia przez Wi-Fi.

2.6. Kontrola Zawartości

Moduł Kontroli Zawartości pomaga w egzekwowaniu polityki firmy dla dozwolonego ruchu, dostępu do sieci, ochrony danych i kontroli aplikacji. Administratorzy mogą definiować opcje skanowania ruchu i wykluczeń, harmonogram dostępu do stron internetowych, podczas blokowania lub dopuszczania niektórych kategorii stron internetowych lub adresów URL, mogą konfigurować zasady ochrony danych i zdefiniować uprawnienia do korzystania z określonych aplikacji.

2.7. Network Attack Defense

Moduł Network Attack Defense polega na Bitdefender technologii skoncentrowanej na wykrywaniu ataków sieciowych zaprojektowanych w celu uzyskania dostępu do punktów końcowych za pomocą określonych technik, takich jak: ataki brute-force, sieciowe exploity, złodzieje haseł, wektory infekcji drive-by-download, boty i Trojany.

2.8. Zarządzanie Aktualizacjami

W pełni zintegrowany z GravityZone, moduł Zarządzania Aktualizacjami aktualizuje systemy operacyjne i oprogramowanie i zapewnia kompleksowy widok statusu aktualizacji zarządzanych punktów końcowych Windows.

Moduł Zarządzania Aktualizacjami GravityZone zawiera kilka funkcji, takich jak skanowanie na żądanie / zaplanowane skanowanie aktualizacji, automatyczne / ręczne aktualizowanie lub raportowanie brakujących aktualizacji .

Możesz dowiedzieć się więcej na temat dostawców i produktów Zarządzania Aktualizacjami GravityZone w tym artykule KB.

Notatka
Moduł Zarządzania Aktualnościami jest dodatkiem dostępnym z oddzielnym kluczem licencyjnym dla wszystkich dostępnych pakietów GravityZone.

2.9. Kontrola Urządzenia

Moduł Kontroli Urządzenia pozwala na zapobieganie wyciekaniu danych wrażliwych i infekcji malware przez urządzenia zewnętrzne podłączone do punktów końcowych przez zastosowanie zasad blokowania i wykluczeń przez politykę w szerokim zasięgu rodzajów urządzeń (tj. Pamięci flash USB, urządzenia Bluetooth, odtwarzacze CD/DVD, urządzenia pamięci masowej itp.).

2.10. Pełne szyfrowanie dysku

Ta warstwa ochrony umożliwia zapewnienie pełnego szyfrowania dysku na punktach końcowych, zarządzając funkcją BitLocker w systemie Windows oraz FileVault i diskutil w systemie MacOS. Możesz zaszyfrować i odszyfrować woluminy rozruchowe i nierozruchowe za pomocą kilku kliknięć, podczas gdy GravityZone obsługuje cały proces, przy minimalnej interwencji użytkowników. Dodatkowo GravityZone przechowuje klucze odzyskiwania wymagane do odblokowania woluminów w przypadku, gdy użytkownicy zapomną hasła.

Notatka
Pełne Szyfrowanie Dysku jest dodatkiem dostępnym z oddzielnym kluczem licencyjnym dla wszystkich dostępnych pakietów GravityZone.

2.11. Security for Exchange

Bitdefender Security for Exchange zapewnia antymalware, antyspam, antyphishing, filtrowanie załączników i treści płynnie zintegrowane z Microsoft Exchange Server, aby zapewnić bezpieczne środowisko komunikacji i współpracy oraz zwiększenie wydajności. Korzystając z wielokrotnie nagradzanych technologii antymalware i antyspamowych, chroni użytkowników Exchange przed najnowszym, najbardziej zaawansowanym złośliwym oprogramowaniem i przed próbami kradzieży cennych i poufnych danych użytkowników.

WAŻNE
Security for Exchange ma za zadanie chronić całą organizację Exchange, do której należy chroniony serwer Exchange. Oznacza to, że chroni wszystkie aktywne skrzynki pocztowe, w tym użytkownika/pokój/sprzęt/współdzielone skrzynki pocztowe.
W nawiązaniu do ochrony Microsoft Exchange licencja obejmuje również moduły ochrony punktów końcowych zainstalowanych na serwerze.

2.12. Kontrola Aplikacji

Moduł Kontroli Aplikacji zapobiega malware, atakom 0-day i zwiększa ochronę bez wpływu na wydajność. Kontrola aplikacji wymusza elastyczne zasady białej listy aplikacji, które identyfikują i zapobiegają instalację i wykonanie jakichkolwiek niepożądanych, niezaufanych lub złośliwych aplikacji.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer zapewnia potężną warstwę ochrony przeciwko zaawansowanym zagrożeniom działającą automatycznie, dzięki dogłębnej analizie podejrzanych plików, które nie są jeszcze podpisane przez silniki skanowania Bitdefender. Sandbox zastosowuje szeroki zestaw technologii Bitdefender do wykonywania ładunków w zamkniętym środowisku wirtualnym hostowanym przez Bitdefender lub wdrażanym lokalnie. Analizuje ich zachowanie i zgłasza wszelkie subtelne zmiany systemowe, które wskazują na złośliwe zamiary.

Sandbox Analyzer wykorzystuje serię czujników do detonacji treści z zarządzanych punktów końcowych, potoków ruchu sieciowego, scentralizowanej kwarantanny i serwerów ICAP.

Dodatkowo, Sandbox Analyzer umożliwia ręczne przesłanie próbki i poprzez API.

2.14. Hypervisor Memory Introspection (HVI)

Powszechnie wiadomo, że dobrze zorganizowani, napędzani profitami napastnicy poszukują nieznanych luk (luk zero-day), albo używają jednorazowych, specjalnie zbudowanych exploitów (exploity zero-day) oraz innych narzędzi. Atakujący stosują również zaawansowane techniki opóźniania i sekwencyjnego uruchamiania złośliwego oprogramowania w celu zamaskowania szkodliwej aktywności. Współczesne ataki nastawione na zysk są tak skonstruowane, by miały niezauważalny przebieg i przełamywały tradycyjne zabezpieczenia.

W przypadku środowisk wirtualnych problem został rozwiązany dzięki HVI, zapewniającemu centrom danych o wysokim zagęszczeniu maszyn wirtualnych ochronę przed zaawansowanymi i złożonymi zagrożeniami, których nie są w stanie powstrzymać silniki oparte na sygnaturach. Rozwiązanie to wykorzystuje mechanizm ścisłej izolacji, zapewniając wykrywanie ataków w czasie rzeczywistym, blokowanie ich w momencie wystąpienia i natychmiastowe usuwanie zagrożeń.

Bez względu na to, czy chroniona maszyna jest oparta na systemie Windows czy Linux, ani czy jest to serwer czy komputer stacjonarny, HVI zapewnia wgląd w dane

na poziomie, który jest niemożliwy do osiągnięcia w wirtualizowanym systemie operacyjnym (gościa). Podobnie jak hiperwizor zarządza dostępem każdej wirtualnej maszyny gościa do sprzętu, HVI posiada dokładną wiedzę na temat pamięci gościa zarówno w trybie użytkownika, jak i jądra. W rezultacie HVI ma pełny wgląd w pamięć gościa, a zarazem zna cały kontekst. Jednocześnie HVI jest izolowany od chronionych gości, tak samo jak izolowany jest sam hiperwizor. Działając na poziomie hiperwizora i wykorzystując jego funkcjonalności, HVI pokonuje techniczne wyzwania tradycyjnej ochrony wykrywając niebezpieczną aktywność w centrach danych.

HVI identyfikuje nie tyle schematy ataku, co techniki ataku. Tym sposobem technologia ta potrafi identyfikować, powiadamiać i zapobiegać stosowaniu typowych technik przechwytywania danych. Jądro jest chronione przed technikami przechwytywania z wykorzystaniem rootkitów, które stosuje się podczas dokonywania ataku dla jego ukrycia. Procesy użytkownika są również chronione przed wstrzyknięciem kodu, przekierowywaniem funkcji oraz wykonywaniem kodu ze stosu (stack) i sterty (heap).

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender [NTSA_ LONG] ([NTSA_ SHORT]) to rozwiązanie bezpieczeństwa sieciowego, które analizuje strumienie ruchu IPFIX pod kątem obecności złośliwego zachowania i złośliwego oprogramowania.

Bitdefender [NTSA_ SHORT] ma działać równolegle z istniejącymi środkami bezpieczeństwa jako zabezpieczenie uzupełniające, które jest w stanie pokryć martwe pola, których tradycyjne narzędzia nie monitorują.

Tradycyjne narzędzia bezpieczeństwa sieci zazwyczaj próbują zapobiegać infekcjom złośliwego oprogramowania, sprawdzając ruch przychodzący (za pośrednictwem sandbox, zapór sieciowych, antywirusa itp.). Bitdefender [NTSA_ SHORT] koncentruje się wyłącznie na monitorowaniu wychodzącego ruchu sieciowego pod kątem złośliwego zachowania.

2.16. Security for Storage

GravityZone Security for Storage zapewnia ochronę w czasie rzeczywistym dla czołowych systemów udostępniania plików i sieciowych systemów pamięci masowej. Aktualizacje algorytmu systemu wykrywania zagrożeń występują automatycznie - bez konieczności podejmowania jakichkolwiek działań przez użytkownika lub tworzenia zakłóceń dla użytkowników końcowych.

Dwa lub więcej GravityZone Security Servers Multi-Platform pełnią rolę serwera ICAP dostarczającego usługi antymalware do urządzeń pamięci masowej podłączonej do sieci (NAS) i rozwiązań wymiany plików zgodnych z Protokołem Adaptacji Treści Internetowych (ICAP, zgodnie z definicją w dokumencie RFC 3507).

Gdy użytkownik prosi o otwarcie, odczytanie, zapisanie lub zamknięcie pliku z laptopa, stacji roboczej, telefonu komórkowego lub innego urządzenia, klient ICAP (NAS lub system wymiany plików) wysyła żądanie skanowania do Security Server i otrzymuje werdykt dotyczący pliku. W zależności od wyniku Security Server umożliwia, odmawia dostępu lub usuwa plik.

Notatka
Ten moduł jest dostępny jako dodatek z oddzielnym kluczem licencyjnym.

2.17. Security for Mobile

Ujednolica w całym przedsiębiorstwie ochronę i zarządzanie oraz zgodność w kontroli urządzeń iPhone, iPad i systemem Android poprzez dostarczenie niezawodnego oprogramowania i dystrybucji aktualizacji za pośrednictwem firmy Apple oraz sklepów Android. Rozwiązanie zostało zaprojektowane tak by umożliwić kontrolowaną adaptację rozwiązania bring-your-own-device (BYOD) poprzez zainicjowanie i konsekwentne egzekwowanie zasad użytkowania na wszystkich urządzeniach przenośnych. Funkcje bezpieczeństwa zawierają blokadę ekranu, kontrolę uwierzytelnienia, lokalizowanie urządzenia, zdalne czyszczenie pamięci, wykrywanie zrootowanych i odblokowanych urządzeń oraz kontroli profili bezpieczeństwa. W przypadku urządzeń z Android poziom bezpieczeństwa jest wyższy dzięki skanowaniu w czasie rzeczywistym i szyfrowaniu karty pamięci. W rezultacie kontrolujemy urządzenia i chronimy znajdujące się na nich poufne dane firmowe.

2.18. GravityZone Dostępność Warstw Ochrony

Dostępność warstw ochrony GravityZone różni się w zależności od systemu operacyjnego punktu końcowego. Aby dowiedzieć się więcej, zapoznaj się z artykułem Dostępność warstw ochrony w GravityZone.

3. ARCHITEKTURA GRAVITYZONE

Unikatowa architektura GravityZone dostarcza nam ułatwione skalowanie i zabezpieczenie dowolnej ilości systemów. GravityZone może zostać skonfigurowany do korzystania z wielu urządzeń wirtualnych w wielu przypadkach i z zastosowaniem określonych ról (Baza danych, serwery komunikacyjne, serwery aktualizacyjne i konsola WWW) by zapewnić skalowalność i niezawodność.

Każda rola instancji może zostać zainstalowana na innym urządzeniu. Wbudowany równoważnik ról zapewnia GravityZone ochronę nawet największych sieci korporacyjnych, nie powodując efektu spowolnienia ani zawężenia przepustowości. Istniejące sprzętowe lub programowe rozwiązania kompensacyjne mogą zastąpić wbudowany stabilizator, jeżeli taki jest używany w danej sieci.

Dostarczany w kontenerze wirtualnym, GravityZone może być zaimportowany do pracy na dowolnej platformie wirtualizacji, w tym VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Integracja z VMware vCenter, Citrix XenServer, Microsoft Active Directory oraz Nutanix Prism Element i Microsoft Azure zmniejszają wysiłek związany z wdrażaniem ochrony dla stacji fizycznych i wirtualnych punktów końcowych.

Rozwiązanie GravityZone zawiera następujące składniki:

- Urządzenie Wirtualne GravityZone
- Security Server
- Pakiet uzupełniający HVI
- Agenci Bezpieczeństwa

3.1. GravityZone VA

Rozwiązanie lokalne GravityZone dostarczane jest jako samoczynnie konfigurowane, hartowane urządzenie wirtualne (VA) Linux, osadzone w obrazie maszyny wirtualnej, łatwe do zainstalowania i skonfigurowania za pomocą interfejsu CLI (Wiersz Poleceń Interfejs). Wirtualne urządzenia są dostępne w kilku formatach kompatybilnych z platformami wirtualizacji (OVA, XVA, VHD, OVF, RAW).

3.1.1. Baza danych GravityZone

Centralna logika architektury GravityZone. Bitdefender używa nie-relacyjnej bazy danych MongoDB, prostej w skalowaniu i replikacji.

3.1.2. Serwer Aktualizacji GravityZone

Serwer aktualizacyjny posiada istotną rolę przy uaktualnianiu rozwiązania GravityZone oraz agentów zainstalowanych na końcówkach poprzez replikowanie i publikowanie potrzebnych paczek oraz plików instalacyjnych.

3.1.3. Serwer Komunikacji GravityZone

Serwer komunikacyjny jest łącznikiem pomiędzy agentami bezpieczeństwa i bazą danych, przekazują polityki i zadania do chronionych urządzeń końcowych oraz zdarzeniowych raportów do agentów bezpieczeństwa.

3.1.4. Konsola Web (GravityZone Control Center)

Rozwiązania bezpieczeństwa Bitdefender są zarządzane z jednego punktu zarządzania, konsoli internetowej Control Center. Zapewnia to łatwiejsze zarządzanie i dostęp do ogólnej postawy bezpieczeństwa, globalnych zagrożeń bezpieczeństwa i kontrolę nad wszystkimi modułami bezpieczeństwa chroniącymi wirtualne lub fizyczne komputery, serwery i urządzenia mobilne. Zasilana przez Architekturę Gravity, Control Center jest w stanie odpowiedź na potrzeby nawet największych organizacji.

Control Center zintegrowana z istniejącym systemem zarządzania i monitorowaniem systemu, aby łatwo automatycznie zatwierdzać ochronę niezarządzanych stacji roboczych, serwerów i urządzeń przenośnych, które pojawiają się w Microsoft Active Directory, VMware vCenter, Nutanix Prism Element i Citrix XenServer lub są po prostu wykrywane w sieci.

3.1.5. Baza danych kreatora raportów

Bazy danych kreatora raportów dostarcza danych wymaganych do tworzenia raportów opartych na zapytaniach.

3.1.6. Procesory kreatora raportów

Procesory kreatora raportów są niezbędne do tworzenia, zarządzania i przechowywania raportów opartych na zapytaniach, które wykorzystują informacje z Bazy danych kreatora raportów.

3.2. Security Server

Security Server jest dedykowaną maszyną wirtualną, która deduplikuje i centralizuje większość funkcjonalności antymalware dla agentów, działających jako serwer.

Są trzy wersje Security Server dla każdego typu środowisk wirtualnych:

- **Security Server dla VMware NSX.** Ta wersja jest automatycznie instalowana na każdym hoście w klastrze, gdzie Bitdefender została wdrożona.
- **Security Server dla VMware vShield Endpoint.** Ta wersja musi być zainstalowana na każdym hoście, aby był chroniony.
- **Security Server Multi-Platform.** Ta wersja jest przeznaczona dla różnych innych środowisk wirtualnych i musi być zainstalowana na jednym lub więcej hostach, aby dostosować się do liczby chronionych maszyn wirtualnych. W przypadku korzystania z HVI, Security Server musi być zainstalowany na każdym hoście zawierającym maszyny wirtualne, które mają być chronione.

3.3. Pakiet uzupełniający HVI

Pakiet HVI zapewnia połączenie między hiperwizorem a Security Server na danym hoście. W ten sposób, Security Server jest w stanie monitorować pamięć wykorzystaną na hoście, na którym jest zainstalowany, w oparciu o polityki bezpieczeństwa GravityZone.

3.4. Agenci Bezpieczeństwa

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować właściwych agentów bezpieczeństwa GravityZone na punktach końcowych sieci.

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

3.4.1. Bitdefender Endpoint Security Tools

GravityZone zapewnia ochronę maszynom fizycznym i wirtualnym systemów Windows i Linux za pomocą Bitdefender Endpoint Security Tools, inteligentnego agenta ochrony środowiska, który dostosowuje się do typu punktu końcowego. Bitdefender Endpoint Security Tools może być wdrożony na dowolnym komputerze, albo wirtualnym lub fizycznym, zapewniając elastyczny system skanowania, będący

idealnym wyborem dla środowisk mieszanych (fizycznych, wirtualnych i cloudowych).

Dodatkowo, system ochrony plików, Bitdefender Endpoint Security Tools obejmuje również ochronę serwera poczty dla serwerów Microsoft Exchange.

Bitdefender Endpoint Security Tools wykorzystuje pojedynczy szablon zasad dla maszyn fizycznych i wirtualnych i jedno źródło zestawu instalacyjnego dla wszelkich środowisk (fizycznych czy wirtualnych) uruchomionych na bieżących edycjach Windows.

Warstwy bezpieczeństwa

Następujące moduły powłok zabezpieczających dostępne są z Bitdefender Endpoint Security Tools:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- HyperDetect
- Zapora Sieciowa
- Kontrola Zawartości
- Network Attack Defense
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne szyfrowanie dysku
- Security for Exchange
- Sandbox Analyzer
- Kontrola Aplikacji

Role Punktów Końcowych

- Power User
- Relay
- Serwerów Buforowania Łatek
- Ochrona Exchange

Power User

Administratorzy Control Center mogą przyznawać prawa Power User użytkownikom punktów końcowych poprzez ustawienia polityk. Moduł Power User umożliwia uprawnienia administratora na poziomie użytkownika, umożliwiając użytkownikowi dostęp do punktów końcowych i modyfikację ustawień zabezpieczeń za pomocą

lokalnej konsoli. Control Center jest powiadamiana, gdy punkt końcowy jest w trybie Power User i administrator Control Center zawsze może nadpisać ustawienia lokalnych zabezpieczeń.

WAŻNE
Moduł ten jest dostępny tylko dla wspieranych desktopowych i serwerowych systemów operacyjnych Windows. Aby uzyskać więcej informacji, zapoznaj się z Instrukcją instalacji GravityZone.

Relay

Agenci Endpoint z rolą Bitdefender Endpoint Security Tools Relay służącą jako serwer komunikacji proxy i aktualizacji dla innych punktów końcowych w sieci. Agenci Endpoint z rolą relay są szczególnie potrzebni w organizacjach z sieciami zamkniętymi, gdzie cały ruch odbywa się za pośrednictwem jednego punktu dostępu.

W firmach z dużym rozproszeniem sieci, agenci relay pomagają obniżenie wykorzystania pasma, zapobiegając bezpośredniemu łączeniu się chronionych punktów końcowych i serwerów bezpieczeństwa za każdym razem bezpośrednio z konsolą zarządzającą GravityZone.

Gdy agent Bitdefender Endpoint Security Tools Relay jest zainstalowany w sieci, inne punkty końcowe mogą być skonfigurowane za pomocą polityki do komunikacji przez agenta relay z Control Center.

Agenci Bitdefender Endpoint Security Tools Relay służą do następujących czynności:

- Wykrywanie wszystkich niezabezpieczonych punktów końcowych w sieci.
- Wdrażanie agenta endpoint w sieci lokalnej.
- Aktualizacja chronionych punktów końcowych w sieci.
- Zapewnienie komunikacji pomiędzy Control Center i podłączonymi punktami końcowymi.
- Działa jako serwer proxy dla chronionych punktów końcowych.
- Optymalizowanie ruchu sieciowego podczas aktualizacji, wdrożenia, skanowania i innych konsumujących zasoby zadań.

Serwerów Buforowania Łatek

Punkty końcowe z rolą Relay mogą również działać jako Serwer Buforowania Aktualizacji. Po włączeniu tej roli, Relay służą do przechowywania aktualizacji oprogramowania pobranych ze stron internetowych dostawców i dystrybuowania

ich do docelowych punktów końcowych w sieci. Kiedy podłączony punkt końcowy ma oprogramowanie z brakującymi aktualizacjami, pobiera je z serwera, a nie ze strony internetowej producenta, optymalizując w ten sposób generowany ruch i obciążenie sieci.

WAŻNE
Ta dodatkowa rola jest dostępna z zarejestrowanym dodatkiem Patch Management.

Ochrona Exchange

Bitdefender Endpoint Security Tools z rolą Exchange może być zainstalowany na serwerach Microsoft Exchange w celu ochrony użytkowników Exchange przed zagrożeniami pochodzącymi z wiadomości e-mail.

Bitdefender Endpoint Security Tools z rolą Exchange chroni zarówno urządzenie serwera oraz rozwiązanie Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac to agent bezpieczeństwa zaprojektowany w celu ochrony stacji roboczych i laptopów opartych na procesorze Intel. Dostępna technologia skanowania to **Skanowanie lokalne** , z zawartością zabezpieczeń przechowywaną lokalnie.

Warstwy bezpieczeństwa

Następujące moduły powłok zabezpieczających dostępne są z Endpoint Security for Mac:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Kontrola Zawartości
- Kontrola Urządzenia
- Pełne szyfrowanie dysku

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client rozszerza z łatwością polityki zabezpieczeń na dowolnej liczbie urządzeń z systemem Android oraz iOS, chroniąc je przed nieautoryzowanym użyciem i ryzykiem utraty poufnych danych. Funkcje bezpieczeństwa zawierają blokadę ekranu, kontrolę uwierzytelnienia, lokalizowanie urządzenia, zdalne czyszczenie pamięci, wykrywanie zrootowanych i odblokowanych urządzeń oraz

kontroli profili bezpieczeństwa. W przypadku urządzeń z Android poziom bezpieczeństwa jest wyższy dzięki skanowaniu w czasie rzeczywistym i szyfrowaniu karty pamięci.

Aplikacja GravityZone Mobile Client jest dystrybuowana wyłącznie poprzez Apple App Store i Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools jest lekkim agentem dla środowisk zwirtualizowanych VMware, które są zintegrowane z vShield Endpoint. Agent bezpieczeństwa instalowany na maszynach wirtualnych chronionych przez Security Server, aby pozwolić skorzystać z dodatkowej funkcjonalności to prowadzi:

- Dopuszcza uruchomienie zadań skanowania pamięci i procesów na maszynie.
- Informuje użytkownika o wykrytych infekcjach i akcjach zastosowanych na nich.
- Dodaje więcej opcji dla wyjątków skanowania antymalware.

3.5. Architektura Sandbox Analyzer

Bitdefender Sandbox Analyzer zapewnia potężną warstwę ochrony przed zaawansowanymi zagrożeniami, wykonując automatyczną, szczegółową analizę podejrzanych plików, które jeszcze nie zostały podpisane przez silniki antimalware Bitdefender.

Sandbox Analyzer jest dostępny w dwóch wariantach:

- Sandbox Analyzer w Chmurze, hostowany przez Bitdefender.
- Sandbox Analyzer On-Premises, dostępny jako urządzenie wirtualne, które można wdrożyć lokalnie.

Sandbox Analyzer w Chmurze

Sandbox Analyzer w Chmurze zawiera następujące elementy:

- **Portal Sandbox Analyzer** - hostowany serwer komunikacyjny używany do przetwarzania żądań pomiędzy punktami końcowymi i klastrem Sandbox Bitdefender.
- **Klaster Sandbox Analyzer** - hostowana infrastrukura sandbox, w której występują analizy zachowawcze. Na tym poziomie przesłane pliki są detonowane na maszynach wirtualnych z systemem Windows 7.

GravityZone Control Center działa jako konsola zarządzania i raportowania, w której konfigurujesz polityki bezpieczeństwa, przeglądasz raporty z analiz i powiadomienia.

Bitdefender Endpoint Security Tools, agent bezpieczeństwa zainstalowany na punktach końcowych, działa jak sensor zasilania dla Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises jest dostarczany jako urządzenie wirtualne z Linux Ubuntu, osadzony w obrazie maszyny wirtualnej, łatwy do instalacji i konfiguracji poprzez interfejs linii komend (CLI). Sandbox Analyzer On-Premises jest dostępny w formacie OVA, możliwy do wrdożenia w VMWare ESXi.

Instancja Sandbox Analyzer On-Premises zawiera następujące komponenty:

- **Menedżer Sandboxa**. Ten komponent jest orkiestratorem sandboxa. Menedżer Sandbox łączy się z hiperwisorem ESXi poprzez API i wykorzystuje swoje zasoby sprzętowe do budowy i obsługi środowiska analizy złośliwego oprogramowania.
- **Detonacja maszyn wirtualnych**. Ten komponent składa się z maszyn wirtualnych wykorzystywanych przez Sandbox Analyzer do wykonywania plików i analizy ich zachowania. Maszyny wirtualne do detonacji mogą działać w 64-bitowych systemach operacyjnych Windows 7 i Windows 10.

GravityZone Control Center działa jako konsola zarządzania i raportowania, w której konfigurujesz polityki bezpieczeństwa, oraz przeglądasz raporty i powiadomienia z analizy.

Sandbox Analyzer On-Premises obsługuje następujące czujniki zasilające:

- **Czujnik punktu końcowego**. Bitdefender Endpoint Security Tools dla systemu Windows działa jako czujnik żywienia zainstalowany na punktach końcowych. Agent Bitdefender korzysta z zaawansowanych algorytmów uczenia maszynowego i sieci neuronowych w celu określenia podejrzanej treści oraz przesłania jej do Sandbox Analyzer, w tym obiektów ze scentralizowanej kwarantanny.
- **Czujnik sieci**. Wirtualne Urządzenie Zabezpieczeń Sieciowych (NSVA) jest urządzeniem wirtualnym, które jest możliwe do wdrożenia w tym samym środowisku zwirtualizowanym ESXi jako instancja Sandbox Analyzer. Czujnik sieciowy pobiera zawartość ze strumieni sieciowych i przesyła ją do Sandbox Analyzer.

- **Czujnik ICAP**. Wdrożony na urządzeniach sieciowej pamięci masowej (NAS), za pomocą protokołu ICAP, Bitdefender Security Server wspiera obsługę przesyłania treści do Sandbox Analyzer.

Oprócz tych czujników, Sandbox Analyzer On-Premises obsługuje ręczne przesyłanie i przez API. Szczegółowe informacje znajdują się w rozdziale **Korzystanie z Sandbox Analyzer** w Przewodniku Administratora GravityZone.

4. PIERWSZE KROKI

Rozwiązania GravityZone mogą być skonfigurowane i zarządzane poprzez scentralizowaną platformę o nazwie Control Center. Control Center posiada interfejs oparty na sieci, do którego możesz uzyskać dostęp za pomocą nazwy użytkownika i hasła.

4.1. Łączenie z Control Center

Dostęp do Control Center odbywa się za pośrednictwem kont użytkowników. Po utworzeniu konta otrzymasz informacje dotyczące logowania na e-mail.

Warunki wstępne:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Zalecana rozdzielczość ekranu: 1280 x 800 lub wyższa

Ostrzeżenie
Control Center nie pracuje / wyświetla poprawnie w Internet Explorer 9+ z włączoną funkcją zgodności, co jest równoznaczne z wykorzystaniem nieobsługiwanych wersji przeglądarki.

Żeby połączyć się z Control Center:

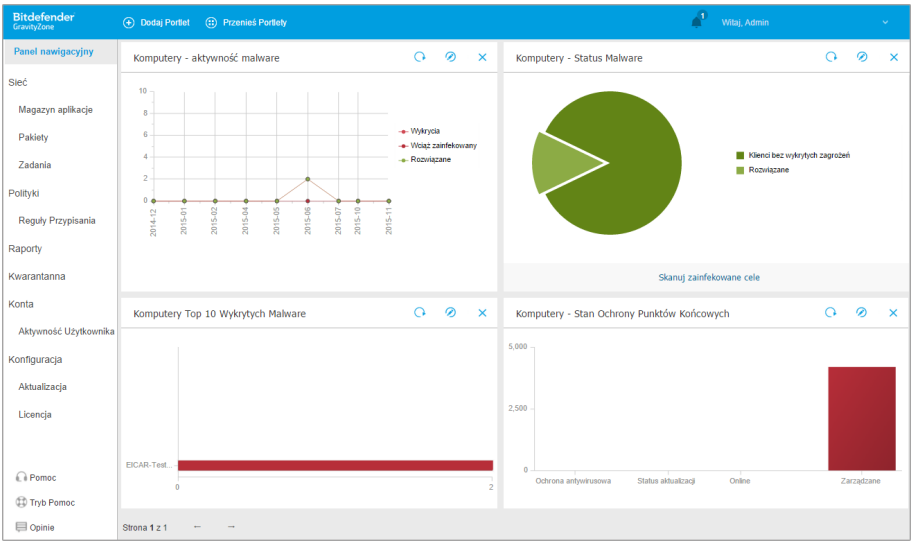
1. W pasku adresu przeglądarki internetowej wpisz adres IP lub nazwę hosta DNS Control Center urządzenia (używając `https://` prefiks).
2. Podaj nazwę użytkownika i hasło.
3. Wprowadź sześcioznakowy kod z Google Authenticator, Microsoft Authenticator lub innej aplikacji uwierzytelniającej TOTP (Time-Based One-Time Password Algorithm) - kompatybilnej ze standardem RFC6238. Szczegółowe informacje znajdują się w „Zarządzanie kontem” (p. 25).
4. Kliknij **„Zaloguj”**.

Przy pierwszym logowaniu musisz się zgodzić na Warunki Korzystania z Usługi Bitdefender. Kliknij **Kontynuuj** aby rozpocząć korzystanie z GravityZone.

Notatka
Jeżeli zapomniałeś hasło, użyj linku przypomnienia hasła, aby otrzymać nowe hasło. Musisz podać adres e-mail twojego konta.

4.2. Control Center w skrócie

Control Center jest uporządkowana w taki sposób, aby umożliwić łatwy dostęp do wszystkich funkcji. Użyj paska menu po prawej stronie, aby poruszać się po konsoli. Dostępne funkcje zależą od typu użytkownika, który chce uzyskać dostęp do konsoli.



Panel

4.2.1. Control Center Przegląd

Użytkownicy z rolą administratora firmy mają pełne uprawnienia konfiguracyjne Control Center i ustawień bezpieczeństwa sieci, jeżeli użytkownicy z rolą administratora mają dostęp do funkcji bezpieczeństwa sieci, włączając zarządzanie użytkownikami.

Użyj **Menu Widok** przycisk w lewym górnym rogu, aby zwinąć do widoku ikony, ukryć lub rozwinąć opcje menu. Kliknij przycisk, aby uruchomić kolejno opcje, lub kliknij dwukrotnie, aby pominąć.

W zależności od twojej roli możesz uzyskać dostęp do następujących opcji menu:

Panel nawigacyjny

Zobacz łatwe do czytania wykresy dostarczające kluczowe informacje na temat bezpieczeństwa sieci.

Sieć
Zainstaluj ochronę, zastosuj polityki do zarządzania ustawieniami bezpieczeństwa, uruchom zadania zdalnie i utwórz szybkie raporty.

Polityki
Utwórz i zarządzaj politykami bezpieczeństwa.

Raporty
Pobierz raporty bezpieczeństwa dotyczące zarządzania klientami.

Kwarantanna
Zdalne zarządzanie plikami kwarantanny.

Konta
Zarządzaj dostępem do Control Center dla innych pracowników firmy.

W tym menu można również znaleźć stronę **Aktywność Użytkownika**, co pozwala na uzyskiwanie dostępu do dziennika aktywności użytkownika.

> **Notatka**
> To menu jest dostępne tylko dla użytkowników z uprawnieniem **Zarządzaj Użytkownikami**.

Konfiguracja
Skonfiguruj ustawienia Control Center, takie jak serwer wiadomości email, integracja z Active Directory bądź środowiska zwirtualizowane, certyfikaty bezpieczeństwa i ustawienia Inwentarza Sieci, jak również zaplanowane reguły automatycznego czyszczenia nie używanych maszyn wirtualnych.

> **Notatka**
> To menu jest dostępne tylko dla użytkowników z uprawnieniami **Zarządzaj Rozwiązaniami**.

Klikając swoją nazwę użytkownika w prawym górnym rogu konsoli, dostępne są następujące opcje:

- **Moje konto**. Kliknij tę opcję, aby zarządzać danymi konta użytkownika i preferencjami.
- **Menedżer uprawnień**. Naciśnij tę opcje aby dodać i zarządzać poświadczeniami uwierzytelniania potrzebnymi do zdalnej instalacji zadań.
- **Pomoc & Wsparcie**. Naciśnij tę opcję aby znaleźć informacje o pomocy i wsparciu.

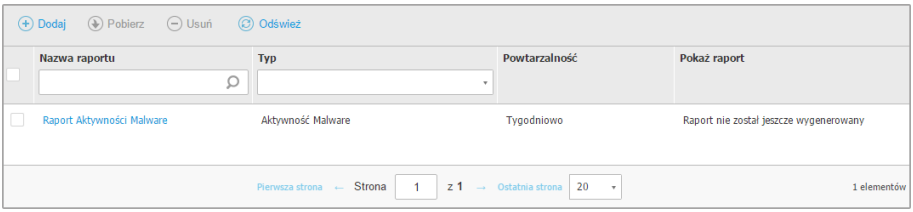
- **Opinie**. Kliknij tę opcję, aby wyświetlić formularz do edytowania i wysyłania wiadomości zwrotnych dotyczących twoich doświadczeń z GravityZone.
- **Wyloguj**. Kliknij tę opcję, aby wylogować się z konta.

W prawym górnym rogu konsoli możesz znaleźć również:

- Ikona **Tryb Pomocy**, która umożliwia rozwijanie podpowiedzi umieszczonych w elementach Control Center. Bez problemu znajdziesz przydatne informacje dotyczące funkcji Control Center.
- Ikona **Powiadomienia**, która zapewni łatwy dostęp do powiadomień i strony **Powiadomień**.

4.2.2. Tabela Danych

Tabele są często używane przez konsolę do uporządkowania danych w przystępnym formacie.



Strona Raportów

Poruszanie się po stronach

Tabele z ponad 20 zgłoszeniami rozciągają się na kilka stron. Domyślnie tylko 20 wpisów jest wyświetlanych na jednej stronie. Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Możesz zmienić liczbę wpisów wyświetlanych na stronie, wybierając inną opcję z menu obok przycisków nawigacyjnych.

Szukanie określonych wpisów

Żeby łatwo znaleźć określone wpisy, użyj pól wyszukiwania dostępnych poniżej kolumny nagłówków.

W odpowiednie pole wpisz szukany termin. Pasujące elementy są wyświetlane w tabeli w trakcie pisania. Aby przywrócić zawartość tabeli, wyczyść pola wyszukiwania.

Sortowanie danych

Aby posortować dane według określonych kolumn, naciśnij na nagłówek kolumny. Kliknij nagłówek ponownie, aby przywrócić kolejność porządkowania.

Odświeżanie Danych Tabeli

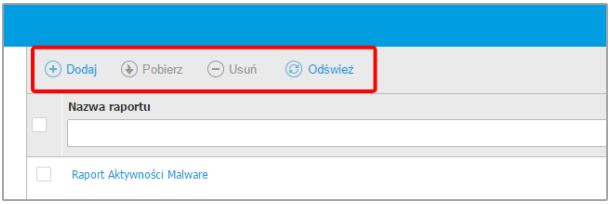
Abby upewnić się, że konsola wyświetla najnowsze informacje, naciśnij przycisk **Odśwież** w górnej części tabeli.

Może być potrzebne abyś spędził więcej czasu na tej stronie.

4.2.3. Paski narzędzi działań

W Control Center, paski narzędzi działań pozwalają na wykonanie określonych czynności należących do sekcji w której się znajdujesz. Każdy pasek narzędzi składa się z zestawu ikon, które zwykle umieszczone są w górnej części tabeli. Na przykład, pasek narzędzi działań w sekcji **Raporty** pozwala wykonać poniższe akcje:

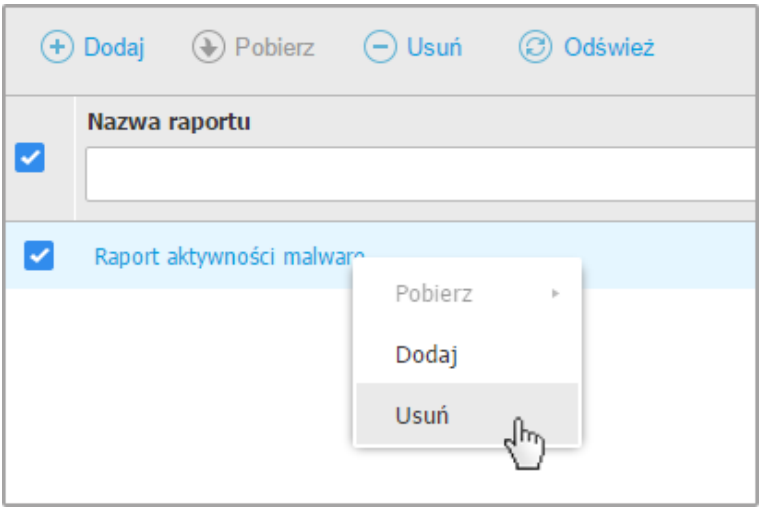
- Stwórz nowy raport.
- Pobierz zaplanowany raport.
- Usuń zaplanowany raport.



Strona raportów - Pasek Narzędzi Akcji

4.2.4. Menu Kontekstowe

Komendy pasków narzędzi działań są również dostępne z menu kontekstowego. Kliknij prawym przyciskiem myszy w sekcji Control Center, której aktualnie używasz i wybierz dostępne polecenie z listy.



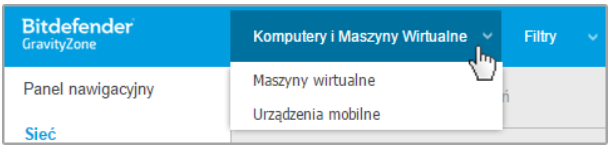
Strona Raportów - menu kontekstowe

4.2.5. Selektor Widoku

Jeśli pracujesz z różnymi typami punktów końcowych, możesz znaleźć je zorganizowane na stronie **Sieć** według ram kilku widoków sieciowych.

- **Komputery & oraz Maszyny Wirtualne**: wyświetlają grupy Active Directory, komputery oraz fizyczne i wirtualne stacje robocze występujące na zewnątrz Active Directory dokrytych w sieci.
- **Maszyny Wirtualne**: wyświetlają infrastrukturę środowisk wirtualnych zintegrowanych z Control Center i wszystkimi zawierającymi maszyny wirtualne.
- **Urządzenia Mobilne**: wyświetla użytkowników oraz urządzenia mobilne przypisane do nich.

Aby wybrać widok sieci, który chcesz, kliknij menu widoków, w prawym górnym rogu strony.



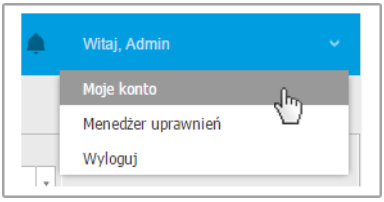
Przełącznik odsłony

Notatka
Zobaczysz tylko te stacje końcowe, do których masz dostęp wglądu, uprawnienia nadawane są przez administratora, który dodał twojego użytkownika do Control Center.

4.3. Zarządzanie kontem

Żeby sprawdzić albo zmienić szczegółowe dane konta lub ustawień:

1. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moje konto**.



Menu konta użytkownika

2. Poprzez **Szczegóły konta**, możesz poprawić lub zaktualizować szczegóły twojego konta. Jeżeli używasz konta użytkownika Active Directory, nie możesz zmienić szczegółów konta.
   - **Nazwa użytkownika.** Nazwa użytkownika jest unikalnym identyfikatorem konta użytkownika i nie może zostać zmieniona.
   - **Pełna nazwa.** Wprowadź swoje imię i nazwisko.
   - **E-mail.** To jest twój login i kontaktowy adres e-mail. Raporty i ważne powiadomienia bezpieczeństwa będą wysyłane na ten adres. Powiadomienia e-mail są wysyłane automatycznie, gdy zostaną wykryte istotne ryzykowne warunki w sieci.
   - Link **Zmień hasło** pozwala Ci na zmianę hasła logowania.

3. W **Ustawienia**, konfiguruj ustawienia konta zgodnie z własnymi preferencjami.
   - **Strefa czasowa.** Wybierz z menu swoją strefę czasową dla swojego konta. Konsola wyświetli informację o czasie, w zależności od wybranej strefy czasowej.
   - **Język.** Wybierz z menu język wyświetlania w konsoli.
   - **Sesja wygasła.** Wybierz czas nieaktywności sesji zanim wygaśnie.
4. W **Bezpieczeństwo logowania**, skonfiguruj uwierzytelnianie dwuskładnikowe i sprawdź status polityk dostępnych do zabezpieczenia twojego konta GravityZone. Zasady obowiązujące w firmie są przeznaczone tylko do odczytu.

   Aby włączyć uwierzytelnienie dwuskładnikowe:

   a. **Uwierzytelnienie dwuskładnikowe.** Uwierzytelnienie dwuskładnikowe dodaje dodatkową warstwę zabezpieczenia do twojego konta GravityZone, wymagając oprócz twoich danych uwierzytelniających Control Center, kodu uwierzytelniającego.

      Podczas pierwszego logowania do swojego konta GravityZone zostaniesz poproszony o pobranie i zainstalowanie Google Authenticator, Microsoft Authenticator lub innej aplikacji uwierzytelniania dwuskładnikowego TOTP (Time-Based One-Time Password Algorithm) - kompatybilej ze standardem RFC6328 na urządzeniu mobilnym, następnie połączenie aplikacji z kontem GravityZone i używanie jej podczas każdego logowania do Control Center. Google Authenticator generuje sześciocyfrowy kod co 30 sekund. Aby dokończyć login do Control Center, po wprowadzeniu hasła musisz podać sześciocyfrowy kod Google Authenticator.

      Notatka
      Możesz pominąć ten proces trzy razy, po czym nie będziesz mógł zalogować się bez uwierzytelnienia dwuskładnikowego.

      Aby włączyć uwierzytelnienie dwuskładnikowe:

      i. Kliknij przycisk **Włącz** pod komunikatem **Uwierzytelnianie dwuskładnikowe**.

      ii. W oknie dialogowym kliknij odpowiedni link, aby pobrać i zainstalować aplikację Google Authenticator na swoim urządzeniu mobilnym.

      iii. Otwórz Google Authenticator na swoim urządzeniu mobilnym.

      iv. W oknie **Dodaj konto**, zeskanuj kod QR, aby połączyć aplikację ze swoim kontem GravityZone.

Możesz również wpisać klucz ręcznie.

To działanie wymagane jest tylko raz, aby włączyć funkcję w GravityZone.

WAŻNE
Upewni się, że skopiowałeś i zapisałeś tajny klucz w bezpiecznej lokalizacji. Kliknij **Wydrukuj kopię zapasową**, aby utworzyć plik PDF z kodem QR i tajnym kluczem . Jeśli urządzenie mobilne używane do aktywacji uwierzytelniania dwuskładnikowego zostanie utracone lub zastąpione, musisz zainstalować Google Authenticator na nowym urządzeniu i podać tajny klucz, aby połączyć go z kontem GravityZone.

v. Wpisz sześciocyfrowy kod w polu **Kodu Google Authenticator**.

vi. Kliknij **Włącz**, aby dokończyć aktywację funkcji.

Notatka
Administrator Twojej firmy może zmienić obowiązkowe uwierzytelnianie dwuskładnikowe dla wszystkich kont GravityZone. W takim przypadku, przy logowaniu zostaniesz poproszony o skonfigurowanie 2FA. Jednocześnie nie będzie można dezaktywować 2FA na swoim koncie, dopóki ta funkcja będzie egzekwowana przez Administratora Firmy.
Pamiętaj, że jeśli aktualnie skonfigurowana usługa 2FA jest wyłączona dla Twojego konta, ten tajny klucz nie będzie już ważny.

b. **Zasady dotyczące wygaśnięcia hasła.** Regularne zmiany hasła zapewniają dodatkową warstwę ochrony przed nieautoryzowanym użyciem haseł lub ograniczają czas trwania nieautoryzowanego użycia. Po włączeniu GravityZone wymaga zmiany hasła maksymalnie co 90 dni.

c. **Zasady blokady konta.** Ta polityka uniemożliwia dostęp do konta po pięciu kolejnych nieudanych próbach logowania. Te działanie ma na celu ochronę przed atakami siłowymi.

   Aby odblokować swoje konto, musisz zresetować swoje hasło ze strony logowania lub skontaktować się z innym administratorem GravityZone.

5. Naciśnij **Zapisz** aby zastosować zmiany.

Notatka
Nie możesz usunąć swojego własnego konta.

4.4. Zmiana hasła logowania

Po utworzeniu Twojego konta, otrzymasz e-mail z poświadczeniami logowania.

Jeśli nie używasz poświadczeń Active Directory, aby uzyskać dostęp do Control Center, zaleca się, aby wykonać następujące czynności:

- Zmień domyślne hasło logowania, gdy po raz pierwszy odwiedzasz Control Center.
- Zmieniaj hasło logowania okresowo.

Aby zmienić hasło logowania:

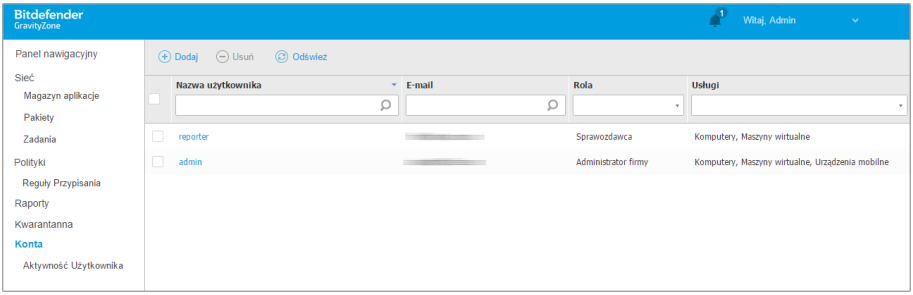
1. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moje konto**.
2. W **Szczegóły Konta**, kliknij **Zmień hasło**.
3. Wprowadź bieżące hasło i nowe hasło w odpowiednich polach.
4. Naciśnij **Zapisz** aby zastosować zmiany.

5. KONTA UŻYTKOWNIKA

Możesz stworzyć pierwsze konto użytkownika GravityZone podczas wstępnej konfiguracji Control Center, po wdrożeniu urządzenia GravityZone. Wstępne konto użytkownika Control Center posiada rolę administratora firmy, z pełnymi prawami konfiguracyjnymi Control Center i zarządzaniem sieci. Z tego konta możesz utworzyć wszystkie inne konta użytkowników, które są potrzebne do zarządzania siecią twojej firmy.

Wszystko co musisz wiedzieć o kontach użytkowników GravityZone:

- By umożliwić innym pracownikom firmy dostęp do Control Center, możesz tworzyć konta użytkowników indywidualnie lub włączyć dynamiczny dostęp dla wielu kont za pomocą integracji Active Directory lub reguł dostępu. Możesz przypisać konta użytkowników z różnymi rolami, zależnie od ich poziomu dostępu w firmie.
- Dla każdego konta użytkownika, możesz dostosować dostęp do funkcji GravityZone lub do określonych części sieci, do których należy.
- Możesz zarządzać tylko kontami z równymi lub mniejszymi przywilejami dla konta.



Strona Kont

Istniejące konta są wyświetlane w tabeli. Dla każdego konta użytkownika, możesz zobaczyć:

- Nazwa użytkownika konta (używana do logowania do Control Center).
- Adres e-mail konta (używany jako adres kontaktowy). Raporty i ważne powiadomienia bezpieczeństwa będą wysyłane na ten adres. Powiadomienia

e-mail są wysyłane automatycznie, gdy zostaną wykryte istotne ryzykowne warunki w sieci.

- Rola użytkownika (administrator firmy / administrator sieci / analityk bezpieczeństwa/ inne).
- Serwisy bezpieczeństwa GravityZone pozwalają użytkownikowi zarządzać (Komputery, wirtualne Maszyny, Urządzenia Przenośne).
- Status 2FA (uwierzytelnianie dwuskładnikowe), który pozwala szybko sprawdzić, czy użytkownik włączył uwierzytelnianie dwuskładnikowe.
- Status Dostępu Reguły, wskazuje konto użytkownika utworzone za pomocą reguły uprawnień dostępu. Ręcznie utworzone konta użytkowników będą wyświetlać **Nie dotyczy**

5.1. Role użytkownika

Rola użytkownika sprowadza się do specyficznej kombinacji uprawnień użytkownika. Podczas tworzenia konta użytkownika, możesz wybrać jedną z dostępnych ról, lub stworzyć niestandardową rolę, wybierając tylko niektóre prawa użytkownika.

Notatka
Możesz zarządzać tylko kontami z równymi lub mniejszymi przywilejami dla konta.

Dostępne są następujące role użytkowników:

1. **Administrator Firmy** - Zazwyczaj, unikalne konto użytkownika z rolą Administratora firmy jest stworzone przez daną firmę, z pełnym dostępem do funkcji zarządzania rozwiązaniami GravityZone. Administrator firmy konfiguruje ustawienia Control Center, zarządza kluczami licencyjnymi usług bezpieczeństwa, zarządza kontami użytkownika które również mają przywileje administracyjne w ustawieniach bezpieczeństwa sieci firmy. Administrator firmy może podzielić się lub przekazać swoje obowiązki operacyjne podległym kontom administratorów i analityków bezpieczeństwa.
2. **Administrator Sieci** - Kilka kont z rolą Administratora Sieci może zostać utworzonych dla firmy, wraz z jego przywilejami administracyjnymi nad wszystkimi agentami lub nad konkretną grupą punktów końcowych, włączając w to zarządzanie użytkownikami. Administratorzy Sieci są odpowiedzialni za aktywne zarządzanie ustawieniami bezpieczeństwa sieci.

3. **Analityk Bezpieczeństwa** - konta Analityków Bezpieczeństwa są kontami tylko do odczytu. Pozwalają one tylko na dostęp do danych, raportów i dzienników związanych z bezpieczeństwem. Takie konta mogą być przydzielone dla pracowników z obowiązkiem kontrolowania bezpieczeństwa lub dla innych pracowników którzy muszą utrzymywać wysoki stan bezpieczeństwa.
4. **Niestandardowe** - Wstępnie zdefiniowane role użytkowników obejmują pewna kombinacje praw użytkowników. Jeżeli wcześniej zdefiniowana rola użytkownika nie spełnia twoich oczekiwań, możesz stworzyć niestandardowe konto poprzez wybranie tylko tych praw, które cie interesują.

Poniższa tabela podsumowuje relacje między różnymi rolami kont i ich prawami. Szczegółowe informacje znajdują się w „Prawa użytkownika” (p. 31).

Rola konta	Dopuszcza konta dzieci	Prawa użytkownika
Administrator firmy	Administratorzy Firm, Administratorzy Sieci, Analitycy Bezpieczeństwa	Zarządzaj Rozwiązaniem Zarządzaj Firmą Zarządzaj Użytkownikami Zarządzaj sieciami Zobacz i przeanalizuj dane
Administrator sieci	Administratorzy Sieci, Analitycy Bezpieczeństwa	Zarządzaj Użytkownikami Zarządzaj sieciami Zobacz i przeanalizuj dane
Analityce Bezpieczeństwa	-	Zobacz i przeanalizuj dane

5.2. Prawa użytkownika

Możesz przypisać prawa dla poniższych użytkowników do kont użytkowników GravityZone:

- **Zarządzaj Rozwiązaniem**. Pozwala na konfigurację ustawień Control Center (mail serwer i ustawienia, proxy, integracja z Active Directory i platformami wirtualizacji, certyfikatami bezpieczeństwa i aktualizacjami GravityZone). Przywileje są określone dla kont administracyjnych firmy.
- **Zarządzaj Użytkownikami**. Twórz, edytuj lub usuwaj konta użytkowników.

- **Zarządzaj Firmą**. Użytkownicy mogą zarządzać ich własnymi kluczami licencyjnymi GravityZone i edytować ich ustawienia profilu firmy. Przywileje są określone dla kont administracyjnych firmy.
- **Zarządzaj sieciami**. Zapewnia uprawnienia administracyjne dla ustawień zabezpieczenia sieci (zasoby sieci, pakiety instalacyjne, kwarantanna). Przywilej ten jest specyficzny dla kont administratorów sieci.
- **Zobacz i przeanalizuj dane**. Zobacz wydarzenia związane z bezpieczeństwem i dzienniki, zarządzaj raportami i pulpitem.

5.3. Zarządzanie kontami użytkownika

Aby tworzyć, edytować, usuwać i konfigurować konta użytkowników, użyj następujących metod:

- Indywidualne Zarządzanie Kontami Użytkowników . Użyj tej metody, aby dodać lokalne konta użytkowników lub konta usługi Active Directory. Aby skonfigurować integrację z Active Directory, zapoznaj się z Przewodnikiem Instalacji GravityZone.

  Przed stworzeniem konta użytkownika, upewnij się, że masz odpowiedni adres email pod ręką. Użytkownik otrzyma szczegółowe dane logowania z GravityZone na podany adres email.
- Zarządzanie Wieloma Kontami Użytkownika. Użyj tej metody, aby umożliwić dynamiczny dostęp poprzez reguły uprawnień dostępu. Ta metoda wymaga integracji domeny Active Directory. Aby uzyskać więcej informacji na temat integracji z Active Directory, zapoznaj się z Przewodnikiem Instalacji GravityZone.

5.3.1. Indywidualne Zarządzanie Kontami Użytkowników

W Control Center możesz indywidualnie tworzyć, edytować i usuwać konta użytkowników

Zależności

- Lokalnie utworzone konta mogą usuwać konta utworzone przez Active Directory niezależnie od ich roli.
- Lokalnie utworzone konta nie mogą usunąć podobnych kont niezależnie od ich roli.

Indywidualne Tworzenie Kont Użytkownika

Aby dodać konto użytkownika w Control Center:

1. Przejdź do strony **Konta**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Pojawia się okno konfiguracji.
3. W sekcji **Szczegóły** skonfiguruj w następujący sposób:
   - Konta użytkowników usługi Active Directory skonfiguruj następujące szczegóły:

     Nazwa użytkownika dla kont użytkowników usługi Active Directory (AD). Wybierz konto użytkownika z listy rozwijanej i przejdź do kroku 4.

     Konta użytkowników AD można dodawać tylko wtedy, gdy integracja jest skonfigurowana. Podczas dodawania konta użytkownika AD dane użytkownika są importowane z powiązanej z nim domeny. Użytkownik loguje się do Control Center przy użyciu nazwy użytkownika AD i hasła.

     Notatka

     – Aby upewnić się, że ostatnie zmiany w Active Directory zostały zaimportowane w Control Center, naciśnij przycisk **Synchronizacja**.

     – Użytkownicy z uprawnieniami **Zarządzaj rozwiązaniem** mogą skonfigurować interwał synchronizacji usługi Active Directory przy użyciu opcji dostępnych na karcie **Konfiguracja > Active Directory** . Aby uzyskać więcej informacji, zapoznaj się z rozdziałem **Instalacja Ochrony > GravityZone Instalacja** i **konfiguracja >Skonfiguruj Centrum Ustawień Control Center** z Podręcznika Instalacyjnego GravityZone.

   - W przypadku kont lokalnych skonfiguruj następujące szczegóły:
     – **Nazwa użytkownika** dla konta lokalnego. Wyłącz **Importuj z Active Directory** i wprowadź nazwę użytkownika.

     – **E-mail**. Podaj adres e-mail użytkownika.

     Adres e-mail musi być unikalny. Nie możesz stworzyć następnego konta użytkownika z tym samym adresem e-mail.

     GravityZone używa tego adresu e-mail do wysyłania powiadomień.

     – **Pełna nazwa**. Wprowadź pełną nazwę użytkownika

- **Hasło**. Wprowadź hasło, którego użytkownik może użyć do zalogowania się.

  Hasło musi zawierać co najmniej jedną wielką liter, co najmniej jedną małą literę i co najmniej jedną cyfrę lub jeden znak specjalny.
- **Potwierdź hasło**. Potwierdź hasło

4. W sekcji **Ustawienia i Przywileje**, skonfiguruj poniższe ustawienia:
   - **Strefa czasowa**. wybierz z menu strefę czasową konta. Konsola wyświetli informację o czasie, w zależności od wybranej strefy czasowej.
   - **Język**. Wybierz z menu język wyświetlania w konsoli.
   - **Rola**. Wybierz role użytkownika. Szczegółowe informacje o rolach użytkownika znajdują się w „Role użytkownika” (p. 30).
   - **Prawa**. Każda predefiniowana rola użytkownika ma pewną konfigurację praw. Jednak, powinieneś wybrać jedynie prawa, które potrzebujesz. W tym przypadku, rola użytkownika zmienia się na **Niestandardowe**. Szczegółowe informacje o uprawnieniach użytkownika znajdują się w „Prawa użytkownika” (p. 31).
   - **Wybierz Cele**. Wybierz grupy sieciowe, gdzie użytkownik będzie mieć dostęp do każdej dostępnej usługi bezpieczeństwa. Możesz zastrzec użytkownikowi dostęp do niektórych usług bezpieczeństwa GravityZone lub konkretnych obszarów sieci.

     Notatka
     Opcje sekcji docelowej nie zostanę wyświetlone dla użytkowników z prawami zarządzania rozwiązaniami, domyślnie, posiadają uprawnienia w całej sieci i usługach bezpieczeństwa.

     WAŻNE
     Za każdym razem, gdy dokonujesz zmian w strukturze sieci lub podczas konfigurowania nowej integracji z innym serwerem vCenter lub systemem XenServer, pamiętaj, aby przeglądać i aktualizować uprawnienia dostępu dla istniejących użytkowników.

5. Naciśnij **Zapisz** aby dodać użytkownika. Nowe konto pokaże się na liście kont użytkowników.

Control Center automatycznie wysyła użytkownikom wiadomość e-mail ze szczegółowymi danymi logowania, pod warunkiem, że ustawienia mail serwera zostaną poprawnie skonfigurowane. Aby uzyskać więcej informacji na temat konfiguracji, zapoznaj się z rozdziałami **Instalacja Ochrony > GravityZone Instalacja i ustawienia >Skonfiguruj Centrum Ustawień Control Center** z Podręcznika Instalacyjnego GravityZone.

Indywidualna Edycja Kont Użytkownika

Aby dodać konto użytkownika w Control Center

1. Zaloguj do Control Center.
2. Przejdź do strony **Konta**.
3. Naciśnij na nazwę użytkownika.
4. Zmień szczegóły i ustawienia konta użytkownika według potrzeb.
5. Naciśnij **Zapisz** aby zastosować zmiany.

Notatka
Wszystkie konta z prawami **Zarządzanie Użytkownikami** możne stworzyć, edytować lub usunąć inny użytkownik. Możesz zarządzać tylko kontami z równymi lub mniejszymi przywilejami dla konta.

Indywidualne Usuwanie Kont Użytkownika

Aby usunąć konto użytkownika w Control Center

1. Zaloguj do Control Center.
2. Przejdź do strony **Konta**.
3. Wybierz konto użytkownika z listy.
4. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli.

   Kliknij **Tak**, aby potwierdzić.

5.3.2. Zarządzanie Wieloma Kontami Użytkownika

Utwórz reguły dostępu, aby udzielić GravityZone Control Center dostępu do użytkowników Active Directory na podstawie grup zabezpieczeń.

Warunki wstępne

Aby zarządzać kontem wielu użytkowników, potrzebujesz integracji domeny Active Directory z GravityZone. Aby zintegrować i zsynchronizować domenę Active Directory, zapoznaj się z rozdziałem **Active Directory** z Podręcznika Instalacji GravityZone.

Zależności

Reguły uprawnień dostępu są powiązane z grupami zabezpieczeń usługi Active Directory (AD) i powiązanymi kontami użytkowników. Wszelkie zmiany dokonane w domenach Active Directory mogą mieć wpływ na powiązane reguły uprawnień dostępu. To jest to, co musisz wiedzieć o związku między regułami, użytkownikami i domenami Active Directory:

- Reguła uprawnień dostępu dodaje konto użytkownika tylko wtedy, gdy wiadomość e-mail nie jest już powiązana z istniejącym kontem.
- W przypadku duplikatów adresów e-mail w grupie zabezpieczeń reguła uprawnień dostępu tworzy konto użytkownika GravityZone tylko dla pierwszego konta użytkownika Active Directory, które loguje się w Control Center.

  Na przykład grupa zabezpieczeń zawiera zduplikowany adres e-mail dla różnych użytkowników i wszyscy próbują zalogować się do Control Center przy użyciu swoich poświadczeń Active Directory. Jeśli reguła uprawnień dostępu jest powiązana z tą konkretną domeną usługi Active Directory, utworzy konto użytkownika tylko dla pierwszego użytkownika, który zalogował się do Control Center przy użyciu duplikatu adresu e-mail.
- Konta użytkowników utworzone za pomocą reguł uprawnień dostępu stają się nieaktywne, jeśli zostaną usunięte z powiązanej grupy zabezpieczeń AD. Ci sami użytkownicy mogą stać się aktywni, jeśli są powiązani z nową regułą dostępu.
- Reguły dostępu stają się tylko do odczytu, gdy skojarzona domena Active Directory nie jest już zintegrowana z GravityZone. Użytkownicy powiązani z tymi regułami stają się nieaktywni.
- Konta użytkowników utworzone przez reguły dostępu nie mogą usuwać lokalnie utworzonych użytkowników.
- Konta użytkowników utworzone przez reguły dostępu nie mogą usuwać podobnych kont, które mają rolę Administratora Firmy.

Tworzenie Wielu Kont Użytkownika

Aby dodać wiele kont użytkowników, tworzysz reguły uprawnień dostępu. Reguły uprawnień dostępu są powiązane z grupami zabezpieczeń usługi Active Directory.

Aby dodać regułę uprawnień dostępu:

1. Przejdź do strony **Konfiguracja > Active Directory > Uprawnienia Dostępu**.
2. Jeśli masz wiele integracji, wybierz domenę w lewym górnym rogu tabeli.
3. Kliknij przycisk ⊕ **Dodaj** po lewej stronie tabeli.
4. Skonfiguruj następujące ustawienia uprawnień dostępu:
   - **Priorytet**. Reguły są uporządkowane według priorytetów. Im niższy numer, tym wyższa ważność.
   - **Nazwa**. Nazwa reguły dostępu
   - **Domena**. Domena, z której należy dodawać grupy zabezpieczeń.
   - **Grupy bezpieczeństwa** . Grupy zabezpieczeń, które zawierają przyszłych użytkowników GravityZone. Możesz użyć pola autouzupełniania. Grupy zabezpieczeń dodane na tej liście nie podlegają zmianie, dodaniu ani usunięciu po zapisaniu reguły dostępu.
   - **Strefa czasowa**. Strefa czasowa użytkownika.
   - **Język**. Język wyświetlania konsoli.
   - **Rola**. Predefiniowane role użytkownika. Więcej informacji można znaleźć w rozdziale **Konta użytkowników** z Podręcznika Administratora GravityZone.

     Notatka
     Możesz przyznawać i odwoływać uprawnienia innym użytkownikom z równymi lub mniejszymi uprawnieniami niż konto.

   - **Prawa**. Każda predefiniowana rola użytkownika ma pewną konfigurację praw. Więcej informacji można znaleźć w rozdziale **Prawa użytkownika** w Przewodniku Administratora GravityZone..
   - **Wybierz Cele** Wybierz grupy sieciowe, do których użytkownik będzie miał dostęp dla każdej dostępnej usługi bezpieczeństwa. Możesz zastrzec użytkownikowi dostęp do niektórych usług bezpieczeństwa GravityZone lub konkretnych obszarów sieci.

Notatka
Opcje sekcji docelowej nie zostanę wyświetlone dla użytkowników z prawami zarządzania rozwiązaniami, domyślnie, posiadają uprawnienia w całej sieci i usługach bezpieczeństwa.

5. Kliknij **Zapisz**.

   Reguła dostępu jest zapisywana, jeśli nie ma wpływu na użytkownika. W przeciwnym razie pojawi się monit o określenie wykluczeń użytkowników. Na przykład po dodaniu reguły o wyższym priorytecie wpływowi użytkownicy powiązani z innymi regułami są powiązani z poprzednią regułą.
6. W razie potrzeby wybierz użytkowników, których chcesz wykluczyć. Więcej informacji można znaleźć w Wyłączeniach konta użytkownika .
7. Kliknij **Potwierdź**. Reguła jest wyświetlana na stronie **Uprawnienia Dostępu**.

Użytkownicy w grupach bezpieczeństwa określonych przez reguły dostępu mogą teraz uzyskać dostęp do GravityZone Control Center z poświadczeniami domeny. Control Center automatycznie tworzy nowe konta użytkowników, gdy logują się po raz pierwszy, używając adresu e-mail i hasła usługi Active Directory.

Konta użytkowników utworzone za pomocą reguły dostępu mają nazwę reguły dostępu wyświetlanej na stronie **Konta** w kolumnie **Reguła Dostępu**.

Edycja Wielu Kont Użytkownika

Aby edytować regułę uprawnień dostępu:

1. Przejdź do strony **Konfiguracja > Active Directory > Uprawnienia Dostępu**.
2. Wybierz nazwę reguły dostępu, aby otworzyć okno konfiguracji.
3. Edytuj ustawienia uprawnień dostępu. Więcej informacji znajdziesz w Dodawanie uprawnień dostępu.
4. Kliknij **Zapisz**. Reguła jest zapisywana, jeśli nie ma wpływu na użytkownika. W przeciwnym razie zostanie wyświetlony monit o określenie wykluczeń konta użytkownika. Na przykład, jeśli zaktualizujesz priorytet reguły, wpływowi użytkownicy mogą przełączyć się na inną regułę.
5. W razie potrzeby wybierz użytkowników, których chcesz wykluczyć. Więcej informacji można znaleźć w Wyłączeniach konta użytkownika .
6. Kliknij **Potwierdź**.

Notatka
Możesz rozłączyć konta użytkowników utworzone przez regułę dostępu, modyfikując ich prawa w Control Center. Konto użytkownika nie może zostać powiązane z regułą dostępu.

Usuwanie Wielu Kont Użytkownika

Aby usunąć regułę dostępu:

1. Przejdź do strony **Konfiguracja > Active Directory > Uprawnienia Dostępu**.
2. Wybierz regułę dostępu, którą chcesz usunąć, i kliknij ⊖ **Usuń**. Okno dialogowe prosi o potwierdzenie Twojego działania. Jeśli wystąpi wpływ na użytkownika, pojawi się monit o określenie wykluczeń użytkowników konta. Na przykład możesz określić wykluczenia użytkowników konta dla użytkowników dotkniętych usunięciem reguły.
3. W razie potrzeby wybierz użytkowników, których chcesz wykluczyć. Więcej informacji można znaleźć w Wyłączeniach Konta Użytkownika.
4. Kliknij **Potwierdź**.

Usunięcie reguły spowoduje unieważnienie dostępu do powiązanych kont użytkowników. Wszyscy użytkownicy utworzeni za jego pośrednictwem zostaną usunięci, chyba że inne reguły przyznają im dostęp.

Wyłączenia Konta Użytkownika

Gdy dodajesz, edytujesz lub usuwasz reguły uprawnień dostępu, które powodują wpływ użytkownika, możesz określić wykluczenia konta użytkownika. Możesz także przejrzeć uzasadnienie i skutki wpływu użytkowników.

Określ wykluczenia użytkowników w następujący sposób:

1. Zaznacz użytkowników, których chcesz wykluczyć. Lub zaznacz pole wyboru u góry tabeli, aby dodać wszystkich użytkowników do listy.
2. Kliknij **X** w polu nazwy użytkownika, aby usunąć go z listy.

5.4. Resetowanie haseł logowania

Właściciele kont, którzy zapomnieli swoich haseł, mogą zresetować je przez użycie linku przywracania hasła na stronie logowania. Możesz również zresetować zapomniane hasło logowania przez edytowanie danego konta w konsoli.

aby zresetować hasło logowania dla użytkownika:

1. Zaloguj do Control Center.
2. Przejdź do strony **Konta**.
3. Naciśnij na nazwę użytkownika.
4. Podaj nowe hasło w odpowiednim polu (w **Szczegóły**).
5. Naciśnij **Zapisz** aby zastosować zmiany. Właściciel konta dostanie wiadomość e-mail z nowym hasłem.

5.5. Zarządzanie Uwierzytelnieniem Dwuskładnikowym

Klikając konto użytkownika, będziesz mógł zobaczyć jego status 2FA (włączony lub wyłączony) w sekcji **Uwierzytelnienie Dwuskładnikowe**. Możesz podjąć następujące działania:

- **Zresetuj lub wyłącz uwierzytelnianie dwuskładnikowe użytkownika** . Jeśli użytkownik z włączoną opcją 2FA zmienił lub wyczyścił urządzenie przenośne i zgubił tajny klucz:
  1. Wprowadź swoje hasło GravityZone w dostępnym polu.
  2. Kliknij **Zresetuj** (gdy 2FA jest wymuszane) lub **Wyłącz** (gdy 2FA nie jest wymuszane).
  3. Komunikat potwierdzający informuje, że uwierzytelnianie dwuskładnikowe zostało zresetowane / wyłączone dla bieżącego użytkownika.

     Po zresetowaniu 2FA, gdy ta funkcja jest wymuszona, podczas logowania okno konfiguracji poprosi użytkownika o ponowne skonfigurowanie uwierzytelniania dwuskładnikowego za pomocą nowego tajnego klucza.
- Jeśli użytkownik ma wyłączone 2FA i chcesz je aktywować, musisz poprosić użytkownika o włączenie tej funkcji z jego ustawień konta.

> **Notatka**
> Jeśli masz konto Administratora firmy możesz włączyć autentykację dwuetapową jako obowiązkową dla wszystkich kont GravityZone. Znajdź więcej informacji w Przewodniku Instalacji, pod **Instalowanie Ochrony > Instalacja i Konfiguracja GravityZone > Konfiguruj Ustawienia Control Center**.

WAŻNE
Wybrana aplikacja uwierzytelniająca (Google Authenticator, Microsoft Authenticator lub inna aplikacja uwierzytelniania dwuskładnikowego TOTP (Time-Based One-Time Password Algorithm) - kompatybilną ze standardem RFC6328 łączy sekretny klucz wraz z czasem mobilnego urządzenia w celu wygenerowania sześcioznakowego kodu. Pamiętaj, że znaczniki czasu na urządzeniu mobilnym i urządzeniu GravityZone muszą być zgodne, aby sześciocyfrowy kod był poprawny. Aby uniknąć problemów z synchronizacją znaczników czasu, zalecamy włączenie automatycznego ustawienia daty i godziny na urządzeniu mobilnym.

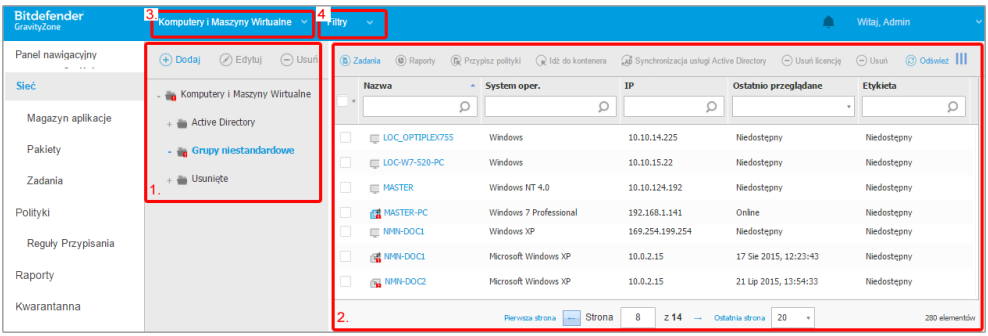
Inną metodą sprawdzania zmian 2FA związanych z kontami użytkowników jest dostęp do strony **Konta > Aktywność Użytkownika** i filtrowanie dzienników aktywności przy użyciu następujących filtry:

- Obszar > Konta / Firma
- Działanie > Zmieniono

Aby uzyskać więcej informacji na temat włączania funkcji 2FA, zapoznaj się z „Zarządzanie kontem” (p. 25)

6. ZARZĄDZANIA OBIEKTAMI SIECI

Strona **Sieć** dostarcza kilku funkcji do przeglądania i zarządzania widocznymi wpisami dostępnymi w Control Center (komputery, maszyny wirtualne i urządzenia przenośne). Sekcja **Sieć** składa się z dwóch paneli interfejsu wyświetlających w czasie rzeczywistym status obiektów sieciowych:



Strona Sieci

1. Lewy panel wyświetla dostępną strukturę drzewka sieci. W zależności od wybranego widoku sieci, ten panel wyświetać będzie infrastruktury sieciowe zintegrowane za pomocą Control Center z Active Directory, vCenter Server lub Xen Server.

   Jednocześnie, wszystkie komputery i maszyny wirutalne wykryte w sieci, nienależące do żadnej zintegrowanej infrastruktury są wyświetlane pod **Niestandardowe grupy**

   Wszystkie usunięte stacje końcowe są gromadzone w katalogu **Usunięte** Aby dowiedzieć się więcej, zobacz „Usuwanie punktów końcowych z zasobów sieci” (p. 210).

   Notatka
   Możesz przeglądać i zarządzać tylko grupami, które maja prawa administracyjne.

2. Prawa strona panela wyświetla zawartość grup które wybrałeś z lewej strony. Ten panel składa się z siatki, w której wiersze zawierają obiekty sieciowe, a kolumny wyświetlają szczegółowe informacje dla każdego obiektu.Ten panel

składa się z sieci, w której wiersze zawierają obiekty sieci i kolumny wyświetlania szczegółowych informacji dla każdego typu obiektu.

W tym panelu, możesz zrobić poniższe punkty:

- Zobacz szczegółowe informacje o każdym obiekcie sieciowym na twoim koncie. Możesz zobaczyć status każdego obiektu sprawdzając ikonę obok nazwy. Umieść kursor na ikonie, aby wyświetlić więcej informacji. Naciśnij nazwę obiektu aby wyświetlić okno zawierające więcej informacji.

  Każdy typ obiektu, taki jak komputer, maszyna wirtualna, katalog jest reprezentowana przez właściwą ikonę. W tym samym czasie, każdy obiekt sieciowy posiada swój konkretny status zależny od stanu zarządzania, kwestii bezpieczeństwa, łączności itp. Dla uzyskania szczegółów odnoszących się do opisu każdej ikony obiektu sieciowego i dostępnych statusów spójrz do „Typy obiektów sieciowych i statusy” (p. 514).
- Użyj Paska narzędzi działania z górnej części tabeli do wykonywania określonych czynności dla poszczególnych obiektów sieciowych (takich jak uruchamianie zadań, tworzenie raportów, przypisywanie polityk i usuwanie) następnie odśwież dane tabeli.

3. selektor widoku w górnej części panel sieci pozwala przełączać się pomiędzy różnymi inwentaryzacjami zawartości sieci, w zależności od typu punktu kocowego, na którym chcesz pracować.
4. Menu **Filtry** dostępne w górnej części panelu sieci pomaga Ci łatwo wyświetlić tylko określone obiekty sieci, dostarczając wiele kryteriów filtrów. Opcje menu **Filtry** jest powiązane do bieżącego widoku sieci.

Z sekcji **Sieć** można zarządzać pakietami instalacyjnymi i zadaniami dla każdego typu obiektu sieciowego.

Notatka
Aby dowiedzieć się więcej o pakietach instalacyjnych, zapoznaj się z Instrukcją instalacji GravityZone.

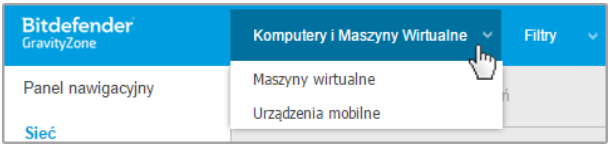
W celu uzyskania szczegółowych informacji o obiektach sieciowych odwołaj się do:

- „Praca z widokami sieci” (p. 44)
- „Komputery” (p. 47)
- „Maszyny wirtualne” (p. 106)
- „Urządzenia mobilne” (p. 166)
- „Inwentarz Aktualizacji” (p. 197)

6.1. Praca z widokami sieci

Różne typy punktów końcowych dostępnych w Control Center są grupowane na stronie **Sieć** z wykorzystaniem różnych widoków sieciowych. Każdy widok sieci wyświetla specyficzny typ infrastruktury sieci, w zależności od rodzaju punktu końcowego którym chcemy zarządzać.

Aby zmienić widok sieci, przejdź do górnej lewej części strony **Sieć** i kliknij przełącznik wyświetleń:



Przełącznik odsłony

Następujące widoki sieci dostępne są:

- Komputery i Maszyny Wirtualne
- Maszyny wirtualne
- Urządzenia mobilne

6.1.1. Komputery i Maszyny Wirtualne

Widok ten zaprojektowany jest dla komputerów i maszyn wirtualnych zintegrowanych z Active Directory, dostarczając specyficznych akcji i filtrów opcji dla zarządzania komputerami w twojej sieci. Jeżeli integracja Active Directory jest dostępna, drzewko Active Directory zostaje załadowane wraz z odpowiednimi punktami końcowymi.

Podczas pracy w widoku **Komputery i Maszyny Wirtualne**, możesz w każdym momencie synchronizować zawartość Control Center z własnym Active Directory używając przycisku **Synchronizacja z Active Directory** z Paska Działania Akcji.

W tym samym czasie, wszystkie komputery i maszyny wirtualne, które nie są zintegrowane z Active Directory są pogrupowane pod Grupami Niestandardowymi. Ten folder może zawierać następujące typy końcówek:

- Komputery i maszyny wirtualne dostępne w Twojej sieci poza Active Directory.
- Maszyny Wirtualne ze zwirtualizowanej infrastruktury dostępnej w Twojej sieci.
- Serwery Bezpieczeństwa już zainstalowane i skonfigurowane na hoście w Twojej sieci.

Notatka
Gdy infrastruktura zwirtualizowana jest dostepna, możesz wdrożyć i zarządzać Serwerami Bezpieczeństwa z widoku **Maszyn Wirtualnych**. W przeciwnym wypadku, Serwery Bezpieczeństwa mogą być jedynie zainstalowane i skonfigurowane lokalnie na hoście.

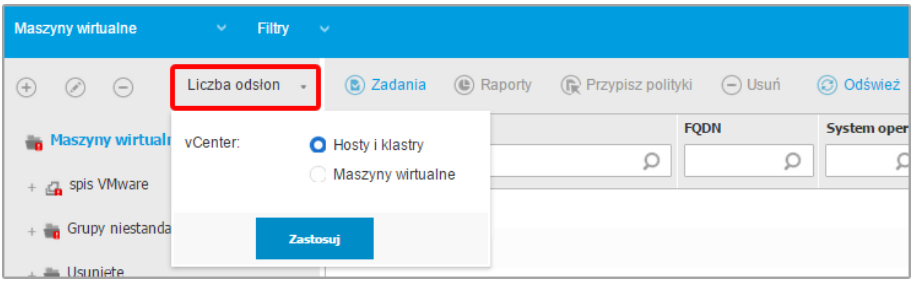
WAŻNE
Przypisywanie zasad do maszyn wirtualnych z poziomu **Komputery i Maszyny Wirtualne** może być ograniczone przez menedżera rozwiązania GravityZone podczas konfigurowania serwera vCenter lub serwera Xen na stronie **Konfiguracji > Dostawcy Wirtualizacji**. Aby dowiedzieć się więcej, przejdź do rozdziału **Instalowanie Ochrony > GravityZone Instalacja i Ustawienia** w Instrukcji Instalacji GravityZone.

6.1.2. Maszyny wirtualne

Pogląd ten jest specjalnie zaprojektowany, aby wyświetlać zwirtualizowane integracje infrastruktury. Dostępne w tym podglądzie opcje filtrowania pozwalają Tobie wybrać specjalne kryteria wyświetlania wpisów środowiska wirtualnego.

Możesz zobaczyć swoje wirtualne wirtualne zasoby Nutanix, VMware oraz Citrix po lewej stronie panela.

W górnej części lewego panela możesz również znaleźć menu **Wyświetlenia** pozwalające na wybranie opcji wyświetlania inwentaryzacji wirtualnej.



Strona sieciowa - widok Maszyn Wirtualnych

Wszystkie maszyny wirtualne w twojej sieci, które nie są zintegrowane z infrastrukturą wirtualną są wyświetlane pod **Niestandardowa Grupa**.

Aby uzyskać dostęp do zwirtualizowanej infrastruktury zintegrowanej z Control Center musisz dostarczyć swojemu użytkownikowi poświadczeń dla każdego dostępnego systemu serwera vCenter. Control Center używa twoich poświadczeń aby połączyć z wirtualną infrastrukturą, pokazywanie tylko zasobów do których masz dostęp (jak określono vCenter Serwer). Jeżeli nie określiłeś poświadczeń uwierzytelnienia, będziesz musiał podać je podczas próby przeglądania spisu dowolnego Serwera vCenter. Po wprowadzeniu swoich poświadczeń, zostaną one zapisane w Menadżerze Poświadczeń tak, by nie było potrzeby wprowadzania ich ponownie.

6.1.3. Urządzenia mobilne

Pogląd ten jest przeznaczony wyłącznie do przeglądania i zarządzania urządzeniami mobilnymi dostępnymi w sieci, zapewniając konkretne działania i opcje filtrowania.

W tym konkretnym widoku można wyświetlić przedmioty sieciowe według użytkowników lub urządzeń.

Panel sieciowy wyświetla Twoją strukturę drzewa Active Directory, jeśli jest dostępna. W tym przypadku, wszyscy użytkownicy Active Directory pojawią się w inwentaryzacji sieci, a także urządzeniach mobilnych im przypisanym.

Notatka
Dane użytkownika Active Directory są automatycznie ładowane i nie mogą być zmieniane.

Niestandardowe Grupy zawierają wszystkich użytkowników urządzeń mobilnych, które zostały dodane ręcznie do Control Center.

6.2. Komputery

Aby wyświetlić komputery przypisane do twojego kota, przejdź do strony **Sieć** i wybierz **Komputery i Maszyny Wirtualne** z selektor sieci.

Możesz przeglądać dostępne struktury sieciowe w lewym bocznym panelu oraz szczegóły na temat każdego punktu końcowego po prawej stronie okienka.

Z początku wszystkie komputery i maszyny wirtualne wykryte w sieci są wyświetlane jako niezarządzane tak by można było zdalnie zainstalować na nich ochronę.

Aby dostosować szczegóły komputera wyświetlone w tabeli:

1. Kliknij przycisk III **Kolumny** z prawej strony Akcja Pasek narzędzi.
2. Wybierz kolumny, które chcesz zobaczyć.
3. Naciśnij przycisk **Reset** aby przywrócić domyślny widok kolumn.

Ze strony **Sieć**, możesz zarządzać punktami końcowymi, według poniższych:

- Sprawdź Stan Komputera
- Przeglądanie szczegółów komputera
- Organizowanie komputerów w grupy
- Sortuj, filtruj i wyszukuj
- Zarządzaj aktualizacjami
- Uruchom zadania
- Twórz szybkie raporty
- Przydziel polityki
- Synchronizuj z Active Directory

Aby przeglądać najnowsze informacje w tabeli, kliknij przycisk ⟳ **Odśwież** w lewym dolnym rogu tabeli. Może być potrzebne abyś spędził więcej czasu na tej stronie.

6.2.1. Sprawdzanie Statusu Komputerów

Na stronie sieci, każdy komputer reprezentuje ikona określająca jego typ i status.

Odnieś się do „Typy obiektów sieciowych i statusy” (p. 514) dla listy ze wszystkimi dostępnymi typami ikon i statusów.

Aby uzyskać szczegółowe informacje, odwołaj się do:

- Stan zarządzania
- Stan łączności

- Stan bezpieczeństwa

Stan zarządzania

Komputery mogą mieć poniższe statusy zarządzania:

- **Zarządzane** - komputery, na których został zainstalowany agent bezpieczeństwa.
- **W oczekiwaniu na restart** - punkty końcowe, które wymagają ponownego uruchomienia systemu po zainstalowaniu lub zaktualizowaniu ochrony Bitdefender.
- **Niezarządzane** - wykrywa komputery, na których agent bezpieczeństwa nie został jeszcze zainstalowany.
- **Usunięte** - komputery które usunięto z Control Center. Aby uzyskać więcej informacji, odwołaj się do „Usuwanie punktów końcowych z zasobów sieci” (p. 210).

Stan łączności

Dotyczy stanu połączenia tylko na zarządzanych komputerach. Z tego punktu widzenia, zarządzane komputery mogą:

- **Online**. Niebieska ikona oznacza, że komputer jest online.
- **Offline**. Szara ikona oznacza, że komputer jest offline.

Komputer zostanie oznaczony jako offline w momencie gdy agent bezpieczeństwa będzie nieaktywny przez czas co najmniej 5 minut. Możliwe powody dlaczego komputery są offline:

- Komputer jest wyłączony, uśpiony albo w hibernacji.

  Notatka
  Komputery pojawiają się w internecie nawet, gdy są zablokowane lub użytkownik jest wylogowany.

- Agenci ochrony nie posiadają łączności z serwerem komunikacyjnym GravityZone:
  - Komputer może być odłączony od sieci.
  - Zapora sieciowa lub router może blokować komunikację pomiędzy agentem ochrony a serwerem komunikacji GravityZone.

– Komputer znajduje się za serwerem proxy a ustawienia proxy nie zostały prawidłowo skonfigurowane dla zastosowanej polityki.

Ostrzeżenie
Dla komputerów znajdujących się za serwerem proxy, ustawienia powinny być prawidłowo skonfigurowane w paczce instalacyjnej agenta bezpieczeństwa, w innym wypadku komputer nie nawiąże komunikacji z konsolą GravityZone i pozostanie offline, bez względu na to czy polityka z prawidłowymi ustawieniami proxy została zastosowana zaraz po instalacji.

- Agent bezpieczeństwa może nie działać poprawnie.

Aby dowiedzieć się, jak długo komputery były nieaktywne:

1. Wyświetl tylko zarządzane komputery. Kliknij menu **Filtry** zlokalizowane z górnej strony tabeli, wybierz wszystkie "Zarządzane" opcje, które potrzebujesz z zakładki **Bezpieczeństwo**, wybierz **Wszystkie obiekty rekurencyjne** z zakładki **Głębokość** i kliknij **Zapisz**.
2. Naciśnij nagłówek kolumny **Ostatnio Widziane** aby posortować komputery według okresu bezczynności.

Można zignorować krótsze okresy bezczynności (minuty, godziny), ponieważ są prawdopodobnie wynikiem warunku czasowego. Na przykład, komputer jest aktualnie wyłączony.

Dłuższe okresy bezczynności (dni, tygodnie), zazwyczaj wskazują na problem z komputerem.

Notatka
Zalecane jest by odświeżyć tabelę sieci od czasu do czasu, aby zaktualizować informacje o najnowszych zmianach na punktach końcowych.

Stan bezpieczeństwa

Dotyczy stanu bezpieczeństwa tylko na zarządzanych komputerach. Możesz zidentyfikować komputery z problemami bezpieczeństwa poprzez sprawdzenie statusu ikony wyświetlającej symbol ostrzeżenia:

- Zarządzany komputer, z problemami, online.
- Zarządzany komputer, z problemami, offline.

Komputer ma problemy z bezpieczeństwem, co najmniej jedna z poniższych sytuacji ma zastosowanie:

- Ochrona antymalware jest wyłączona.
- Klucz licencyjny wygasł.
- Agent bezpieczeństwa produktu jest przestarzały.
- Zawartość bezpieczeństwa jest nieaktualna.
- Wykryto złośliwe oprogramowanie.
- Łączność z Usługą Chmury Bitdefender nie może zostać ustalona, z następujących przyczyn:
  - Komputer posiada problemy z łączem internetowym.
  - Zapora sieciowa blokuje połączenie z Usługą Chmury Bitdefender.
  - Port 443, wymagany do komunikacji z Usługą Chmury Bitdefender jest zamknięty.

  W tym przypadku ochrona przed złośliwym oprogramowaniem opiera się wyłącznie na silnikach lokalnych, podczas gdy skanowanie w chmurze jest wyłączone oznacza to, że agent ochrony nie może dostarczyć pełnej ochrony w czasie rzeczywistym.

Jeżeli zauważysz komputer z problemami bezpieczeństwa, kliknij jego nazwę aby wyświetlić okno **Informacje**. Można identyfikować problemy bezpieczeństwa poprzez ikonę ! . Upewnij się, aby sprawdzić informacje o ochronie we wszystkich zakładkach informacji na stronie. Wyświetl ikony podpowiedzi aby znaleźć więcej szczegółów. Mogą być potrzebne dalsze badania lokalne.

Notatka
Zalecane jest by odświeżyć tabelę sieci od czasu do czasu, aby zaktualizować informacje o najnowszych zmianach na punktach końcowych.

6.2.2. Przeglądanie szczegóły komputera.

Możesz uzyskać szczegółowe informacje o każdym komputerze w zakładce **Sieć**, w następujący sposób:

- Sprawdzanie zakładki **Sieci**
- Sprawdzanie okna **Informacji**

Sprawdzane strony Sieci

Aby dowiedzieć się szczegółów dotyczących komputera, sprawdź informacje dostępne w tabeli po prawej stronie ekranu na stronie **Sieć**.

Kolumny można dodawać lub usuwać za pomocą informacji o punkcie końcowym, klikając przycisck **Kolumny** W prawym górnym rogu panelu.

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego.

   Wszystkie punkty końcowe dostępne w wybranej grupie są wyświetlane w prawym panelu tabeli.
4. Możesz w łatwy sposób zidentyfikować stan komputera przez sprawdzenie odpowiedniej ikony. Szczegółowe informacje znajdują się w „Sprawdzanie Statusu Komputerów” (p. 47).
5. Sprawdź informacje wyświetlane w kolumnach dla każdego komputera.

   Użyj wiersza nagłówka do wyszukiwania podczas wpisywania określonych punktów końcowych, zgodnie z dostępnymi kryteriami:

   - **Nazwa**: nazwa punktu końcowego.
   - **FQDN**: w pełni kwalifikowana nazwa domeny zawierająca nazwę hosta i nazwę domeny.
   - **OS**: system operacyjny zainstalowany na punkcie końcowym.
   - **IP**: adres IP punktu końcowego.
   - **Ostatnio Widziany**: Data i godzina kiedy punkt końcowy był ostatnio widziany.

     Notatka
     Monitorowanie pola **Ostatnio widziany** jest istotne, ponieważ dłuższe okresy bezczynności mogą wskazywać na problem z komunikacją lub odłączenie komputera.

   - **Etykieta**: niestandardowy opis z dodatkowymi informacjami na temat punktu końcowego. Możesz dodać etykietę w oknie **Informacje** punktu końcowego, a następnie użyć go w wyszukiwaniu.
   - **Polityka**: polityka dotycząca punktu końcowego z linkiem do przeglądania lub zmiany ustawień polityki.

Sprawdzanie okna Informacji

W prawym okienku strony **Sieć** kliknij nazwę punktu końcowego, który Cię interesuje, aby wyświetlić okno **Informacje**. To okno wyświetla tylko dane dostępne dla wybranego punktu końcowego, pogrupowane na kilka kart.

Poniżej znajdziesz wyczerpującą listę informacji, które można znaleźć w oknie **Informacje** w zależności od typu punktu końcowego i konkretnych informacji o jego zabezpieczeniach.

Zakładka Ogólne

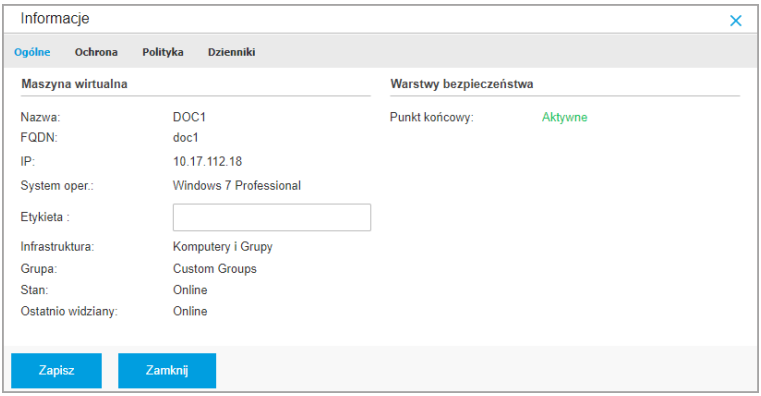
- Najważniejsze informacje o komputerze jak : FQDN, adres IP, System Operacyjny, infrastruktura, grupa nadrzędna i obecny status połączenia.

  W tej sekcji można przypisać etykietę punktowi końcowemu. Będziesz mógł szybko znaleźć punkty końcowe o tej samej etykiecie i podejmować na nich działania, niezależnie od tego, gdzie znajdują się w sieci. Aby uzyskać więcej informacji o filtrowaniu punktów końcowych, przejdź do „Sortowanie, filtrowanie i wyszukiwanie komputerów.” (p. 67).

- Informacje o warstwach zabezpieczających, w tym listę technologii zabezpieczeń zakupionych wraz z rozwiązaniem GravityZone i ich statusem licencji, które mogą być:
  - **Dostępny / Aktywny** - klucz licencyjny dla tej warstwy ochronnej jest aktywny na punkcie końcowym.
  - **Wygasł** - klucz licencyjny dla tej warstwy ochrony wygasł.
  - **Oczekujący** - klucz licencyjny nie został jeszcze zatwierdzony.

  > **Notatka**
  > Dodatkowe informacje o warstwach ochrony są dostępne w zakładce **Ochrona**.

- **Połączenie przekaźnikowe**: nazwa, adres IP i etykieta przekaźnika, do którego podłączony jest punkt końcowy.



Okno informacyjne - Ogólne

Zakładka Ochrony

Ta zakładka zawiera informacje na temat ochrony zastosowanej na punkcie końcowym i odnosi się do:

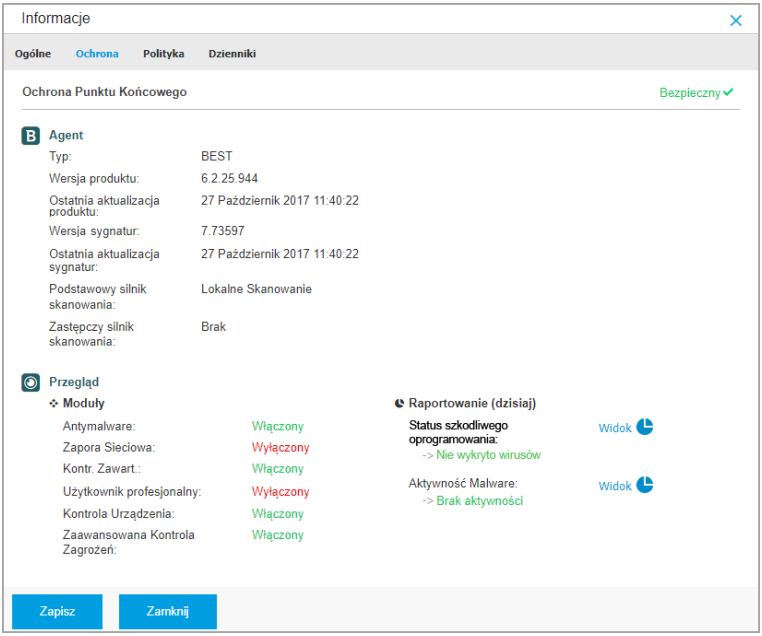
- Informacje agenta bezpieczeństwa takie jak nazwa produktu, wersja, status aktualizacji i lokalizacja aktualizacji jak i również silniki skanowania, konfiguracja i wersje zawartości bezpieczeństwa Dla Ochrony Exchange, wersja silnika antyspamowego także jest dostępna.
- Status zabezpieczenia każdej warstwy ochrony. Ten status pojawia się po prawej stronie nazwy warstwy zabezpieczającej:
  - **Bezpieczny**, jeśli nie wystąpiły problemy dotyczące zabezpieczeń punktów końcowych, na których zastosowana jest warstwa ochrony.
  - **Narażony**, jeśli wystąpiły problemy dotyczące zabezpieczeń punktów końcowych, na których zastosowana jest warstwa ochrony. Szczegółowe informacje znajdują się w „Stan bezpieczeństwa” (p. 49).
- Powiązany Security Server. Każdy przydzielony Security Server wyświetlany jest w przypadku bez-agentowego wdrożenia lub kiedy silniki skanowania agentów ochrony są ustawione na zdalne skanowanie. Informacje o Security Server pomagają ci zidentyfikować wirtualne urządzenie i dostać status jego aktualizacji.

- Status nodułów ochrony. Możesz z łatwością zobaczyć, który moduł ochrony został zainstalowany na punkcie końcowym oraz sprawdzić status dostępnych modułów (**Wł/Wył.**) ustawionych przez zastosowane polityki.
- Szybki przegląd dotyczący aktywności modułów i raportowania malware w obecnym dniu.

  Kliknij link **Zobacz** aby wejść do opcji raportów i wtedy wygenerować raport. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie raportów” (p. 435)
- Informacje dotyczące warstwy ochrony Sandbox Analyzer:
  - Status wykorzystania Sandbox Analyzer na punkcie końcowym, wyświetlany po prawej stronie okna:
    - **Aktywny**: Sandbox Analyzer jest licencjonowany (dostępny) i włączony poprzez politykę w punkcie końcowym.
    - **Nieaktywny**: Sandbox Analyzer jest licencjonowany (dostępny) ale nie jest włączony poprzez politykę w punkcie końcowym.
  - Nazwa agenta, który pełni rolę czujnika zasilania.
  - Status modułu na punkcie końcowym:
    - **Włączony** - Sandbox Analyzer jest włączony w punkcie końcowym za pomocą polityki.
    - **Wyłączony** - Sandbox Analyzer nie jest włączony w punkcie końcowym za pomocą polityki.
  - Wykrywanie zagrożeń z poprzedniego tygodnia klikając link **Pokaż**, aby uzyskać dostęp do raportu.
- Dodatkowe informacje dotyczące modułu szyfrowania, takie jak:
  - Wykryte woluminy (wspominające dysk rozruchowy).
  - Stan szyfrowania dla każdego woluminu (**Zaszyfrowane**, **Szyfrowanie w toku**, **Odszyfrowywanie w toku**, **Niezaszyfrowane**, **Zablokowane** lub **Wstrzymane**).

    Kliknij link **Odzyskiwanie** aby pobrać klucz odzyskiwania dla powiązanych zaszyfrowanych woluminów. Szczegółowe informacje na temat pobierania kluczy odzyskiwania można znaleźć w „” (p. 105).

- Status telemetrii bezpieczeństwa, który informuje Cię czy ustanowione jest połączenie pomiędzy punktem końcowym i serwerem SIEM jest ustanowione oraz czy działa, jest wyłączone lub ma problemy.



Okno informacyjne - zakładka Ochrony

Zakładka Polityki

W punkcie końcowym może być zastosowana jedna lub kilka polityk, ale tylko jedna polityka może być aktywna w tym samym czasie. Zakładka **Polityka** wyświetla informacje o wszystkich politykach odnoszących się do punktu końcowego.

- Nazwa aktywnej polityki. Kliknij nazwę polityki by otworzyć szablon polityki oraz zobaczyć swoje ustawienia.
- Typ aktywnej polityki, taki jak:
  - **Urządzenie**: gdy polityka jest przypisana ręcznie do punktu końcowego przez administratora sieci.

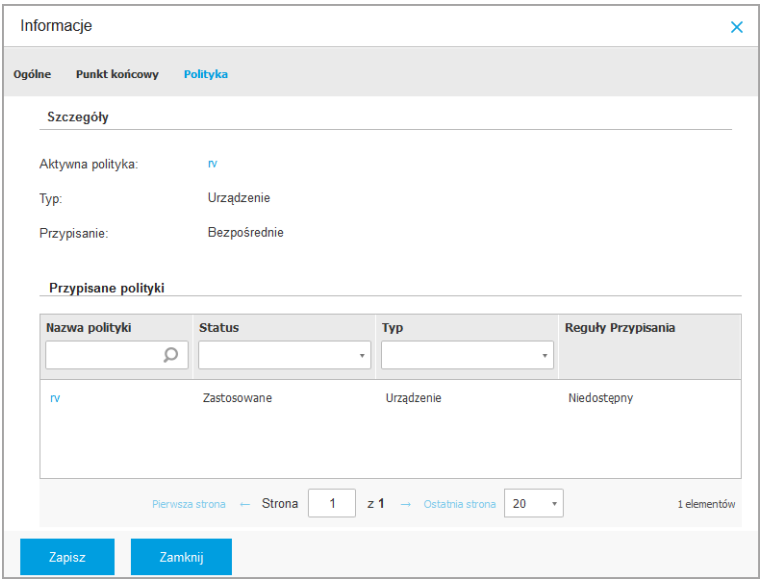
- **Lokalizacja**: polityka oparta na zasadach jest automatycznie przypisywana do punktu końcowego, jeśli ustawienia sieciowe punktu końcowego są zgodne z warunkami istniejącej zasady przypisywania.

  Na przykład, laptop ma przypisane 2 polityki świadomości lokalizacji: jedna nazwana `Biuro`, która jest aktywna gdy łączy się z siecią firmową LAN, a druga `Roaming`, która staje się aktywna, gdy użytkownik pracuje zdalnie i łączy się do innej sieci.

- **Użytkownik**: polityka oparta na zasadach jest automatycznie przypisywana do punktu końcowego, jeśli odpowiada ona celom Active Directory określonym w istniejącej zasadzie przypisywania.

- **Zewnętrzny (NSX)**: gdy polityka jest zdefiniowana w środowisku VMware NSX.

- Typ przypisania aktywnej polityki, taki jak:
  - **Bezpośrednia**: gdy polityka jest bezpośrednio stosowana do punktu końcowego.
  - **Odziedziczona**: jeśli punkt końcowy dziedziczy politykę z grupy nadrzędnej.
- **Obowiązujące polityki**: wyświetla listę polityk powiązanych z istniejącymi regułami przypisywania. Zasady te mogą mieć zastosowanie do punktu końcowego, jeśli jest on zgodny z określonymi warunkami reguł przypisania.

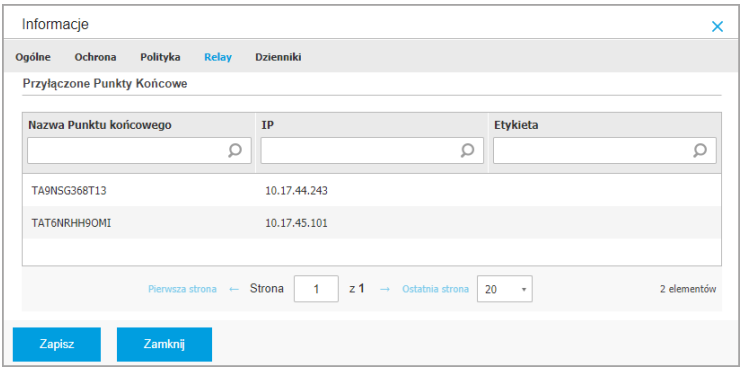


Okno informacyjne - Polityka

Aby uzyskać więcej informacji dotyczących polityk, zapoznaj się z „Zmiany ustawień polityk.” (p. 232)

Zakładka Połączone Punkty końcowe

Zakładka **Połączone Punkty końcowe** jest dostępna tylko dla punktów z rolą Relay. Ta zakładka wyświetla informacje na temat punktów końcowych połączonych to aktualnego pośrednika, takie jak nazwa, IP i etykieta.

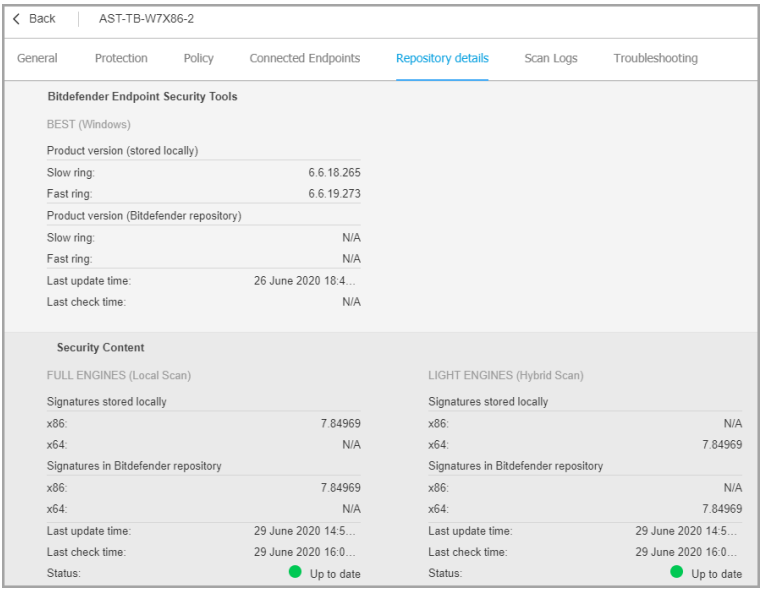


Okno Informacyjne - Zakładka połączone punkty końcowe

Zakładka Szczegóły repozytorium

Zakładka **Szczegóły Repozytorium** jest dostępna tylko dla punktów końcowych z rolą Relay i wyświetla informacje o aktualizacjach agenta bezpieczeństwa i zawartości bezpieczeństwa.

Zakładka zawiera szczegółowe informacje o produkcie i wersjach podpisów przechowywanych na relay'u i tych dostępnych w oficjalnym repozytorium, pierścienie aktualizacji, datę i godzinę aktualizacji oraz ostatnie sprawdzenie dostępności nowych wersji.



Okno informacyjne - zakładka Szczegóły repozytorium

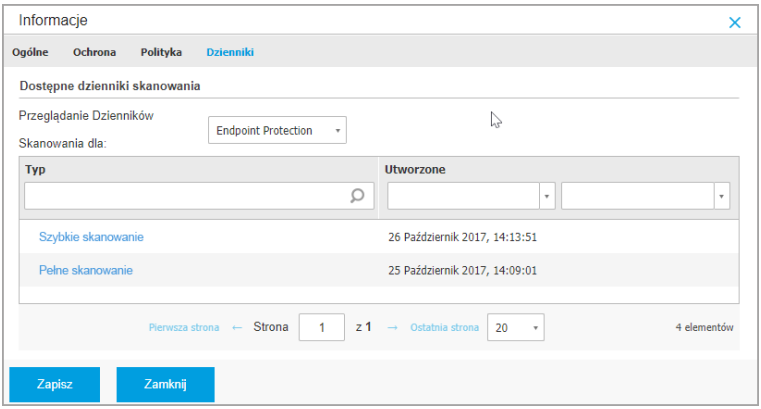
Zakładka Dziennika Skanowania

Zakładka **Dzienniki Skanowania** wyświetla szczegółowe informacje na temat wszystkich zadań skanowania wykonanych na punkcie końcowym.

Logi są pogrupowane według warstw ochrony i możesz wybrać z rozwijalnej listy z której warstwy chcesz wyświetlić logi.

Kliknij zadanie skanowania, które cie interesuje, następnie log otworzy się w nowej karcie przeglądarki.

Kiedy wiele logów skanowania jest dostępnych, mogą rozszerzać się przez wiele stron. Do poruszania się po kolejnych stronach służą opcje nawigacji znajdujące się na dole tabeli. Jeżeli jest tam za dużo wpisów, możesz użyć opcji filtra dostępnych na górze tabeli.

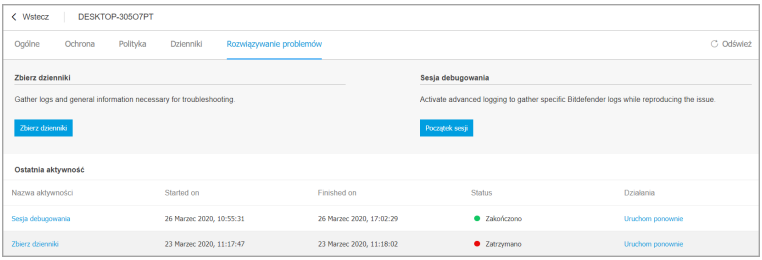


Okno informacyjne - logi skanowania

Tabela Rozwiązywanie problemów

Ta sekcja jest poświęcona działaniom rozwiązywania problemów z agentami. Możesz zbierać logi ogólne lub szczegółowe z punktu końcowego lub podejmować działania w związku z bieżącymi zdarzeniami dotyczącymi rozwiązywania problemów i przeglądać poprzednie działania.

WAŻNE
Rozwiązywanie problemów jest dostępne dla systemu Windows oraz wszystkich rodzajów typów serwerów bezpieczeństwa.



Okno informacyjne - Tabela Rozwiązywania problemów

- **Zbierz dzienniki**

  Ta opcja pomaga zebrać zestaw logów i ogólne informacje niezbędne do rozwiązywania problemów, takie jak ustawienia, aktywne moduły lub polityki

specyficzne dla docelowej maszyny. Wszystkie wygenerowane dane są zapisywane w archiwum.

Zaleca się użycie tej opcji, gdy przyczyna problemu jest niejasna.

Aby rozpocząć proces rozwiązywania problemów:

1. Kliknij przycisk **Zbierz logi**. Wyświetlono okno konfiguracji.
2. W sekcji **Przechowywanie Logów**, wybierz lokalizację magazynu:
   - **Docelowa maszyna**: archiwum logów zostanie zapisane w podanej lokalnej ścieżce Nie można skonfigurować tej ścieżki dla Serwerów Bezpieczeństwa.
   - **Udział sieciowy**: Archiwum logów jest zapisywane w dostarczonej ścieżce z współdzielonej lokacji.

   Możesz użyć opcji **Zapisz logi również na docelowej maszynie**, aby zapisać kopię archiwum logów w zagrożonym punkcie końcowym jako kopię zapasową.
3. Podaj niezbędne informacje (ścieżka lokalna, poświadczenia dla udziału sieciowego, ścieżka do udostępnionej lokalizacji) w zależności od wybranej lokalizacji.
4. Kliknij przycisk **Zbierz logi**.

- **Sesja debugowania**

  Za pomocą sesji debugowania można aktywować zaawansowane rejestrowanie na wybranej maszynie, aby zebrać określone logi podczas odtwarzania problemu.

  Powinieneś użyć tej opcji, gdy dowiedziałeś, który moduł powoduje problemy lub na polecenie Biznesowej Pomocy Bitdefender. Wszystkie wygenerowane dane są zapisywane w archiwum.

  Aby rozpocząć proces rozwiązywania problemów:

  1. Kliknij przycisk **Rozpocznij sesję**. Wyświetlono okno konfiguracji.
  2. W sekcji **Typ problemu**, wybierz problem, który Twoim zdaniem wpływa na maszynę:

     Rodzaje problemów dla maszyn z systemem Windows i macOS:

Rodzaj zagadnienia	Przypadek użycia
Antymalware (skanowanie Dostępowe i Na żądanie)	– Ogólne spowolnienie punktu końcowego – Odpowiedź programu lub zasobu systemowego trwa zbyt długo – Proces skanowania trwa dłużej niż zwykle – Błąd połączenia z usługą bezpieczeństwa hosta
Błędy aktualizacji	– Wiadomości o błędach otrzymane podczas aktualizacji produktu lub treści bezpieczeństwa
Kontrola Zawartości (skanowanie ruchu i kontrola użytkownika)	– Witryna się nie wczytuje – Elementy strony internetowej nie są wyświetlane poprawnie
Łączność z usługami w chmurze	– Punkt końcowy nie ma łączności z Bitdefender Cloud Services
Ogólne problemy z produktem (rejestrowanie wysokiej szczegółowości)	– Odtwórz ogólny zgłoszony problem z pełnym rejestrowaniem

Rodzaje problemów dla maszyn z Linux:

Rodzaj zagadnienia	Przypadek użycia
Antymalware i Aktualizacja	– Proces skanowania trwa dłużej niż zwykle i zużywa więcej zasobów – Wiadomości o błędach otrzymane podczas aktualizacji produktu lub treści bezpieczeństwa – Punkt końcowy nie łączy się z konsolą GravityZone.
Ogólne problemy z produktem (rejestrowanie wysokiej szczegółowości)	– Odtwórz ogólny zgłoszony problem z pełnym rejestrowaniem

Rodzaje problemów dla Serwerów Bezpieczeństwa:

Rodzaj zagadnienia	Przypadek użycia
Antymalware (skanowanie Dostępowe i Na żądanie)	Jakiekolwiek nieoczekiwanie zachowanie Serwera Bezpieczeństwa wliczając: – Wirtualne maszyny nie są poprawnie chronione – Skanowanie antymalware kończy się niepowodzeniem lub zajmuje dłużej niż powinno – Aktualizacje produktów nie są poprawnie zainstalowane – Ogólny Serwer Bezpieczeństwa działa nieprawidłowo (nie działają daemony bd)
Komunikacja z GravityZone Control Center	Jakiekolwiek nieoczekiwane zachowanie obserwowane z konsoli GravityZone: – Wirtualne maszyny nie są poprawnie raportowane w konsoli GravityZone – Problemy polityk (polityka nie jest zastosowana) – Serwer Bezpieczeństwa nie może połączyć się z konsolą GravityZone **Notatka** Użyj tej metody na polecenie Biznesowego Wsparcia Bitdefender.

3. Dla **Czas trwania sesji debugowania** wybierz przedział czasu, po którym sesja debugowania automatycznie się zakończy.

   Notatka
   Zaleca się ręczne zatrzymanie sesji za pomocą opcji **Zakończ sesję**,zaraz po odtworzeniu problemu.

4. W sekcji **Przechowywanie Logów**, wybierz lokalizację magazynu:

- **Docelowa maszyna**: archiwum logów zostanie zapisane w podanej lokalnej ścieżce Nie można skonfigurować tej ścieżki dla Serwerów Bezpieczeństwa.
- **Udział sieciowy**: Archiwum logów jest zapisywane w dostarczonej ścieżce z współdzielonej lokacji.

Możesz użyć opcji **Zapisz logi również na docelowej maszynie**, aby zapisać kopię archiwum logów w zagrożonym punkcie końcowym jako kopię zapasową.

5. Podaj niezbędne informacje (ścieżka lokalna, poświadczenia dla udziału sieciowego, ścieżka do udostępnionej lokalizacji) w zależności od wybranej lokalizacji.
6. Kliknij przycisk **Rozpocznij sesję**.

WAŻNE
Jednocześnie można uruchomić tylko jeden proces rozwiązywania problemów (**Zbierz logi Sesja debugowania** na zainfekowanej maszynie.

- **Historia rozwiązywania problemów**

Sekcja **Ostatnia aktywność** przedstawia czynności rozwiązywania problemów na danym komputerze. Siatka wyświetla tylko 10 ostatnich zdarzeń rozwiązywania problemów w odwrotnej kolejności chronologicznej i automatycznie usuwa aktywność starszą niż 30 dni.

Siatka wyświetla szczegóły każdego procesu rozwiązywania problemów.

Proces ma status główny i status pośredni. W zależności od dostosowanych ustawień możesz mieć następujący status, w którym musisz podjąć działania:

- **W toku (gotowe do odtworzenia problemu)** - uzyskaj dostęp do zainfekowanej maszyny ręcznie lub zdalnie i odtwórz problem.

Istnieje kilka opcji zatrzymania procesu rozwiązywania problemów:

- **Zakończ sesję**: kończy sesję debugowania i proces gromadzenia na wybranej maszynie, jednocześnie zapisując wszystkie zebrane dane w określonym miejscu przechowywania.

  Zaleca się użycie tej opcji zaraz po odtworzeniu problemu.
- **Anuluj**: ta opcja anuluje proces i żadne logi nie zostaną zebrane.

  Użyj tej opcji jeśli nie chcesz zebrać żadnych logów z docelowej maszyny.

– **Wymuś zatrzymanie**: wymusza zatrzymanie procesu rozwiązywania problemu.

  Użyj tej opcji jeśli anulowanie sesji trwa zbyt długo lub maszyna nie odpowiada i będziesz w stanie rozpocząć nową sesję za kilka minut.

Aby zrestartować proces rozwiązywania problemów:

– **Restart**: ten przycisk, skojarzony z każdym zdarzeniem i umiejscowiony pod **Działania** restartuje wybrany proces rozwiązywania problemów zachowując poprzednie ustawienia.

WAŻNE

– Aby upewnić się, że konsola wyświetla najnowsze informacje, użyj przycisku **Odśwież** w górnej części z prawej strony w zakładce **Rozwiązywanie problemów**.

– Aby uzyskać więcej informacji na temat określonego zdarzenia, kliknij nazwę zdarzenia z siatki.

6.2.3. Organizowanie Komputerów w Grupy

Możesz zarządzać grupami komputerów w lewym panelu strony **Siec**.

Główną zaletą tej funkcji jest to, że możesz korzystać z polityk grupy w celu spełnienia różnych wymogów bezpieczeństwa.

Komputery zaimportowane z Active Directory są grupowane w folderze **Active Directory**. Nie możesz edytować grup Active Directory. Można tylko przeglądać i zarządzać odpowiednimi komputerami.

Wszystkie komputery nie należące do Active Directory wykryte przez przeszukiwanie sieci są w **Niestandardowe Grupy**, gdzie możesz organizować je między grupami które chcesz. W **Niestandardowe Grupy** możesz utworzyć, usunąć, zmienić nazwę i przesunąć grupy komputerów w ramach zdefiniowanej niestandardowej struktury drzewa.

Notatka

- Grupa może zawierać zarówno komputery jak i inne grupy.
- Po wybraniu grupy z lewej strony panelu, możesz zobaczyć wszystkie komputery z wyjątkiem tych ulokowanych w podgrupach. Aby zobaczyć wszystkie komputery zawarte w grupie i jej podgrupie, klikamy menu **Filtry** zlokalizowane w górnej części tabeli i wybieramy **Wszystkie elementy rekurencyjne** w sekcji **Głębokość**.

Tworzenie grup

Przed rozpoczęciem tworzenia grup, pomyśl dlaczego ich potrzebujesz i wymyśl schemat grup. Dla przykładu, możesz grupować punkty końcowe bazujące na jednej lub na kombinacji następujących kryteriów:

- Struktura organizacyjna (Sprzedaż, Marketing, Zapewnienie Jakości, Rozwój Oprogramowania, Zarządzanie itp.).
- Potrzeby bezpieczeństwa (Komputery stacjonarne, Laptopy, Serwery, itd.).
- Lokalizacja (Siedziba Główna, Biura Lokalne, Pracownicy zdalni, Biura Domowe itp.).

Aby zorganizować swoją sieć w grupy:

1. Wybierz **Niestandardowe Grupy** w lewym panelu.
2. Kliknij przycisk ⊕ **Dodaj grupę** z górnej strony lewego panelu.
3. Podaj sugestywna nazwę dla grupy i naciśnij **OK**. Nowa grupa pojawi się w folderze **Niestandardowe Grupy**.

Zmienianie nazw grup

Aby zmienić nazwę grupy:

1. Wybierz grupę z lewego panelu bocznego.
2. Kliknij przycisk ✎ **Edytuj grupę** z górnej strony lewego panelu.
3. Wprowadź nową nazwę w odpowiednim polu.
4. Kliknij **OK**, aby potwierdzić.

Przenoszenie Grup i Komputerów

Możesz przenosić podmioty do **Grupy Niestandardowe** gdziekolwiek wewnątrz grupowej hierarchii. Aby przenieść podmioty, przeciągnij i upuść je z prawego panelu bocznego do pożądanej grupy lewego panelu.

Notatka

Przeniesiony podmiot odziedziczy ustawienia polityki nowej grupy macierzystej, chyba że inna polityka zostanie bezpośrednio do niej przypisana. Aby uzyskać więcej informacji o dziedziczeniu polityk, odwołaj się do „Polityki Bezpieczeństwa” (p. 218).

Usuwanie grup

Usunięcie grupy jest działaniem końcowym. W rezultacie, agent bezpieczeństwa zainstalowany na docelowym punkcie końcowym zostanie usunięty.

Aby usunąć grupę:

1. Wybierz pustą grupę w lewym bocznym panelu **Strona Sieci**.
2. Kliknij **Usuń grupę** przycisk z górnej strony lewego panela. Czynności należy potwierdzić, klikając **Tak**.

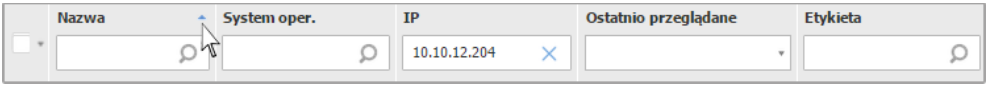
6.2.4. Sortowanie, filtrowanie i wyszukiwanie komputerów.

W zależności od liczby punktów końcowych, tabela z prawej strony może obejmować kilka strony (domyślnie tylko 20 wpisów jest wyświetlanych na tej stronie). Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

Jeżeli jest zbyt dużo wpisów, można użyć pól wyszukiwania pod nagłówkiem kolumny lub menu **Filtry** z górnej części strony aby wyświetlić tylko interesujące nas podmioty. Na przykład, możesz szukać konkretnego komputera lub chcesz zobaczyć tylko zarządzane komputery.

Sortowanie komputerów

Aby posortować dane według określonych kolumn, naciśnij na nagłówek kolumny. Przykładowo, jeśli chcesz posortować komputery według nazwy, kliknij nagłówek **Nazwa**. Po ponownym kliknięciu komputery zostaną posortowane w odwrotnej kolejności.

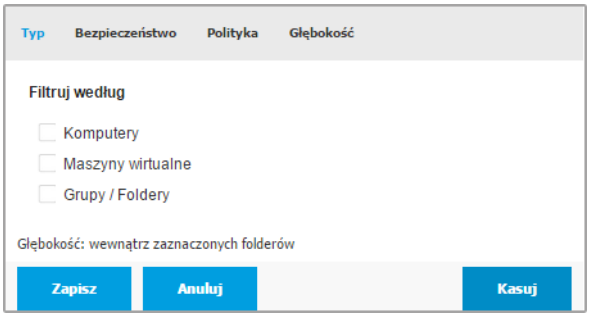


Sortowanie komputerów

Filtrowanie komputerów

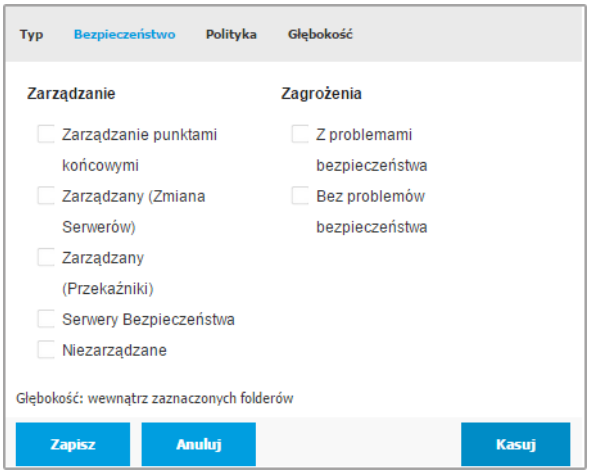
Aby filtrować swoje podmioty sieciowe, użyj menu **Filtry** z górnej strony panela sieci.

1. Wybierz pożądaną grupę z lewego panelu bocznego.
2. Kliknij menu **Filtry**z górnej bocznej strony obszaru panela sieciowego.
3. Wybierz kryteria filtrowania według:
   - **Typ**. Wybierz rodzaj wpisów jakie chcesz wyświetlić (komputery, maszyny wirtualne, foldery).



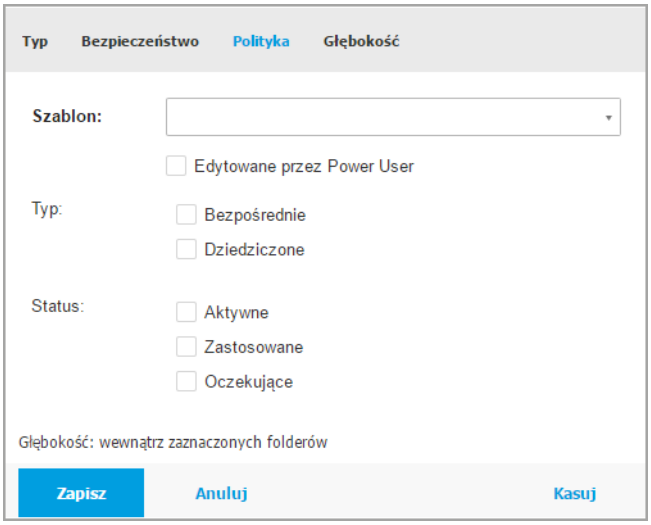
Komputery - Filtrowanie po Rodzaju

- **Bezpieczeństwo**. Wybierz wyświetlanie komputerów według zarządzania ochroną, statusu bezpieczeństwa bądź oczekujących aktywności.



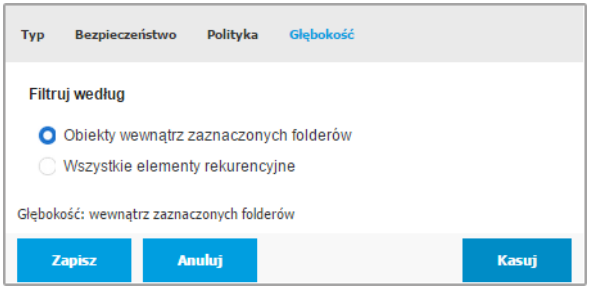
Komputery - Filtrowanie po Bezpieczeństwie

- **Polityka**. Wybierz szablon polityki jakim chcesz filtrować komputery, rodzaj przypisania polityki (bezpośrednia lub dziedziczona), status przypisanej polityki (aktywna, przypisana lub w toku). Możesz również wybrać wyświetlanie jedynie podmioty z politykami modyfikowanymi w trybie Power User.



Komputery - Filtrowanie po Polityce

- **Głębokość**. Kiedy zarządzamy siecią o strukturze drzewa, komputery umiejscowione w podgrupach nie są wyświetlane, gdy wybieramy grupy źródłowe. Wybierz **Wszystkie elementy rekurencyjne** aby zobaczyć wszystkie komputery zawarte w obecnej grupie i wszystkich jej podgrupach.



Komputery - Filtrowanie po Głębokości

Wybierając rekurencyjnie przeglądanie wszystkich elementów, Control Center wyświetla je w formie prostej listy. Aby znaleźć lokalizację elementu, wybierz element, który Cię interesuje, a następnie kliknij **Przejdź do kontenera** w

górnej części tabeli. Zostaniesz przekierowany do grupy nadrzędnej wybranego elementu.

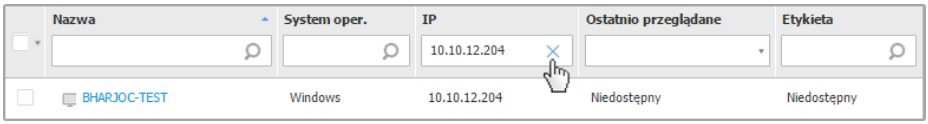
Notatka
Możesz zobaczyć wszystkie wybrane kryteria filtrów w dolnej części okna **Filtry**. Jeżeli chcesz wyczyścić wszystkie filtry, naciśnij przycisk **Reset**.

4. Naciśnij **Zapisz** aby odfiltrować komputery według wybranych kryteriów. Filtr pozostaje aktywny na stronie **Sieć** dopóki się nie wylogujesz lub nie zrestartujesz filtru.

Wyszukiwanie komputerów

1. Wybierz żądaną grupę w lewym panelu bocznym.
2. Podaj wyszukiwaną frazę w odpowiednim polu pod nagłówkami kolumny z prawego bocznego panelu. Na przykład,w polu **IP** podaj adres IP komputera, którego szukasz. Tylko pasujące komputery pokażą się w tabeli.

   Wyczyść pole wyszukiwania aby wyświetlić pełną listę komputerów.



Wyszukiwanie komputerów

6.2.5. Uruchamianie Zadań

Na stronie **Sieć**, możesz uruchomić zdalnie liczbę zadań administracyjnych na komputerach

Oto co możesz zrobić:

- „Skanowanie” (p. 71)
- „Zadania Uaktualnienia” (p. 81)
- „Skanowanie Exchange” (p. 84)
- „Zainstaluj” (p. 88)
- „Odinstaluj Klienta” (p. 95)
- „Aktualizacja klienta” (p. 96)
- „Rekonfiguruj Klienta” (p. 97)

- „Napraw Klienta” (p. 98)
- „Restartuj maszynę” (p. 99)
- „Przeszukiwanie sieci” (p. 100)
- „Wykrywanie Aplikacji” (p. 100)
- „Aktualizuj Security Server” (p. 101)
- „Wstaw Narzędzie Niestandardowe” (p. 102)

Możesz wybrać aby stworzyć indywidualne zadania dla każdego komputera lub dla grup komputerów. Na przykład, możesz zdalnie zainstalować agenta bezpieczeństwa na grupie niezarządzanych komputerów. W późniejszym czasie, możesz stworzyć zadanie skanowania dla określonego komputera z tej samej grupy.

Dla każdego komputera możesz rozpocząć kompatybilne zadania. Na przykład, jeżeli wybierzesz niezarządzany komputer, możesz jedynie dokonać wyboru instalacji agenta bezpieczeństwa, wszystkie pozostałe zadania będą nieaktywne.

Dla grupy, wybierane zadania będą stworzone tylko dla kompatybilnych komputerów. Jeżeli żaden komputer w grupie nie jest kompatybilny z wybranymi zadaniami, zostaniesz poinformowany, że zadanie nie może zostać utworzone.

Po utworzeniu, zadanie uruchamia się natychmiast na komputerach będących online. Jeżeli komputer jest offline, zadanie rozpocznie się zaraz po podłączeniu online.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

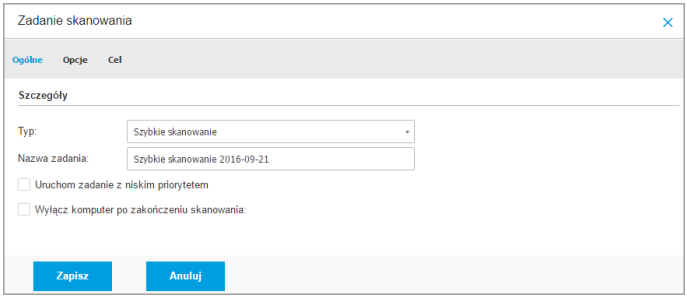
Skanowanie

Aby uruchomić zadanie skanowania na kilku komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz pola wyboru komputerów lub grup, które chcesz przeskanować.
5. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Skanowanie**.

   Wyświetlone zostanie okno konfiguracji.
6. Skonfiguruj opcje skanowania:

- W zakładce **Ogólne** możesz wybrać rodzaj skanowania i podać nazwę zadania skanowania. Zadanie skanowania ma pomóc Ci zidentyfikować aktualne skanowanie na stronie **Zadania**.



Zadanie skanowania komputerów - Konfigurowanie ustawień ogólnych

Wybierz rodzaj skanowania z menu **Rodzaj**:

– **Szybkie skanowanie** Do wykrywania w systemie złośliwego oprogramowania Szybkie Skanowanie wykorzystuje skanowanie w chmurze. Ten typ skanowania jest wstępnie skonfigurowany aby pozwolić na skanowanie tylko krytycznych lokalizacji systemów Windows i Linux. Wykonanie szybkiego skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.

  Kiedy zostaje wykryte złośliwe oprogramowanie lub rootkity, Bitdefender automatycznie przeprowadza dezynfekcję. Jeśli z jakiegokolwiek powodu plik nie może zostać zdezynfekowany, zostaje przeniesiony do kwarantanny. Ten typ skanowania ignoruje podejrzane pliki.

– **Pełne Skanowanie**sprawdza cały system w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu, takiego jak wirusy, oprogramowanie typu spyware/adware, rootkity i inne.

  Bitdefender automatycznie próbuje zdezynfekować wykryte pliki zawierające złośliwe oprogramowanie. W przypadku, gdy nie można usunąć złośliwego oprogramowania, znajduje się ono w kwarantannie, gdzie nie może wyrządzić żadnej szkody. Podejrzane pliki są ignorowane. Jeśli chcesz podjąć działania dotyczące podejrzanych plików lub inne

domyślne akcje zainfekowanych plików, wybierz opcję uruchomienia skanowania niestandardowego.

– **Skanowanie Pamięci** sprawdza programy działające w pamięci komputera.

– **Skanowanie Sieci** jest typem niestandardowego skanowania, pozwalającego na skanowanie dysków sieciowych wykorzystywanych przez zainstalowanego agenta bezpieczeństwa Bitdefender na docelowym punkcie końcowym.

  W celu uruchomienia zadania skanowania sieciowego:

  - Musisz przypisać zadanie do jednego pojedynczego punktu końcowego w swojej sieci.
  - Musisz wprowadzić listy uwierzytelniające dla użytkowników kont z prawem odczytu/zapisu na docelowym dysku sieciowym, dla umożliwienia agentowi bezpieczeństwa dostanie się i podejmowanie czynności na tych dyskach sieciowych. Wymagane poświadczenia mogą być skonfigurowane w zakładce **Cel** nowego okna zadania.

– **Niestandardowe skanowanie**dopuszcza wybranie lokacji, które mają zostać przeskanowane i skonfigurować opcje skanowania.

Dla pamięci, sieci i niestandardowych skanów, masz następujące opcje:

– **Uruchom zadanie z niskim priorytetem**. Wybierz ten checkbox aby zmniejszyć priorytet procesu skanowania i pozwolić innym programom działać szybciej. Zwiększy to czas potrzebny na zakończenie skanowania.

> **Notatka**
> Ta opcja dotyczy tylko Bitdefender Endpoint Security Tools i Endpoint Security (agent legacy).

– **Wyłącz komputer po zakończeniu skanowania**. Wybierz ten checkbox, aby wyłaczyć twoją maszynę, jeśli nie zamierzasz z niej korzystać przez jakiś czas.

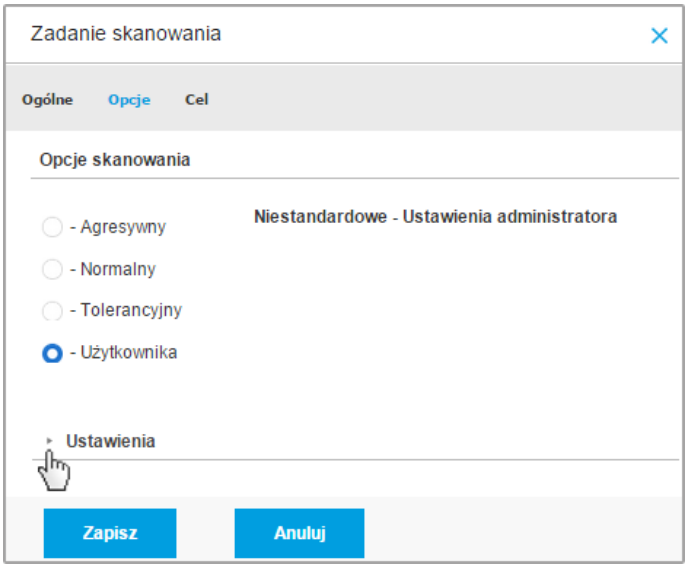
> **Notatka**
> Ta opcja dotyczy Bitdefender Endpoint Security Tools, Endpoint Security (agent legacy) i Endpoint Security for Mac.

Notatka
Te dwie opcje stosuje się tylko do Bitdefender Endpoint Security Tools i Endpoint Security (legacy agent).

Dla niestandardowego skanowania, skonfiguruj następujące ustawienia:

– Przejdź do zakładki **Opcje** aby ustawić opcje skanowania. Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

  Bazując na wybranym profilu, opcje skanowania w sekcji **Ustawienia** zostaną automatycznie skonfigurowane. Jednak, jeżeli chcesz, możesz skonfigurować je szczegółowo. Aby to zrobić, zaznacz pole wyboru **Niestandardowe** po czym rozwiń sekcję **Ustawienia**.



Zadanie Skanowania Komputerów - Konfiguracja Niestandardowego Skanowania

Dostępne są następujące opcje:

- **Typy plików.** Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Możesz ustawić agenta bezpieczeństwa tak by skanował wszystkie pliki (niezależnie od rozszerzenia pliku), tylko pliki aplikacji

lub określone rozszerzenia plików, które uważasz za potencjalnie niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.

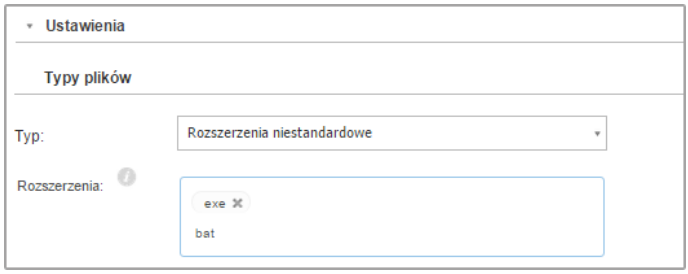
Notatka

Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji" (p. 516).

Jeżeli chcesz aby tylko określone rozszerzenia zostały przeskanowane, wybierz **Niestandardowe rozszerzenia** z menu wtedy podaj rozszerzenia w polu edycji, naciskając `Enter` po każdym rozszerzeniu.

WAŻNE

Agenty bezpieczeństwa Bitdefender zainstalowane na systemie operacyjnym Windows i Linux, skanują większość formatów .ISO, ale nie podejmują żadnych działań na nich.



Opcje zadania skanowania komputerów - Dodawanie niestandardowych rozszerzeń

- **Archiwa.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym. Jakkolwiek, zaleca się skanować archiwa w celu wykrycia i usunięcia potencjalnych zagrożeń, nawet jeśli nie są to zagrożenia bezpośrednie.

WAŻNE
Skanowanie zarchiwizowanych plików wydłuża ogólny czas skanowania i wymaga więcej zasobów systemowych.

– **Skanowanie wewnątrz archiwów.** Wybierz tę opcję tylko jeżeli chcesz sprawdzać pliki archiwów w poszukiwaniu malware. Jeżeli zdecydowałeś aby używać tej opcji, możesz skonfigurować poniższe opcje optymalizacji:

  • **Ogranicz rozmiar archiwum do (MB).** Możesz ustawić maksymalną akceptowalną wielkość archiwum do skanowania. Zaznacz odpowiadające pole wyboru i wpisz maksymalny rozmiar archiwum (w MB).

  • **Maksymalna głębokość archiwum (poziomy).** Zaznacz odpowiednie pole i wybierz maksymalną głębokość archiwum z menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.

– **Skanowanie archiwum e-mail.** Zaznacz tę opcję jeżeli chcesz włączyć skanowanie plików wiadomości e-mail i bazy e-mail, włączając formaty takie jak .eml, .msg, .pst, .dbx, .mbx, .tbb i inne.

WAŻNE
Skanowanie archiwum e-mail zużywa wiele zasobów i może mieć wpływ na wydajność systemu.

• **Inne.** Zaznacz odpowiednie pola, aby włączyć żądane opcje skanowania.

– **Skanowanie sektorów startowych.** Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu rozruchu. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.

– **Skanowanie rejestru.** Włącz tę opcję, aby skanować klucze rejestru. Rejestr systemu Windows jest bazą danych przechowującą ustawienia konfiguracji i opcje dla komponentów systemu operacyjnego Windows oraz dla zainstalowanych aplikacji.

- **Skanowanie w poszukiwaniu rootkitów.** Zaznacz tę opcję, aby skanować w poszukiwaniu rootkitów i ukrytych obiektów, które korzystają z tego rodzaju oprogramowania.
- **Skanuj w poszukiwaniu keyloggerów.** Zaznacz opcje skanowania dla oprogramowania keylogger.
- **Skanuj zasoby sieciowe.** Ta opcja skanuje zamontowane dyski sieciowe.

  Dla szybkiego skanowania, ta opcja jest domyślnie dezaktywowana. Dla pełnego skanowania, to jest domyślnie aktywowane. Dla skanowania niestandardowego, jeśli ustawisz poziom ochrony na **Agresywny/Normalny** opcja **Skanuj zasoby sieciowe** będzie automatycznie dostępna. Jeśli ustawisz poziom ochrony na **Tolerancyjny**, opcja **Skanuj zasoby sieciowe** będzie automatycznie wyłączona.
- **Skanowanie pamięci.** Wybierz tę opcję, aby przeskanować programy działające w pamięci systemu.
- **Skanowanie ciasteczek.** Wybierz tę opcję, aby przeskanować ciasteczka zapisane w przeglądarce.
- **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Potencjalnie nie chciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-suppored). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.
- **Skanowanie wymiennych woluminów.** Wybierz tę opcję aby przeskanować wymienne dyski i nośniki podłączone do komputera.

- **Akcje.** W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:
  - **Gdy zostanie wykryty zainfekowany plik.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI). Agent bezpieczeństwa Bitdefender może normalnie usunąć złośliwy kod z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

    Domyślnie, jeśli zainfekowany plik jest wykryty, agent ochrony Bitdefender automatycznie spróbuje go wyleczyć. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.

    WAŻNE
    W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

  - **Przy wykryciu podejrzanego pliku .** Pliki są wykryte jako podejrzane przez analizę heurystyczną i inne technologie Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

    Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny. Pliki kwarantanny są wysyłane do analizy do Laboratorium Bitdefender w regularnych odstępach czasu. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

  - **Gdy zostanie wykryty rootkit.** Rootkity stanowią specjalistyczne oprogramowanie wykorzystywane do ukrywania plików systemowych. Rootkity choć są nieszkodliwe, często są używane do ukrywania złośliwego oprogramowania lub intruza w systemie.

Wykrywanie rootkitów i ukrywanie plików jest domyślnie ignorowane.

Choć nie jest to polecane, możesz zmienić domyślne działania. Można tu wybrać osobną czynność dla każdej kategorii, a także określić drugą czynność, jaka ma zostać podjęta, jeśli pierwsza nie przyniesie skutku. Wybierz z odpowiedniego menu pierwszą i drugą czynność, jaka ma zostać zastosowana do każdego z wykrytych plików. Dostępne są następujące działania:

Dezynfekuj
Usuń złośliwy kod z zainfekowanych plików. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach.

Przenieś pliki do kwarantanny
Przenieś wykrytych plików z ich obecnego miejsca położenia do folderu kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami kwarantanny ze strony Kwarantanna w konsoli.

Usuń
Usuwa wykryte pliki z dysku, bez żadnego ostrzeżenia. Wskazane jest, aby unikać tego działania.

Ignoruj
Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania.

– Przejdź do zakładki **Cel** aby skonfigurować lokalizacje którą chcesz przeskanować na docelowych komputerach.

W sekcji **Cel skanowania** możesz dodać nowy filtr lub folder do przeskanowania:

a. Wybierz wcześniej zdefiniowaną lokalizacje z rozwijanego menu lub wprowadź **Określoną ścieżkę**, którą chciałbyś przeskanować.

b. W polu edycji określ ścieżkę do obiektów, które mają zostać przeskanowane.

- Jeżeli wybrałeś wcześniej zdefiniowana lokalizację, wypełnij ścieżkę jeśli potrzebujesz. Na przykład, aby przeskanować folder

`Program Files` wystarczy wybrać odpowiednią ścieżkę z rozwijanego menu. Aby przeskanować konkretny folder z `Program Files`, musisz uzupełnić ścieżkę dodając backslash (\) i nazwę folderu.

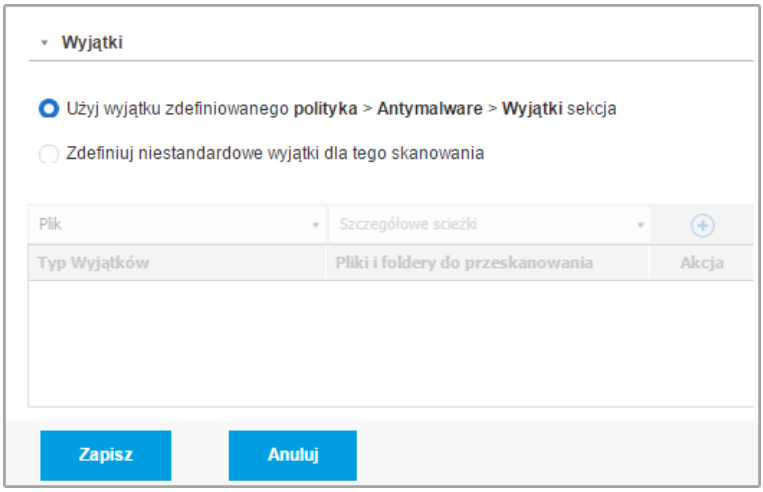
- Jeżeli wybrałeś **Określona ścieżka**, podaj pełną ścieżkę do obiektu, który chcesz przeskanować. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych. Aby uzyskać więcej informacji dotyczących zmiennych systemowych, zapoznaj się z „Zmienne systemowe” (p. 517).

c. Naciśnij przycisk ⊕ **Dodaj**.

Aby edytować istniejącą lokalizację, kliknij ją. Aby usunąć lokalizację z listy, kliknij odpowiedni przycisk ⊗ **Usuń**.

W celu wykonania zadania skanowania sieciowego, musisz wprowadzić listy uwierzytelniające dla kont użytkowników posiadających prawo odczytu/zapisu na docelowych dyskach sieciowych, dla umożliwienia agentowi bezpieczeństwa dostęp i podejmowanie czynności na dyskach sieciowych.

Kliknij sekcję **Wykluczenia** , jeśli chcesz zdefiniować wykluczenia celu.



Zadanie skanowania komputerów - Definiowanie wyjątków.

Możesz korzystać z wykluczeń określonych przez politykę lub określić wyraźne wykluczenia dla bieżącego zadania skanowania. Aby uzyskać więcej informacji dotyczących wykluczeń, odwołaj się do „Wykluczenia" (p. 287).

7. Kliknij **Zapisz**, aby utworzyć zadanie skanowania. Pojawi się nowa wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Notatka
Aby zaplanować zadanie skanowania, idź do strony **Polityki**,wybierz politykę, do której przypisane są komputery, którymi jesteś zainteresowany i dodaj zadanie skanowania w sekcji **Antymalware >Na żądanie** Aby uzyskać więcej informacji, zapoznaj się z „Na żądanie" (p. 267).

Zadania Uaktualnienia

Zaleca się regularne sprawdzanie aktualizacji oprogramowania i stosowanie ich tak szybko, jak to możliwe. GravityZone automatyzuje ten proces za pomocą polityk bezpieczeństwa, ale jeśli potrzebujesz od razu zaktualizować oprogramowanie niektórych punktów końcowych, uruchom zadania w następującej kolejności:

1. Skanowanie Uaktualnień
2. Instalacja aktualizacji

Warunki wstępne

- Agent bezpieczeństwa z modułem Zarządzania Aktualizacjami jest zainstalowany na docelowych punktach końcowych.
- Aby zadania skanowania i instalacji zakończyły się powodzeniem, punkty końcowe systemu Windows muszą spełniać następujące warunki:
  - **Zaufane Główne Urzędy Certyfikacji** przechowuje certyfikat **DigiCert Assured ID Root CA**.
  - **Pośrednie Urzędy Certyfikujące** obejmują **DigiCert SHA2 Assured ID Code Signing CA**.
  - Na punktach końcowych zainstalowane są aktualizacje dla Windows i Windows Server 2008 R2 wspomniane w tym artykule: Microsoft Security Advisory 3033929

Skanowanie Uaktualnień

Punkty końcowe z nieaktualnym oprogramowaniem są podatne na ataki. Zaleca się regularne sprawdzanie oprogramowania zainstalowanego na punktach końcowych i aktualizowanie go tak szybko, jak to możliwe. Aby zeskanować swoje punkty końcowe pod kątem brakujących aktualizacji:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Wybierz docelowe punkty końcowe.
5. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Skanowanie Aktualizacji**. Pojawi się nowe okno potwierdzające.
6. Kliknij **Tak**, aby potwierdzić zadanie skanowania.

   Kiedy zadanie się zakończy, GravityZone dodaje do Zasobów Aktualizacji wszystkie aktualizacje, których potrzebuje twoje oprogramowanie. Aby uzyskać więcej informacji, odwołaj się do „Inwentarz Aktualizacji” (p. 197).

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Notatka
Aby zaplanować skanowanie aktualizacji, edytuj polityki przypisane do docelowych punktów końcowych i skonfiguruj ustawienia w sekcji **Zarządzanie Aktualizacjami**. Aby uzyskać więcej informacji, zapoznaj się z „Zarządzanie Aktualizacjami" (p. 334).

Instalacja aktualizacji

Aby zainstalować jedno lub więcej aktualizacji na docelowych punktach końcowych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Instalacja Aktualizacji**.

   Wyświetlone zostanie okno konfiguracji. Tutaj możesz zobaczyć wszystkie aktualizacje, których brakuje w docelowych punktach końcowych.
5. W razie potrzeby użyj opcji sortowania i filtrowania w górnej części tabeli, aby znaleźć określone aktualizacje.
6. Kliknij przycisk **Kolumny** po prawej stronie panelu, aby zobaczyć dodatkowe informacje.
7. Wybierz aktualizacje, które chcesz zainstalować.

   Niektóre aktualizacje są zależne od innych, W takim przypadku są one automatycznie wybierane jeśli mają aktualizaje.

   Klikając na **CVEs** lub **Products** wyświetli się panel po lewej stronie. Panel zawiera dodatkowe informacje, takie jak CVE, które rozwiązuje aktualizacja, lub produkty, których dotyczy aktualizacja. Po zakończeniu czytania kliknij **Zamknij**, aby ukryć panel.
8. Wybierz opcję **Uruchom ponownie punkty końcowe po zainstalowaniu aktualizacji, jeśli jest to wymagane**, aby ponownie uruchomić punkty końcowe natychmiast po instalacji aktualizacji, jeśli wymagane jest ponowne uruchomienie systemu. Weź pod uwagę, że to działanie może zakłócić aktywność użytkownika.

9. Kliknąć **Instaluj**.

   Zadanie instalacji jest tworzone wraz z pod-zadaniami dla każdego docelowego punktu końcowego.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Notatka

- Aby zaplanować wdrożenie aktualizacji, zmodyfikuj polityki przypisane do docelowych punktów końcowych i skonfiguruj ustawienia w sekcji **Zarządzanie Aktualizajami**. Aby uzyskać więcej informacji, zapoznaj się z „Zarządzanie Aktualizacjami" (p. 334).
- Możesz również zainstalować aktualizację ze strony **Inwentarz Aktualizacji**, zaczynając od aktualizacji, którą jesteś zainteresowany. W takim przypadku wybierz aktualizację z listy, kliknij przycisk **Zainstaluj** w górnej części tabeli i skonfiguruj szczegóły instalacji aktualizacji. Szczegółowe informacje znajdują się w „Instalowanie Aktualizacji" (p. 201).
- Po zainstalowaniu aktualizacji zalecamy wysłanie zadania Skanowanie Aktualizacji w celu dotarcia do punktów końcowych. Ta czynność uaktualni informacje o aktualizacji zapisane w GravityZone dla zarządzanych sieci.

Możesz odinstalować aktualizacje:

- Zdalnie, wysyłając zadanie odinstalowania aktualizacji z GravityZone.
- Lokalnie w punkcie końcowym. W takim przypadku musisz zalogować się jako administrator do punktu końcowego i ręcznie uruchomić dezinstalator.

Skanowanie Exchange

Możesz zdalnie skanować bazy danych Serwera Exchange poprzez uruchomienie zadania **Skanowanie Exchange**.

Aby być w stanie przeskanować bazę danych Exchange, musisz włączyć skanowanie na żądanie poprzez dostarcze uwierzytelnienia administratora Exchange. Aby uzyskać więcej informacji, odwołaj się do „Skanowanie Exchange Store" (p. 359).

Aby przeskanować bazę danych Serwera Exchange:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.

3. Z panela po lewej stronie, wybierz grupę zawierającą docelowy Serwer Exchange. Możesz odnaleźć serwer wyświetlony w panelu po prawej stronie.

   Notatka
   Optymalnie możesz zastosować filtry szybkiego odnajdywania docelowych serwerów:
   - Kliknij menu **Filtry** aby wybrać następujące opcje: **Zarządzane (Serwery Exchange)** z zakładki **Bezpieczeństwo** i **Wszystkie elementy rekurencyjne** z zakładki **Głębokość**.
   - Wprowadź nazwę hosta serwera lub adres IP w polach odpowiedniego nagłówka kolumny.

4. Wybierz pole wyboru Serwera Exchange którego bazę danych chcesz przeskanować.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Skanowanie Exchange**. Wyświetlone zostanie okno konfiguracji.
6. Skonfiguruj opcje skanowania:
   - **Ogólne.** Wprowadź sugestywną nazwę dla zadania.

     W przypadku dużych baz danych, zadanie skanowania może zająć dużo czasu i może mieć wpływ na wydajność serwera. W takich wypadkach, pole wyboru **Zatrzymaj skanowanie jeżeli zajmie to więcej niż** i wybierz dogodny przedział czasowy odpowiedniego menu.
   - **Cel.** Wybierz kontener i obiekty do skanowania. Możesz wybrać by skanowanie skrzynek pocztowych, publicznych folderów lub obu. Oprócz wiadomości e-mail, możesz skanować inne obiekty takie jak **Kontakty**, **Zadania**, **Spotkania** oraz **Elementy pocztowe**. Możesz ponadto ustawić następujące ograniczenia odnoszące się do skanowanej treści:
     – Tylko nieprzeczytane wiadomości
     – Tylko elementy z załącznikami
     – Tylko nowe pozycje, otrzymały określony przedział czasowy.

     Dla przykładu, możesz wybrać skanowanie tylko e-maili ze skrzyynek pocztowych użytkowników, które otrzymali w ciągu ostatnich siedmiu dni.

     Zaznacz pole wyboru **Wykluczenia**, jeżeli chcesz zdefiniować skanowanie wyjątków. Aby utworzyć wyjątek, użyj pól z nagłówka tabeli w następujący sposób:
     a. Wybierz typ repozytorium z menu.
     b. Zależnie od rodzaju magazynu, określ obiekt jaki ma być wykluczony:

Typ repozytorium	Format obiektu
Skrzynka pocztowa	Adres e-mail
Folder publiczny	Ścieżka folderu, zaczynająca się od źródła
Baza danych	Tożsamość bazy danych

Notatka
By posiąść tożsamość bazy danych użyj polecenia shell Exchange:
`Get-MailboxDatabase | fl name,identity`

Możesz dodać tylko jedną pozycję naraz. Jeżeli posiadasz kilka pozycji tego samego typu, musisz zdefiniować tyle zasad ile posiadasz pozycji.

c. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli by zapisać wyjątek i dodać go do listy.

Aby usunąć zasadę wyjątku z listy, kliknij odpowiadający mu przycisk ⊖ **Usuń**.

- **Opcje.** Skonfiguruj ustawienia skanowania dla wiadomości mailowych odpowiadającym zasadom:
  - **Przeskanowane typy plików.** Użyj tej opcji aby sprecyzować które typy plików chcesz przeskanować. Możesz ustalić skanowanie wszystkich plików (bez względu na ich rozszerzenie), samych plików aplikacji, lub określonego rozszerzenia, które uważasz za potencjalnie niebezpieczne. Skanowanie wszystkich plików zapewnia najlepszą ochronę, podczas gdy skanowanie jedynie aplikacji jest zalecane dla szybszego skanowania.

    Notatka
    Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji” (p. 516).

    Jeżeli chcesz skanować tylko pliki o konkretnym rozszerzeniu, masz dwie alternatywy:
    - **Zadeklarowane rozszerzenia użytkownika**, tutaj musisz wprowadzić rozszerzenia które mają być skanowane.
    - **Wszystkie pliki za wyjątkiem określonych rozszerzeń** tutaj należy podać rozszerzenia które mają zostać pominięte podczas skanowania.

- **Maksymalnym rozmiar załącznika / maila (MB).** zaznacz to pole wyboru i wprowadź wartość w odpowiednim polu aby ustawić maksymalny dopuszczalny rozmiar pliku załącznika lub długości treści maila, który ma być poddawany skanowaniu.
- **Maksymalna głębokość archiwum (poziomy).** Zaznacz pole wyboru i podaj maksymalną głębokość archiwum w odpowiednim polu. Im niższy poziom głębokości, tym większa wydajność i niższy stopień ochrony.
- **Sanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Zaznacz to pole wyboru by skanować w poszukiwaniu złośliwych i niechcianych aplikacji takich jak adware, który może instalować bez wiedzy użytkownika inne oprogramowanie,zmieniać działanie oprogramowania i obniżać wydajność systemu.

- **Akcje.** Możesz określić różne działania dla agenta bezpieczeństwa, aby je automatycznie podjął na plikach, w zależności od rodzaju detekcji.

  Rodzaj detekcji dzieli pliki na trzy kategorie:
  - **Pliki zainfekowane.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI).
  - **Podejrzane pliki.** Te pliki są wykryte jako podejrzane przez analizę heurystyczną i inne techonogię Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach.
  - **Nieskanowalne pliki.** Te pliki nie mogą być przeskanowane. Nieskanowalne pliki obejmują, ale nie ograniczają się do chronionych hasłem, zaszyfrowanych lub nadmiernie skompresowanych plików.

  Dla każdego rodzaju wykrycia, posiadasz domyślne lub główne działania oraz alternatywne działanie w przypadku awarii jednego z powyższych. Choć nie jest to zalecane, można zmienić ustawienia akcji w odpowiednim menu. Wybierz reakcję, która ma być podjęta:
  - **Dezynfekuj.** Usuwa złośliwy kod z zainfekowanego pliku i odbudowuje oryginalny plik. W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.
  - **Odrzuć / Usuń email.** Na serwerze z rolą Edge Transport, wykryty email jest odrzucany wraz z kodem błedu 550 SMTP. W każdym innym

przypadku, wiadomość email jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Skasuj plik.** Kasuje załączniki w których wystąpiło zdarzenie bez wcześniejszego ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Plik zastępczy.** W miejsce skasowanego pliku umieszczany jest plik tekstowy który powiadamia użytkownika o podjętej czynności.
- **Przenieś plik do kwarantanny.** Przenosi wykryty plik do katalogu kwarantanny i umieszcza plik tekstowy który informuje użytkownika o podjętej czynności. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami w kwarantannie ze strony **Kwarantanna**

> **Notatka**
> Miej na uwadze, że kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni na partycji dysku twardego gdzie zainstalowano agenta. Rozmiar kwarantanny zależy od liczby elementów przechowywanych oraz ich wielkości.

- **Nie podejmuj działania.** Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania. Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny.
- Domyślnie, gdy email pasuje do zakresu reguł, jest przetwarzany wyłącznie ze zgodnymi zasadami, bez sprawdzania pod kątem wszelkich innych zasad. Jeśli chcesz kontynuować sprawdzanie pod kątem innych zasad, wyczyść pole wyboru **Jeżeli warunki reguł są dopasowane, wstrzymaj przetwarzanie kolejnych reguł**.

7. Kliknij **Zapisz**, aby utworzyć zadanie skanowania. Pojawi się nowa wiadomość potwierdzająca.
8. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Zainstaluj

By chronić swoje komputery przy pomocy agenta bezpieczeństwa Bitdefender, musisz zainstalować go na każdym z nich.

WAŻNE

W izolowanych sieciach, które nie mają bezpośredniej łączności z urządzeniem GravityZone, możesz zainstalować agenta bezpieczeństwa z rolą Relay. W tym wypadku, komunikacja pomiędzy urządzeniem GravityZone a pozostałymi agentami bezpieczeństwa będzie wykonywane poprzez agenta Relay, który będzie również pełnił rolę lokalnego serwera aktualizacji dla agentów bezpieczeństwa chroniących izolowane środowisko.
Zaraz po zainstalowaniu agenta Relay, automatycznie wykryje on niechronione komputery w tej samej sieci.

Notatka

- Zalecana się, by komputery na których instaluje się agentów Relay były zawsze włączone.
- Jeżeli żaden agent Relay nie został zainstalowany w sieci, wykrycie niechronionych komputerów może zostać wykonane ręcznie poprzez wysyłanie zadania **Network Discovery** do chronionych stacji końcowych.

Ochrona Bitdefender może zostać zainstalowana na komputerach zdalnie z poziomu Control Center.

Zdalna instalacja jest wykonywana w tle, bez wiedzy użytkownika.

Ostrzeżenie

Przed instalacją, należy odinstalować istniejące oprogramowanie antymalware i zapory sieciowej z komputerów. Instalując ochronę Bitdefender na istniejące oprogramowanie bezpieczeństwa możemy wpłynąć na jego działanie i spowodować poważne problemy z pracą systemu. Windows Defender i Windows Firewall zostaną automatycznie wyłączone, gdy rozpocznie się instalacja.

Jeśli chcesz zainstalować agenta bezpieczeństwa na komputerze z programem Bitdefender Antivirus for Mac 5.X, musisz go najpierw usunąć ręcznie. Szczegółowe instrukcje można znaleźć w tym artykule KB.
Podczas wdrażania agenta za pośrednictwem Linux Relay muszą być spełnione następujące warunki:

- Punkt końcowy Relay musi mieć zainstalowany pakiet Samba (`smbclient`) w wersji 4.1.0 lub nowszy i binarny/ wiersz poleceń `net` do wdrażania agentów Windows.

  Notatka

  Polecenie binarne/ `net` jest zwykle dostarczane razem z pakietami samba-client i/lub samba-common. W niektórych dystrybucjach Linuxa

(takich jak CentOS 7.4) polecenie `net` jest instalowane tylko podczas instalowania pełnego pakietu Samba (Common + Client + Server) Upewnij się, że Twój punkt końcowy Relay ma dostępne polecenie `net`.

- Docelowe punkty końcowe Windows muszą mieć włączone Zasoby Administracyjne i udostępnianie Sieciowe.
- Docelowe punkty końcowe Linux oraz Mac muszą mieć włączone SSH oraz wyłączony Firewall.

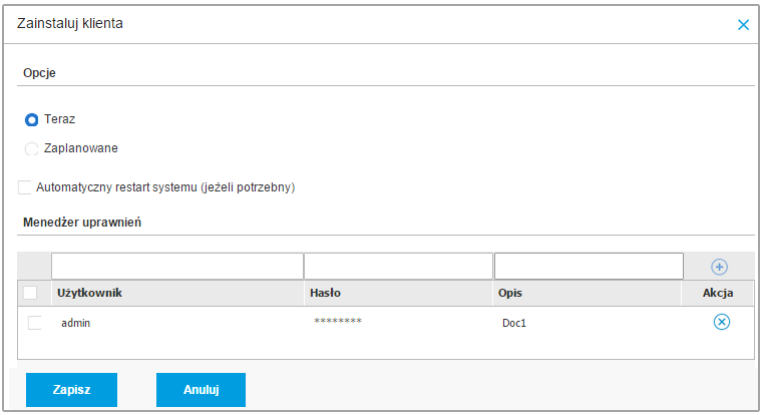
Aby uruchomić zdalną instalacje:

1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz **Komputery i Wirtualne Maszyny** z selektora widoku.
4. Wybierz żądaną grupę z lewego panelu bocznego. Jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.

   Notatka
   Opcjonalnie, możesz zastosować filtry, aby wyświetlić tylko punkty końcowe niezarządzane. Naciśnij menu **Filtry** i wybierz poniższe opcje: **Niezarządzane** z zakładki **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z zakładki **Głębokość**.

5. Wybierz wpisy (punkty końcowe lub grupy punktów końcowych), na których chcesz zainstalować ochronę.
6. Kliknij przycisk **Zadanie** z górnej strony tabeli i wybierz **Instaluj**.

   Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Bitdefender Endpoint Security Tools z menu zadań

7. W sekcji **Opcje** skonfiguruj czas instalacji:
   - **Teraz**, aby rozpocząć wdrożenie natychmiast.
   - **Zaplanowane**, aby ustawić przedział czasu na rozpoczęcie wdrożenia. W tym przypadku, wybierz przedział czasu jaki chcesz (godziny, dni lub tygodnie) i skonfiguruj go tak jak potrzebujesz.

     Notatka
     Na przykład, gdy określone operacje są wymagane na maszynach docelowych przed instalowaniem klienta (takie jak odinstalowanie innego oprogramowania albo ponowne uruchomienie systemu), możesz zaplanować zadanie wdrożenia aby uruchamiało się co 2 godziny. Zadanie rozpocznie się dla każdej maszyny docelowej w ciągu 2 godzin od udanego wdrożenia.

8. Jeśli chcesz, by docelowe punkty końcowe samoczynnie się uruchamiały, aby zakończyć instalację, wybierz **Automatyczny restart (w razie potrzeby)**.
9. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na docelowych punktach końcowych. Możesz dodać poświadczenia przez wpisanie użytkownika i hasła dla docelowego systemu operacyjnego.

WAŻNE
Dla Windows 8.1 musisz podać poświadczenia wbudowanego konta administratora lub konta administratora domeny. Aby nauczyć się więcej, odwołaj się do tego artykułu KB.

Aby dodać wymagane poświadczenia OS:

a. Wprowadź nazwę użytkownika i hasło konta administratora w odpowiednie pola z nagłówka tabeli.

   Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

   Użyj konwencji Windows podczas wprowadzania nazwy użytkownika konta

   - Dla maszyn Active Directory użyj tych składni: `username@domain.com` i `domain\username`. Aby upewnić się że wprowadzone poświadczenia będą działać, dodaj je w obu formach (`username@domain.com` i `domain\username`).
   - Dla maszyn z grupy roboczej, wystarczy wprowadzić tylko nazwę użytkownika, bez nazwy grupy roboczej.

   Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto.

b. Kliknij przycisk ⊕ **Dodaj** . Konto jest dodane do listy poświadczeń.

Notatka
Określone poświadczenia, zostaną automatycznie zapisane w Menadżer Poświadczeń tak, by nie trzeba było wprowadzać ich następnym razem. Aby uzyskać dostęp do Menedżera Poświadczeń wskaż tylko swoją nazwę użytkownika w prawym górnym rogu konsoli.

WAŻNE
Jeżeli dostarczone poświadczenia są nieważne, instalacja klienta nie powiedzie się na odpowiednich punktach końcowych. Upewnij się, że zaktualizowałeś wprowadzone poświadczenia OS w Menedżerze Poświadczeń, gdy są one zmieniane na docelowych punktach końcowych.

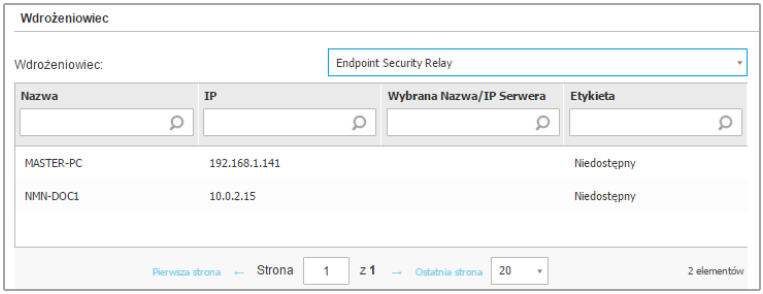
10. Zaznacz pola odpowiadające kontom, które chcesz używać.

Notatka
Ostrzeżenie jest wyświetlane tak długo jak nie wybierzesz żadnych poświadczeń. Ten krok jest obowiązkowy, aby zdalnie zainstalować agenta bezpieczeństwa na punktach końcowych.

11. W sekcji **Wdrożeniowiec**, wybierz podmiot, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:
    - **Urządzenie GravityZone**, gdy punkty końcowe łączą się bezpośrednio do Urządzenia GravityZone.

      W tym przypadku, możesz także zdefiniować:
      - Niestandardowy Communication Server wpisując jego adres IP lub nazwę hosta, jeśli jest to wymagane.
      - Ustawienia proxy, jeśli docelowy punkt końcowy komunikuje się z Urządzeniem GravityZone poprzez proxy. W tym przypadku, wybierz **Użyj proxy do komunikacji** i wprowadź wymagane ustawienia proxy w polach poniżej.
    - **Endpoint Security Relay**, jeśli chcesz połączyć punkty końcowe z zainstalowanym w Twojej sieci klientem Relay. Wszystkie maszyny z rolą Relay wykryte w Twojej sieci pokażą się w tabeli poniżej. Wybierz maszynę Relay. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego Relay.

      WAŻNE
      Port 7074 musi być otwarty dla wdrożenia poprzez agenta Relay aby mógł działać.



12. Użyj sekcji **Dodatkowe cele** jeśli chcesz wdrożyć klienta do konkretnych maszyn w sieci, które nie są widoczne w zasobach sieci. Rozwiń sekcję i podaj adres IP lub nazwy hostów tych maszyn w odpowiednich polach, oddzielone przecinkiem. Możesz dodać dowolną liczbę adresów IP.
13. Musisz wybrać jeden pakiet instalacyjny dla aktualnego wdrożenia. Kliknij listę **Użyj pakietu** i wybierz pakiet instalacyjny, który chcesz. Można tu znaleźć wszystkie pakiety instalacyjne wcześniej utworzone dla Twojego konta, a także domyślny pakiet instalacyjny dostępny z Control Center.
14. Jeśli to potrzebne, można zmienić niektóre ustawienia wybranego pakietu instalacyjnego, klikając przycisk **Dostosuj** obok pola **Użycie pakietu**.

    Ustawienia pakietu instalacyjnego pojawią się poniżej i możesz wprowadzić zmiany, które potrzebujesz. Aby dowiedzieć się więcej o edycji pakietów instalacyjnych, zapoznaj się z Instrukcją instalacji GravityZone.

    Jeśli chcesz zapisać zmiany jako nowy pakiet, wybierz opcję **Zapisz jako pakiet** umieszczoną na dole listy ustawień pakietów, a następnie wpisz nazwę dla nowego pakietu instalacyjnego.
15. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**.

WAŻNE

Jeśli korzystasz z VMware Horizon View Persona Management, zaleca się skonfigurowanie zasad grupy Active Directory w celu wykluczenia następujących procesów Bitdefender (bez pełnej ścieżki):

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

Wykluczenia te muszą obowiązywać, dopóki agent bezpieczeństwa działa na punkcie końcowym. Aby uzyskać szczegółowe informacje, zapoznaj się z tą stroną dokumentacji VMware Horizon.

Upgrade klienta

To zadanie jest dostępne tylko wtedy, gdy agent Endpoint Security jest zainstalowany i wykryty w sieci. Bitdefender zaleca uaktualnienie z Endpoint Security do nowego Bitdefender Endpoint Security Tools, w celu ochrony punktu końcowego ostatniej generacji.

Aby łatwo znaleźć klientów, którzy nie są uaktualnieni, możesz wygenerować raport o stanie aktualizacji. Aby uzyskać szczegółowe informacje na temat tworzenia raportów, patrz „Tworzenie raportów" (p. 435).

Odinstaluj Klienta

Aby zdalnie odinstalować ochronę Bitdefender:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz pola wyboru dla komputerów na których chcesz dokonać odinstalowania agentów bezpieczeństwa Bitdefender.
5. Kliknij przycisk **Zadania** z bocznej strony tabeli i wybierz **Odinstaluj klienta**.
6. Konfiguracja okna jest wyświetlana w celu umożliwienia ustawienia następujących opcji:
   - Możesz zdecydować się na przechowywanie elementów podlegających kwarantannie na komputerze klienta.
   - Dla środowisk integracji vShield, musisz wybrać wymagane poświadczenia dla każdej maszyny, w innym wypadku odinstalowanie nie powiedzie się. Wybierz **Użyj poświadczeń dla integracji vShield**, po czym sprawdź wszystkie właściwe poświadczenia w tabeli Menadżera Poświadczeń wyświetlonej poniżej.
7. Naciśnij **Zapisz** aby utworzyć zadanie. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Notatka
Jeżeli chcesz przeinstalować ochronę, upewnij się czy zrestartowałeś wcześniej komputer.

Aktualizacja klienta

Sprawdź status zarządzanych komputerów okresowo. Jeżeli zauważysz komputer z problemami bezpieczeństwa, należy kliknąć jego nazwę, aby wyświetlić stronę **Informacje**. Aby uzyskać więcej informacji, odwołaj się do „Stan bezpieczeństwa" (p. 49).

Nieaktualni klienci lub przestarzała zawartość zabezpieczeń stanowią problemy z bezpieczeństwem. W tym wypadku, musisz uruchomić aktualizację dla określonego komputera. To zadanie może zostać zrobione lokalnie z komputera lub zdanie z Control Center.

Aby zdalnie zaktualizować klienta i zawartość zabezpieczeń na zarządzanych komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz pola dla komputerów, na których chcesz uruchomić klienta aktualizacji.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Aktualizacja**. Wyświetlone zostanie okno konfiguracji.
6. Możesz wybrać aktualizację tylko produktu, tylko zawartości zabezpieczeń lub obu.
7. Dla systemu operacyjnego Linux i maszyn zintegrowanych z vShield, obowiązkowym jest wybranie odpowiednich poświadczeń. Zaznacz opcję **Użyj poświadczeń dla integracji Linux i vShield**, po czym wybierz właściwe poświadczenia z tabeli Menadżera Poświadczeń wyświetlonej poniżej.
8. Naciśnij **Aktualizuj** aby uruchomić zadanie. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Rekonfiguruj Klienta

Moduły ochrony agentów bezpieczeństwa, ich role i moduły skanowania są wstępnie skonfigurowane wewnątrz paczki instalacyjnej. Po zainstalowaniu agenta bezpieczeństwa w swojej sieci, można w każdym momencie zmienić wstępne ustawienia poprzez przesłanie zdalnego zadania **Przekonfiguruj Klienta** do pożądanego i zarządzanego punktu końcowego.

Ostrzeżenie
Należy pamiętać, że zadanie **Rekonfiguracji Klienta** nadpisuje wszystkie ustawienia instalacyjne, a żadne z początkowych ustawień nie zostaną zapisane. Podczas wykonywania zadania, upewnij się, że przekonfigurowałeś wszystkie ustawienia instalacyjne dla docelowego punktu końcowego.

Notatka
Zadanie **Ponownie Konfiguruj klienta** usunie wszystkie nieobsługiwane moduły z istniejących instalacji w starszym systemie Windows.

Możesz zmienić ustawienia instalacji z obszaru **Sieć** lub z raportu **Stan modułów punktu końcowego**.

By zmienić ustawienia instalacyjne dla jednego lub kilku komputerów:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz pola wyboru dla komputerów, którym chcesz zmienić ustawienia instalacyjne.
5. Kliknij przycisk **Zadania** w górnej części tabeli i wybierz **Rekonfiguracja klienta**.
6. Wybierz jedno z poniższych działań:
   - **Dodaj**. Dodaj nowe moduły oprócz istniejących.
   - **Usuń**. Usuń określone moduły z istniejących.
   - **Lista Zgodności**. Dopasuj zainstalowane moduły do wybranych opcji.
7. Wybierz moduły i role, które masz zamiar usunąć lub zainstalować na docelowych punktach końcowych.

Ostrzeżenie
Zainstalowane zostaną tylko wspierane moduły. Na przykład, Zapora Sieciowa instaluje się tylko na wspieranych stacjach roboczych z Windows.
Po więcej informacji, odnieś się do Dostępności warstw ochrony GravityZone.

8. Zaznacz **Usuń konkurencję, jeśli wymagane** aby upewnić się, że wybrane moduły nie będą kolidować z innymi rozwiązaniami bezpieczeństwa zainstalowanymi na docelowych punktach końcowych.
9. Wybierz jeden z dostępnych trybów skanowania:
   - **Automatyczne**. Agent bezpieczeństwa wykrywa, które silniki skanowania są odpowiednie dla zasobów punktów końcowych.
   - **Użytkownika**. Wyraźnie wybierasz jakich silników skanować użyć.

     Szczegółowe informacje na temat dostępnych opcji znajdują się w sekcji Tworzenie pakietów instalacyjnych w Instrukcji instalacji.

Notatka
Ta sekcja jest dostępna tylko z **Listą Zgodności**.

10. W sekcji **Harmonogram**, wybierz kiedy zadanie ma się uruchomić:
    - **Teraz**, aby uruchomić natychmiast.
    - **Zaplanowane**, aby ustawić częstotliwość powtórzeń zadania.

      W tym przypadku, wybierz przedział czasu jaki chcesz (co godzinę, codziennie lub cotygodniowo) i dostosuj go do swoich potrzeb.
11. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

    Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Napraw Klienta

Użyj zadania Naprawa Klienta jako zadanie do wstępnego rozwiązywania problemów dla dowolnej liczby problemów na punkcie końcowym. Zadanie pobiera ostatnie pakiety instalacyjne na wybranym punkcie końcowym i przeprowadza reinstalację agenta.

Notatka

- The modules currently configured on the agent will not be changed.
- Zadanie naprawy zresetuje agenta bezpieczeństwa do wersji opublikowanej w **Konfiguracja > Aktualizacja > Komponenty**.

Aby wysłać zadanie Naprawa Klienta do klienta:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz pola dla komputerów, na których chcesz uruchomić naprawę klienta.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Napraw Klienta**. Pojawi się nowe okno potwierdzające.
6. Zaznacz **Rozumiem i zgadzam się** i kliknij **Zapisz**, aby uruchomić zadanie.

   Notatka
   Aby zakończyć zadanie naprawy, może być wymagane ponowne uruchomienie klienta.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Restartuj maszynę

Możesz wybrać zdalne zarządzanie uruchamianiem komputerów.

Notatka
Sprawdź stronę **Sieć > Zadania** przed ponownym uruchomieniem niektórych komputerów. Wcześniej utworzone zadania mogą być jeszcze przetwarzane na komputerach docelowych.

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.

4. Zaznacz pola wyboru dla komputerów, które chcesz uruchomić ponownie.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Zrestartuj maszynę**.
6. Wybierz opcje harmonogramu restartu:
   - Zaznacz **Uruchom ponownie teraz** aby natychmiast uruchomić komputer ponownie.
   - Wybierz **Ponowne Uruchamianie włączone** i użyj pola poniżej do zaplanowania restartu komputera danego dnia o określonej porze.
7. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Przeszukiwanie sieci

Wyszukiwanie sieci jest wykonywane automatycznie za pośrednictwem agentów bezpieczeństwa z rolą Relay. Jeżeli nie posiadasz zainstalowanego agenta Relay w swojej sieci, możesz ręcznie przesłać zadanie network discovery z poziomu chronionego punktu końcowego.

Aby uruchomić zadanie wykrywania sieci:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz pola wyboru dla komputerów na których chcesz dokonać network discovery.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Network Discovery**.
6. Pojawi się nowa wiadomość potwierdzająca. Naciśnij **Tak**.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Wykrywanie Aplikacji

Aby wykryć aplikacje w twojej sieci:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz komputery na których chcesz wykonać wykrywanie aplikacji.
5. Kliknij przycisk **Zadania** na górnej stronie tabeli i wybierz **Wykrywanie Aplikacji**.

   Notatka
   Bitdefender Endpoint Security Tools musi być zainstalowany z Kontrolą Aplikacji i aktywowany na zaznaczonych komputerach. W innym przypadku, zadanie będzie wyszarzone. Kiedy wybrana grupa zawiera jednocześnie aktywne i nieaktywne cele, zadanie wyślę tylko do aktywnych punktów końcowych.

6. Kliknij **Tak** w oknie potwierdzenia, aby kontynuować.

Wykryte aplikacje i procesy są wyświetlone na stronie **Sieć > Magazyn Aplikacji**. Aby uzyskać więcej informacji, zapoznaj się z „Magazyn Aplikacji" (p. 192).

Notatka
Zadanie **Wykrywanie Aplikacji** może zająć chwilę, w zależności od ilości zainstalowanych aplikacji. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Aktualizuj Security Server

Zainstalowany Security Server może być przeglądany i zarządzany również z **Komputery i Maszyny Wirtualne** spod folderu **Niestandardowe Grupy**.

Jeżeli Security Server jest nieaktualny, możesz wysłać mu zadanie aktualizacji:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz grupę gdzie Security Server jest zainstalowany.

   Aby łatwo zlokalizować Security Server, możesz użyć menu **Filtry** według poniższych:

   - Przejdź do zakładki **Bezpieczeństwo** i wybierz tylko **Serwer bezpieczeństwa**.
   - Przejdź do zakładki **Głębokość** i wybierz **Wszystkie elementy rekursywanie**.

4. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Aktualizacje Security Server**.
5. Będziesz musiał potwierdzić swoje działanie. Kliknij **Tak** aby utworzyć zadanie.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

WAŻNE
Zaleca się skorzystać z tej metody, aby zaktualizować Security Server przez NSX, w przeciwnym razie kwarantanny zapisane na urządzeniu zostaną usunięte.

Wstaw Narzędzie Niestandardowe

Aby wstrzyknąć narzędzia do wnętrza systemu operacyjnego:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Zaznacz pola wyboru docelowych punktów końcowych.
5. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Wstrzyknij Narzędzie Niestandardowe**. Wyświetlono okno konfiguracji.
6. Z rozwijanego menu wybierz wszystkie narzędzia, które chcesz wstrzyknąć. Dla każdego wybranego narzędzia zostanie wyświetlona sekcja z jego ustawieniami.

   Narzędzia te zostały wcześniej przesłane do GravityZone. Jeśli nie znajdziesz odpowiedniego narzędzia na liście, przejdź do **Centrum Zarządzania Narzędziami** i dodaj go z tego poziomu. Aby uzyskać więcej informacji, zapoznaj się z „Iniekcja Narzędzi Niestandardowych z HVI" (p. 483).
7. Dla każdego narzędzia wyświetlonego w oknie:
   a. Kliknij nazwę narzędzia, aby zobaczyć lub ukryć jego sekcje.
   b. Wpisz wiersz polecenia narzędzia, wraz z wszystkimi potrzebnymi parametrami wejściowymi, podobnie jak w Wierszu Polecenia lub w Terminalu. Na przykład:

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

W przypadku Narzędzi Naprawczych BD można wybrać tylko działanie naprawcze i działanie zaradcze kopii zapasowych z obu rozwijanych menu.

c. Wskaż lokalizację, z której serwer Security Server powinien zbierać dzienniki:

- **stdout**. Zaznacz to pole wyboru, aby przechwycić dzienniki ze standardowego kanału komunikacyjnego.
- **Plik wyjściowy**. Zaznacz to pole wyboru, aby zebrać plik dziennika zapisany w punkcie końcowym. W tym przypadku należy wprowadzić ścieżkę, na której Security Server może odnaleźć plik. Możesz używać ścieżek bezwzględnych lub zmiennych systemowych.

  Tutaj masz dodatkową opcję: **Usuń pliki dziennika z Gościa po ich przesłaniu**. Zaznacz pliki, których nie potrzebujesz w punkcie końcowym.

8. Jeśli chcesz przenieść plik dzienników z Security Server do innej lokalizacji, musisz podać ścieżkę do miejsca docelowego i dane uwierzytelniające.
9. Czasami narzędzie może wymagać dłuższego czasu niż oczekiwano, aby zakończyć pracę lub może przestać reagować. Aby uniknąć awarii w takich sytuacjach, w sekcji **Konfiguracja Bezpieczeństwa** wybierz, po upływie jakiego czasu Security Server powinien automatycznie zakończyć proces.
10. Kliknij **Zapisz**.

    Stan zadania można zobaczyć na stronie **Zadania**. Aby uzyskać więcej informacji, możesz też sprawdzić raport **status wstrzyknięcia zewnętrznego HVI**.

6.2.6. Tworzenie szybkich raportów

Możesz wybrać żeby stworzyć błyskawiczne raporty nw temat zarządzanych komputerów począwszy od strony **Sieć**:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu. Wszystkie komputery z wybranej grupy są wyświetlane w tabeli prawego panelu bocznego.

   Opcjonalnie, możesz filtrować zawartość wybranej grupy jedynie przez zarządzane komputery.

4. Zaznacz pole wyboru dla komputera, który chcesz chcesz uwzględnić w raporcie.
5. Kliknij przycisk **Raport** w górnej części tabeli i wybierz rodzaj raportu z menu.

   Aby uzyskać więcej informacji, odwołaj się do „Komputer i Raporty Wirtualnej Maszyny” (p. 416).
6. Konfiguracja opcji raportu. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie raportów” (p. 435).
7. Kliknij **Wygeneruj**. Raport jest natychmiast wyświetlony.

   Czas wymagany do utworzenia raportu może być zależny od ilości wybranych komputerów.

6.2.7. Przypisywanie polityk

Możesz zarządzać opcjami bezpieczeństwa na komputerach wykorzystując, polityki.

Ze strony **Sieć** możesz zobaczyć, zmienić i przypisać polityki dla każdego komputera lub grupy komputerów.

Notatka
Ustawienia Bezpieczeństwa są dostępne jedynie dla zarządzanych komputerów. Aby ułatwić przeglądanie i zarządzanie ustawieniami bezpieczeństwa, możesz filtrować inwentaryzacjami sieci jedynie poprzez zarządzane komputery.

Aby zobaczyć przypisane polityki dla konkretnego komputera:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
4. Naciśnij nazwę zarządzanego komputera, który Cię interesuje. Pojawi się okno informacyjne.
5. W zakładce **Ogólne**, w sekcji **Polityki**, kliknij nazwę obecnej polityki, aby zobaczyć jej ustawienia.
6. Możesz zmienić ustawienia bezpieczeństwa jakie potrzebujesz, pod warunkiem, że właściciel polityki zezwala użytkownikom na wprowadzenie zmian w tej polityce. Pamiętaj, że wszystkie wprowadzone zmiany będą miały wpływ na wszystkie komputery przypisane do tej samej polityki.

Aby uzyskać informacje na temat ustawień polityk komputerów, odwołaj się do „Polityki Komputerów i Maszyn Wirtualnych" (p. 233).

Aby przypisać politykę do komputera lub grupy:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
4. Zaznacz pole wyboru docelowych komputerów lub grup. Możesz wybrać jeden z kilku obiektów tego samego rodzaju tylko tego samego poziomu.
5. Kliknij przycisk **Przypisz Polityki** w górnej części tabeli.
6. Dokonaj niezbędnych ustawień w oknie **Przypisanie polityki**. Aby uzyskać więcej informacji, odwołaj się do „Przypisywanie polityk" (p. 222).

Korzystanie z Menedżera Odzyskiwania dla Zaszyfrowanych Woluminów

Gdy użytkownicy zapomną swoich haseł szyfrowania i nie mogą uzyskać dostępu do zaszyfrowanych dysków, możesz im pomóc odzyskując klucze ze strony **Sieć**

Aby pobrać klucz odzyskiwania:

1. Przejdź do strony **Sieć**.
2. Kliknij **Menedżer Odzyskiwania** w pasku narzędzi po lewej stronie. Pojawi się nowe okno.
3. W sekcji **Identyfikator** wprowadź następujące dane:
   a. ID klucza odzyskiwania zaszyfrowanego woluminu. ID klucza odzyskiwania jest ciągiem cyfr i liczb dostępnym na punkcie końcowym na ekranie odzyskiwania Bitlockera.

      Na Windows, ID klucza odzyskiwania jest ciągiem cyfr i liczb dostępnym na punkcie końcowym na ekranie odzyskiwania Bitlockera.

      Możesz także użyć opcji **Odzyskiwanie** w zakładce **Ochrona** we właściwościach komputera aby automatycznie wprowadzić ID klucza odzyskiwania, zarówno dla punktów końcowych z Windows jak i macOs.

   b. Hasło do twojego konta GravityZone.

4. Kliknij **Ujawnij**. Okno się rozwija.

   W **Informacjach o Woluminie** znajdziesz następujące dane:

   a. Nazwa woluminu

   b. Typ woluminu (rozruchowy lub nierozruchowy).

   c. Nazwa punktu końcowego (wymieniona w Zasobach Sieci)

   d. Klucz Odzyskiwania. Na Windows, klucz odzyskiwania jest hasłem automatycznie generowanym podczas szyfrowania woluminu. Dla Mac, klucz odzyskiwania jest jednocześnie hasłem użytkownika.

5. Wyślij klucz odzyskiwania do użytkownika.

Szczegółowe informacje o szyfrowaniu i odszyfrowywaniu woluminów przy użyciu GravityZone znajdują się w „Szyfrowanie” (p. 381).

6.2.9. Synchronizowanie z Active Directory.

Zasoby sieci są automatycznie synchronizowane z Active Directory w przedziałach czasu określonych w sekcji konfiguracyjnej Control Center. Aby uzyskać więcej informacji, zapoznaj się z rozdziałem Instalacja i Konfiguracja GravityZone w Przewodniku Instalacyjnym GravityZone.

Aby ręcznie zsynchronizować obecnie wyświetlane zasoby sieci przy pomocy Active Directory:

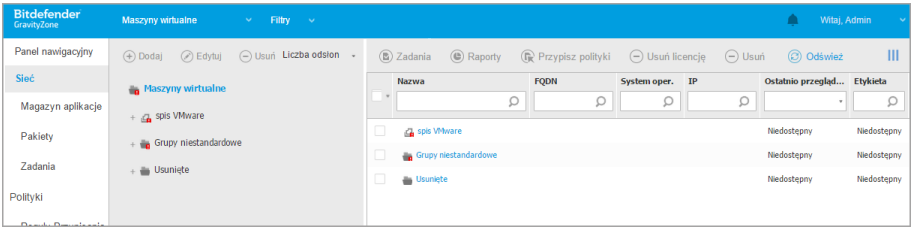
1. Przejdź do strony **Sieć**.
2. Wybierz **Komputer i Wirtualna Maszyna** dla selektora widoku.
3. Naciśnij przycisk **Synchronizuj z Active directory** z górnej strony tabeli.
4. Czynności należy potwierdzić, klikając **Tak**.

> **Notatka**
> Dla duzych sieci Active directory, synchronizacja może zajać więcej czasu.

6.3. Maszyny wirtualne

Aby zobaczyć zwirtualizowaną pod swoim kontem infrastrukturę, przejdź do strony **Sieć** i wybierz **Maszyny Wirtualne** z Selektora widoku.

Notatka
Możesz zarządzać maszynami wirtualnymi również z widoku **Komputery i Maszyny Wirtualne**, ale by zobaczyć zawartość infrastruktury wirtualizacji oraz filtry musimy użyć określonych kryteriów z widoku **Maszyny Wirtualne**.
Dla uzyskania szczegółowych informacji na temat pracy z widokami sieci, zapoznaj się z „Praca z widokami sieci” (p. 44).



Sieć - widok Maszyn Wirtualnych

Możesz przeglądać dostępne sieci wirtualnych maszyn w lewym panelu i szczegóły każdej wirtualnej maszyny w prawym panelu.

Aby spersonalizować szczegółowe dane o maszynach wirtualnych wyświetlanych w tabeli:

1. Kliknij przycisk III **Kolumny** z prawej górnej strony tabeli.
2. Wybierz kolumny, które chcesz zobaczyć.
3. Naciśnij przycisk **Reset** aby przywrócić domyślny widok kolumn.

Prawy panel wyświetla drzewo jako przegląd wirtualnej infrastruktury. Administracją drzewa nazywamy **Wirtualne Maszyny** i wirtualne maszyny są zgrupowane pod administratorem, w poniższych kategoriach bazujących na dostawcach technologii wirtualizacji:

- **Zasoby Nutanix.** Zawiera listę systemów Elementów Prism Nutanix, do których masz dostęp.
- **Zasoby VMware.** Zawiera listę serwerów vCenter do których masz dostęp.
- **Zasoby Citrix.** Zawiera listę systemów XenServer do których masz dostęp.
- **Grupy niestandardowe.** Zawiera serwer bezpieczeństwa i wykrytą maszynę wirtualną w sieci po za jakimkolwiek Serwerem vCenter lub systemem XenServer.

Lewy panel zawiera menu zwane **Widoki** z którego użytkownik może wybrać rodzaj widoku dla każdego dostawcy technologi wirtualizacji.

Aby uzyskać dostęp do zwirtualizowanej infrastruktury zintegrowanej z Control Center musisz dostarczyć swojemu użytkownikowi poświadczeń dla każdego dostępnego systemu serwera vCenter. Po wprowadzeniu swoich poświadczeń, zostaną one zapisane w Menadżerze Poświadczeń tak, by nie było potrzeby wprowadzania ich ponownie. Aby uzyskać więcej informacji, odwołaj się do „Manager uprawnień” (p. 215).

W sekcji **Sieć**, możesz zarządzać wirtualnymi masznami, według poniższych:

- Sprawdź status maszyny wirtualnej
- Sprawdź szczegóły wirtualnej maszyny.
- Organizuj maszyny wirtualne w grupy
- Sortuj, filtruj i wyszukuj
- Uruchom zadania
- Twórz szybkie raporty
- Przydziel polityki
- Wyczyść miejsca licencji

W sekcji **Konfiguracja > Ustawienia sieciowe** możesz skonfigurować zaplanowane reguły dla automatycznego usuwania nieużywanych maszyn wirtualnychz Inwentarza Sieci.

6.3.1. Sprawdzanie Statusu Maszyn Wirtualnych

Każda maszyna wirtualna jest reprezentowana na stronie sieci jako odpowiednia do swojego typu i statusu ikona.

Odnieś się do „Typy obiektów sieciowych i statusy” (p. 514) dla listy ze wszystkimi dostępnymi typami ikon i statusów.

Aby uzyskać szczegółowe informacje, odwołaj się do:

- Stan zarządzania
- Stan łączności
- Stan bezpieczeństwa

Stan zarządzania

Maszyny Wirtualne mogą posiadać następujący status zarządzania:

- **Zarządzane** - maszyny wirtualne, na których została zainstalowana ochrona Bitdefender.

- **W oczekiwaniu na restart** - maszyny wirtualne, które wymagają ponownego uruchomienia systemu po zainstalowaniu lub zaktualizowaniu ochrony Bitdefender.
- **Niezarządzane** - wykryte maszyny wirtualne, na których ochrona Bitdefender nie została jeszcze zainstalowana.
- **Usunięte** - maszyny wirtualne, które usunęliśmy z konsoli Control Center. Aby uzyskać więcej informacji, odwołaj się do „Usuwanie punktów końcowych z zasobów sieci" (p. 210).

Stan łączności

Status połączenia dotyczy zarządzanych maszyn wirtualnych i Security Server. Z tego punktu widzenia, zarządzane maszyny wirtualne mogą być:

- **Online**. Niebieska ikona oznacza, że punkt końcowy jest online.
- **Offline**. Szara ikona oznacza, że maszyna jest offline.

Maszyna Wirtualna jest offline, jeżeli agent bezpieczeństwa jest nieaktywny dłużej niż 5 minut. Możliwe powody, dlaczego maszyny wirtualne pojawiają się jako offline:

- Maszyna wirtualna jest wyłączana, usypiana lub hibernowana.

  Notatka
  Maszyny Wirtualne wydają się być online nawet gdy są zablokowane lub użytkownik jest wylogowany.

- Agenci ochrony nie posiadają łączności z serwerem komunikacyjnym GravityZone:
  - Maszyny wirtualne mogą zostać rozłączone od sieci.
  - Zapora sieciowa lub router mogą blokować komunikację między agentem ochrony a Control Center Bitdefender lub przydzielonego Endpoint Security Relay.
  - Maszyna Wirtualna znajduje się za serwerem proxy a jego ustawienia nie zostały prawidłowo skonfigurowane w zastosowanej polityce.

    Ostrzeżenie
    Dla maszyn wirtualnych za serwerami proxy, ustawienia proxy muszą być prawidłowo skonfigurowane w paczce instalacyjnej agenta bezpieczeństwa, w innym wypadku maszyna wirtualna nie będzie komunikowała się z konsolą

GravityZone i pozostanie offline, bez względu na to czy zastosowano polityki ustawień właściwego proxy po instalacji.

- Agent bezpieczeństwa został ręcznie odinstalowany z maszyny wirtualnej, podczas gdy maszyna wirtualna nie była połączona z Control Center Bitdefender lub przypisanym Endpoint Security Relay. Zwykle, gdy agent bezpieczeństwa zostaje ręcznie odinstalowany z maszyny wirtualnej, Control Center otrzymuje informacje o tym zdarzeniu, a maszyna wirtualna zostaje oznaczona jako niezarządzana.
- Agent bezpieczeństwa może nie działać poprawnie.

Aby dowiedzieć się, jak długo maszyny wirtualne były nieaktywne:

1. Wyświetlaj tylko zarządzane maszyny wirtualne. Kliknij menu **Filtry** zlokalizowane z górnej strony tabeli, wybierz wszystkie "Zarządzane" opcje, które potrzebujesz z zakładki **Bezpieczeństwo**, wybierz **Wszystkie obiekty rekurencyjne** z zakładki **Głębokość** i kliknij **Zapisz**.
2. Naciśnij nagłówek kolumny **Ostatnio Widziane** aby posortować wirtualne maszyny według okresu bezczynności.

Można zignorować krótsze okresy bezczynności (minuty, godziny), ponieważ są prawdopodobnie wynikiem warunku czasowego. Na przykład, wirtualna maszyna jest aktualnie wyłączony.

Dłuższe okresy bezczynności (dni, tygodnie), zazwyczaj wskazują na problem z wirtualną maszyną.

Notatka
Zalecane jest by odświeżyć tabelę sieci od czasu do czasu, aby zaktualizować informacje o najnowszych zmianach na punktach końcowych.

Stan bezpieczeństwa

Status bezpieczeństwa dotyczy zarządzanych maszyn wirtualnych i Security Server. Możesz identyfikować maszyny wirtualne lub Security Servers z problemami bezpieczeństwa poprzez zaznaczenie ikony statusu wyświetlającej symbol ostrzeżenia:

- Z problemami.
- Bez problemów.

Maszyna wirtualna lub Security Server posiada problem bezpieczeństwa spowodowany co najmniej jedną z poniższych sytuacji:

- Ochrona Antymalware jest wyłączona (tylko dla maszyn wirtualnych).
- Klucz licencyjny wygasł.
- Produkt Bitdefender jest nieaktualny.
- Zawartość bezpieczeństwa jest nieaktualna.
- HVI Pakiet Uzupełniający jest przestarzały.
- Malware zostało wykryte (tylko na maszyny wirtualne).
- Łączność z Usługą Chmury Bitdefender nie może zostać ustalona, z następujących przyczyn:
  - Maszyna wirtualna posiada problemy z łącznością internetową.
  - Zapora sieciowa blokuje połączenie z Usługą Chmury Bitdefender.
  - Port 443, wymagany do komunikacji z Usługą Chmury Bitdefender jest zamknięty.

  W tym przypadku ochrona przed złośliwym oprogramowaniem opiera się wyłącznie na silnikach lokalnych, podczas gdy skanowanie w chmurze jest wyłączone oznacza to, że agent ochrony nie może dostarczyć pełnej ochrony w czasie rzeczywistym.

Jeżeli zauważysz maszynę wirtualną z problemami bezpieczeństwa, kliknij jej nazwę aby wyświetlić okno **Informacje**. Można identyfikować problemy bezpieczeństwa poprzez ikonę ! . Upewnij się, aby sprawdzić informacje o ochronie we wszystkich zakładkach informacji na stronie. Wyświetl ikony podpowiedzi aby znaleźć więcej szczegółów. Mogą być potrzebne dalsze badania lokalne.

Notatka
Zalecane jest by odświeżyć tabelę sieci od czasu do czasu, aby zaktualizować informacje o najnowszych zmianach na punktach końcowych.
Punkty końcowe, które nie otrzymały żadnych aktualizacji w ciągu ostatnich 24 godzin, są automatycznie oznaczane **Z błędami**, niezależnie od wersji sygnatur obecnych na przekaźniku lub w GravityZone Update Server.

6.3.2. Wyświetlanie Szczegółów Maszyny Wirtualnej

Szczegółowe informacje o każdej maszynie wirtualnej można uzyskać na stronie **Sieć**:

- Sprawdzanie zakładki **Sieci**
- Sprawdzanie okna **Informacji**

Sprawdzane strony Sieci

Aby dowiedzieć się szczegółów dotyczących maszyny wirtualnej, sprawdź informacje dostępne w tabeli po prawej stronie ekranu na stronie **Sieć**.

Kolumny można dodawać lub usuwać za pomocą informacji o maszynie wirtualnej, klikając przycisk **Kolumny** w prawym górnym rogu panelu.

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego.

   Wszystkie wirtualne maszyny należące do wybranej grupy są wyświetlone w prawym bocznym panelu tabeli.
4. Możesz w łatwy sposób identyfikować status maszyny wirtualnej przez sprawdzenie odpowiedniej ikony. Szczegółowe informacje znajdują się w „Sprawdzanie Statusu Maszyn Wirtualnych” (p. 108).
5. Sprawdź informacje wyświetlane w kolumnach tabeli dla każdej wirtualnej maszyny.

   Użyj wiersza nagłówka do wyszukiwania podczas wpisywania określonych maszyn wirtualnych, zgodnie z dostępnymi kryteriami:

   - **Nazwa**: nazwa maszyny wirtualnej.
   - **FQDN**: w pełni kwalifikowana nazwa domeny zawierająca nazwę hosta i nazwę domeny.
   - **OS**:zainstalowany system operacyjny na wirtualnej maszynie.
   - **IP**: adres wirtualnej maszyny IP.
   - **Ostatnio widziany**: Data i czas kiedy wirtualna maszyna była ostatni raz widoczna online.

     Notatka
     Monitorowanie pola **Ostatnio widziany** jest istotne, ponieważ dłuższe okresy bezczynności mogą wskazywać na problem z komunikacją lub odłączenie wirtualnej maszyny.

   - **Etykieta**: niestandardowy opis z dodatkowymi informacjami na temat punktu końcowego. Możesz dodać etykietę w oknie **Informacje** maszyny wirtualnej, a następnie użyć jej w wyszukiwaniu.

- **Polityka**: polityka dotycząca maszyny wirtualnej, z linkiem do przeglądania lub zmiany ustawień polityki.

Sprawdzanie okna Informacji

W prawym okienku strony **Sieć** kliknij nazwę maszyny wirtualnej, która Cię interesuje, aby wyświetlić okno **Informacje**. To okno wyświetla tylko dane dostępne dla wybranej maszyny wirtualnej, pogrupowane na kilka kart.

Poniżej znajdziesz wyczerpującą listę informacji, które można znaleźć w oknie **Informacje**, w zależności od typu maszyny (wirtualna maszyna, instancja Security Server) i konkretnych informacji o jej zabezpieczeniach.

Zakładka Ogólne

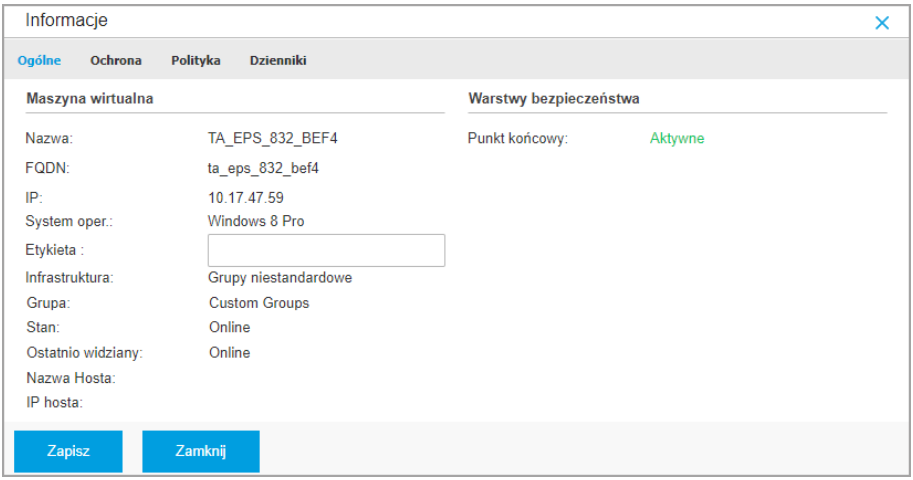
- Ogólne informacje o maszynach wirtualnych, takie jak nazwa, informacje FQDN, adresy IP, system operacyjny, infrastruktura, grupa nadrzędna i obecny status.

  W tej sekcji można przypisać etykietę maszynie wirtualnej. Będziesz mógł szybko znaleźć maszyny wirtualne o tej samej etykiecie i podejmować na nich działania, niezależnie od tego, gdzie znajdują się w sieci. Aby uzyskać więcej informacji o filtrowaniu maszyn wirtualnych, przejdź do „Sortowanie, Filtrowanie i Wyszukiwanie dla Maszyn Wirtualnych” (p. 122).

- **Wymagania HVI**, zawierają informację o tym czy możesz użyć Security Server do wdrożenia ochronyHVI lub nie. Tak więc, jeśli host Security Server jest uruchomiony na obsługiwanej wersji XenServer, a pakiet uzupełniający jest zainstalowany, możesz włączyć HVI na maszynach wirtualnych z tego hosta.
- Informacje o warstwach zabezpieczających, w tym listę technologii zabezpieczeń zakupionych wraz z rozwiązaniem GravityZone i ich statusem licencji, które mogą być:
  - **Dostępny / Aktywny** - klucz licencyjny dla tej warstwy ochronnej jest aktywny na maszynie wirtualnej.
  - **Wygasł** - klucz licencyjny dla tej warstwy ochrony wygasł.
  - **Oczekujący** - klucz licencyjny nie został jeszcze zatwierdzony.

    Notatka
    Dodatkowe informacje o warstwach ochrony są dostępne w zakładce **Ochrona**.

- **Połączenie Przekaźnikowe**: nazwa, adres IP i etykieta przekaźnika, do którego podłączona jest maszyna wirtualna.



Okno informacyjne - Ogólne

Zakładka Ochrony

Ta zakładka zawiera szczegółowe informacje o każdej warstwie ochrony licencjonowanej na punkcie końcowym. Szczegóły znajdują się:

- Informacje z Agenta Ochrony takie jak Nazwa i wersja, konfiguracja silników skanowania oraz status aktualizacji. Dla Ochrony Exchange, silnik i sygnatury antyspam też są już dostępne
- Status zabezpieczenia każdej warstwy ochrony. Ten status pojawia się po prawej stronie nazwy warstwy zabezpieczającej:
  - **Bezpieczny**, jeśli nie wystąpiły problemy dotyczące zabezpieczeń punktów końcowych, na których zastosowana jest warstwa ochrony.
  - **Narażony**, jeśli wystąpiły problemy dotyczące zabezpieczeń punktów końcowych, na których zastosowana jest warstwa ochrony. Szczegółowe informacje znajdują się w „Stan bezpieczeństwa” (p. 110).
- Powiązany Security Server. Każdy przydzielony Security Server wyświetlany jest w przypadku bez-agentowego wdrożenia lub kiedy silniki skanowania agentów ochrony są ustawione na zdalne skanowanie. Informacje o Security

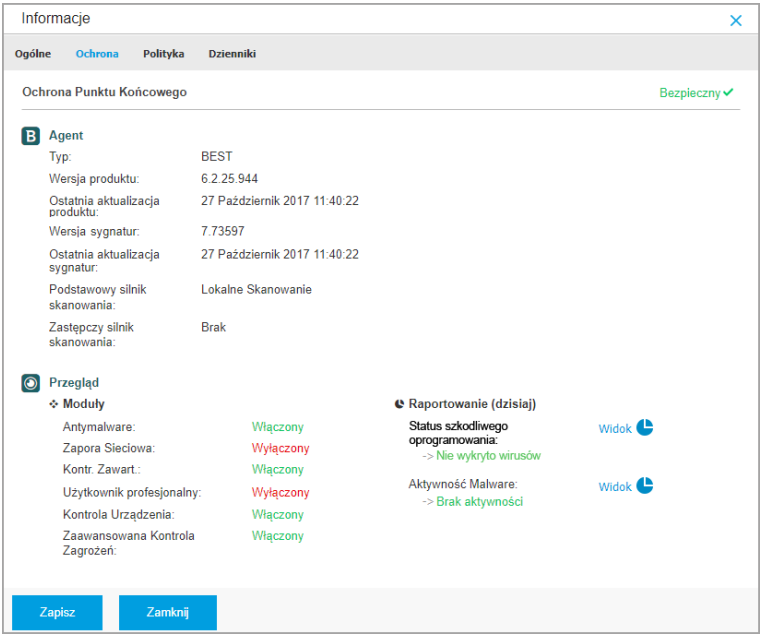
Server pomagają ci zidentyfikować wirtualne urządzenie i dostać status jego aktualizacji.

- Informacje związane z NSX, takie jak status wirusów i grupy ochrony do których należy maszyna wirtualna. Jeśli nalepka zabezpieczająca została umieszczona, to świadczy o tym, że urządzenie jest zainfekowane. W przeciwnym razie maszyna jest czysta lub tagi bezpieczeństwa nie były używane.
- Status nodułów ochrony. Możesz z łatwością zobaczyć, który moduł ochrony został zainstalowany na punkcie końcowym oraz sprawdzić status dostępnych modułów (**Wł/Wył.**) ustawionych przez zastosowane polityki.
- Szybki przegląd dotyczący aktywności modułów i raportowania malware w obecnym dniu.

  Kliknij link **Zobacz** aby wejść do opcji raportów i wtedy wygenerować raport. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie raportów” (p. 435)
- Informacje dotyczące warstwy ochrony Sandbox Analyzer:
  - Status wykorzystania Sandbox Analyzer na wirtualnej maszynie, wyświetlany jest po prawej stronie okna:
    - **Aktywny**: Sandbox Analyzer jest licencjonowany (dostępny) i włączony poprzez politykę w maszynie wirtualnej.
    - **Nieaktywny**: Sandbox Analyzer jest licencjonowany (dostępny) ale nie jest włączony poprzez politykę w maszynie wirtualnej.
  - Nazwa agenta, który pełni rolę czujnika zasilania.
  - Status modułu na maszynie wirtualnej:
    - **Włączony** - Sandbox Analyzer jest włączony na maszynie wirtualnej za pomocą polityki.
    - **Wyłączony** - Sandbox Analyzer nie jest włączony na maszynie wirtualnej za pomocą polityki.
  - Wykrywanie zagrożeń z poprzedniego tygodnia klikając link **Pokaż**, aby uzyskać dostęp do raportu.
- Dodatkowe informacje dotyczące modułu szyfrowania, takie jak:
  - Wykryte woluminy (wspominające dysk rozruchowy).

– Stan szyfrowania dla każdego woluminu (**Zaszyfrowane**, **Szyfrowanie w toku**, **Odszyfrowywanie w toku**, **Niezaszyfrowane**, **Zablokowane** lub **Wstrzymane**).

  Kliknij link **Odzyskiwanie** aby pobrać klucz odzyskiwania dla powiązanych zaszyfrowanych woluminów. Szczegółowe informacje na temat pobierania kluczy odzyskiwania można znaleźć w „Korzystanie z Menedżera Odzyskiwania dla Zaszyfrowanych Woluminów” (p. 164).



Okno informacyjne - zakładka Ochrony

W przypadku Security Server ta karta zawiera informacje o module Ochrony Pamięci. Szczegóły znajdują się:

- Status usługi:
  – **Nie dotyczy** - Ochrona Pamięci jest licencjonowana, ale usługa nie jest jeszcze skonfigurowana.
  – **Włączone** - usługa jest włączona w politykach i funkcjonowaniu.
  – **Wyłączone** - usługa nie działa, ponieważ została wyłączona z polityki lub klucz licencyjny wygasł.

- Lista podłączonych urządzeń pamięci zgodnych z ICAP z następującymi szczegółami:
  - Nazwa urządzenia pamięci
  - IP urządzenia pamięci
  - Typ urządzenia pamięci
  - The date and time of the last communication between the storage device and Security Server.

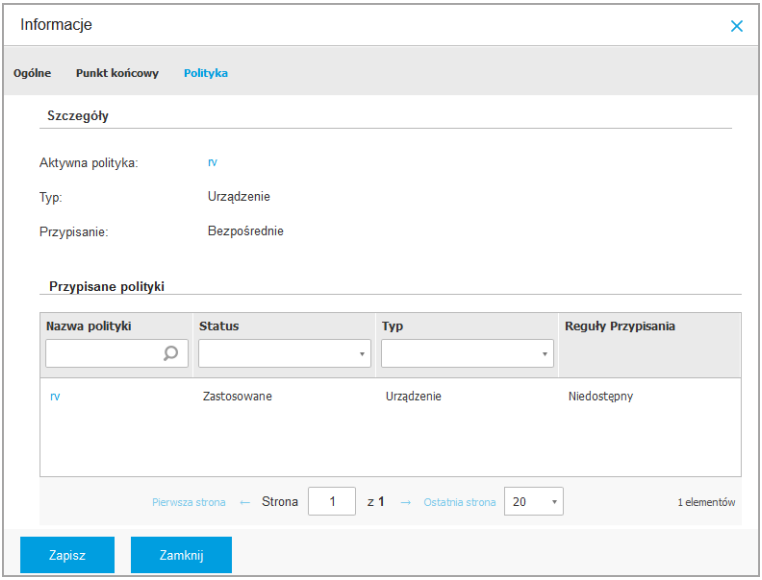
Zakładka Polityki

Dla maszyny wirtualnej może być zastosowana jedna lub kilka polityk, ale tylko jedna polityka może być aktywna w tym samym czasie. Zakładka **Polityka** wyświetla informacje o wszystkich politykach odnoszących się do maszyny wirtualnej.

- Nazwa aktywnej polityki. Kliknij nazwę polityki by otworzyć szablon polityki oraz zobaczyć swoje ustawienia.
- Typ aktywnej polityki, taki jak:
  - **Urządzenie**: gdy polityka jest przypisana ręcznie do maszyny wirtualnej przez administratora sieci.
  - **Lokalizacja**: polityka oparta na zasadach jest automatycznie przypisywana do maszyny wirtualnej, jeśli ustawienia sieciowe maszyny są zgodne z warunkami istniejącej zasady przypisywania.
  - **Użytkownik**: polityka oparta na zasadach jest automatycznie przypisywana do punktu końcowego, jeśli odpowiada ona celom Active Directory określonym w istniejącej zasadzie przypisywania.

    Na przykład, maszyna może mieć przypisane dwie polityki świadomości użytkownika, jedną dla administratorów i drugą dla innych pracowników. Każda polityka staje się aktywna, gdy użytkownik z odpowiednimi uprawnieniami zaloguje się.
  - **Zewnętrzny (NSX)**: gdy polityka jest zdefiniowana w środowisku VMware NSX.
- Typ przypisania aktywnej polityki, taki jak:
  - **Bezpośrednia**: gdy polityka jest bezpośrednio stosowana do maszyny wirtualnej.
  - **Odziedziczona**: jeśli maszyna wirtulna dziedziczy politykę z grupy nadrzędnej.

- **Obowiązujące polityki**: wyświetla listę polityk powiązanych z istniejącymi regułami przypisywania. Zasady te mogą mieć zastosowanie do maszyny wirtualnej, jeśli jest ona zgodna z określonymi warunkami reguł przypisania.

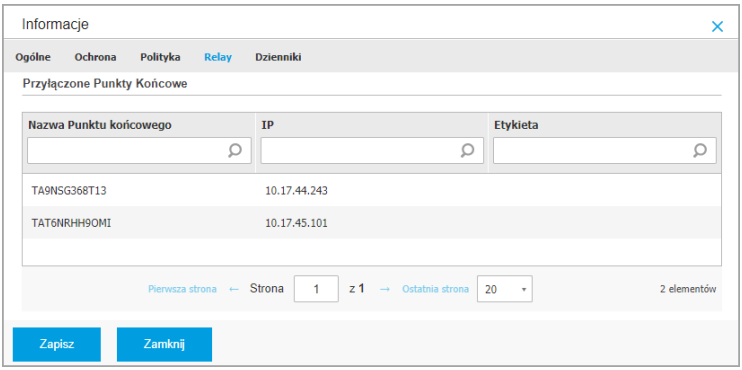


Okno informacyjne - Polityka

Aby uzyskać więcej informacji dotyczących polityk, zapoznaj się z „Zarządzanie politykami” (p. 219)

Zakładka Przekaźnika

Zakładka **Relay** jest dostępna tylko dla maszyn wirtualnych z rolą relay. Ta zakładka wyświetla informacje na temat punktów końcowych połączonych to aktualnego pośrednika, takie jak nazwa, IP i etykieta.



Okno informacyjne - Relay

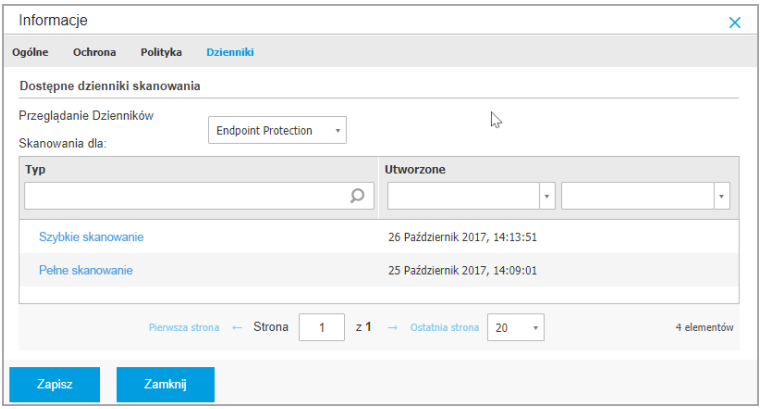
Zakładka Dziennika Skanowania

Sekcja **Dziennik Skanowania** wyświetla szczegółowe informacje na temat wszystkich zadań skanowania wykonanych na maszynach wirtualnych.

Logi są pogrupowane według warstw ochrony i możesz wybrać z rozwijalnej listy z której warstwy chcesz wyświetlić logi.

Kliknij zadanie skanowania, które cie interesuje, następnie log otworzy się w nowej karcie przeglądarki.

Kiedy wiele logów skanowania jest dostępnych, mogą rozszerzać się przez wiele stron. Do poruszania się po kolejnych stronach służą opcje nawigacji znajdujące się na dole tabeli. Jeżeli jest tam za dużo wpisów, możesz użyć opcji filtra dostępnych na górze tabeli.



Okno informacyjne - logi skanowania

Każdy element w tym oknie, który generuje problemy z bezpieczeństwem jest oznaczony ikoną **!** . Sprawdź ikony podpowiedzi aby znaleźć więcej szczegółów. Mogą być potrzebne dalsze badania lokalne.

6.3.3. Organizuj wirtualne maszyny w grupy.

Możesz zarządzać grupami maszyn wirtualnych w lewym panelu bocznym strony **Sieci**, w folderze **Niestandardowe Grupy**.

Wirtualne Maszyny importowane z Nutanix Prism Element są pogrupowane w folderze **Zasób Nutanix**. Wirtualne Maszyny importowane z VMware vCenter są pogrupowane w folderze **Zasób VMware**. Wirtualne Maszyny importowane zXenServer są pogrupowane w folderze **Zasób Citrix**. Nie można edytować Inwentarza Nutanix, Inwentarza VMware ani Inwentarza Citrix. Można tylko przeglądać i zarządzać odpowiednimi maszynami wirtualnymi.

Wszystkie maszyny wirtualne, które nie są zarządzane przez Nutanix Prism, vCenter i system XenServer są wykryte przez wyszukiwanie sieci i znajdują się w **Grupy Niestandardowe**, gdzie możesz zorganizować je w grupy. Główną zaletą jest to, że możesz korzystać z polityk grupy w celu spełnienia różnych wymogów bezpieczeństwa.

W **Niestandardowe Grupy** możesz utworzyć, usunąć, zmienić nazwę i przesunąć grupy maszyn wirtualnych w ramach zdefiniowanej niestandardowej struktury drzewa.

Notatka

- Grupa może zawierać zarówno maszyny wirtualne jak i inne grupy.
- Wybierając grupę w lewym panelu bocznym, możesz zobaczyć wszystkie maszyny wirtualne z wyjątkiem tych umiesz w podgrupach. Aby zobaczyć wszystkie maszyny wirtualne uwzględnione w grupie oraz swoich podgrupach, kliknij menu **Filtry** zlokalizowanego z górnej strony tabeli i wybierz **Wszystkie elementy rekurencyjnie** w sekcji **Głębia**.

Tworzenie grup

Przed rozpoczęciem tworzenia grup, pomyśl dlaczego ich potrzebujesz i wymyśl schemat grup. Na przykład, możesz zgrupować maszyny wirtualne bazujące na jednym lub kilku poniższych kryteriów:

- Struktura organizacyjna (Sprzedaż, Marketing, Zapewnienie Jakości, Rozwój Oprogramowania, Zarządzanie itp.).
- Potrzeby bezpieczeństwa (Komputery stacjonarne, Laptopy, Serwery, itd.).
- Lokalizacja (Siedziba Główna, Biura Lokalne, Pracownicy zdalni, Biura Domowe itp.).

Aby zorganizować swoją sieć w grupy:

1. Wybierz **Niestandardowe Grupy** w lewym panelu.
2. Naciśnij przycisk ⊕ **Dodaj grupę** u góry lewego panelu bocznego.
3. Podaj sugestywna nazwę dla grupy i naciśnij **OK**. Nowa grupa wyświetli się w **Grupy Niestandardowe**.

Zmienianie nazw grup

Aby zmienić nazwę grupy:

1. Wybierz grupę z lewego panelu bocznego.
2. Naciśnij przycisk ✎ **Edytuj grupę** u góry lewego panelu bocznego.
3. Wprowadź nową nazwę w odpowiednim polu.
4. Kliknij **OK**, aby potwierdzić.

Przenoszenie Grup i wirtualnych Maszyn

Możesz przesunąć wpisy gdziekolwiek wewnątrz hierarchii **Niestandardowe Grupy**. Aby przenieść podmioty, przeciągnij i upuść je z prawego panelu bocznego do pożądanej grupy lewego panelu.

Notatka

Ten wpis został przeniesiony, odziedziczy ustawienia polityki nowej grupy macierzystej, chyba że dziedziczona polityka została wyłączona i inne licencje zostały przypisane do niego. Aby uzyskać więcej informacji o dziedziczeniu polityk, odwołaj się do „Polityki Bezpieczeństwa" (p. 218).

Usuwanie grup

Grupa nie może zostać usunięta jeżeli należy do niej przynajmniej jedna wirtualna maszyna. Przenieś wszystkie maszyny wirtualne z grupy, którą chcesz usunąć do innych grup. Jeżeli grupa zawiera podgrupy, możesz przenieść wpis podgrupy, a nie indywidualne maszyny wirtualne.

Aby usunąć grupę:

1. Wybierz pustą grupę.
2. Naciśnij przycisk ⊗ **Usuń grupę** u góry lewego panelu bocznego. Czynności należy potwierdzić, klikając **Tak**.

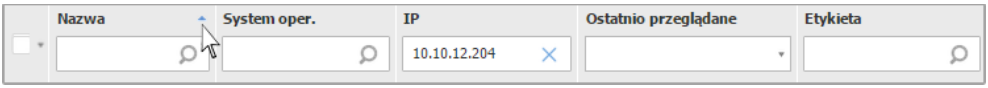
6.3.4. Sortowanie, Filtrowanie i Wyszukiwanie dla Maszyn Wirtualnych

W zależności od liczby maszyn wirtualnych, ich tabela może obejmować kilka stron (domyślnie tylko 20 wpisów jest wyświetlanych na każdej stronie). Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

Jeżeli jest zbyt dużo wpisów, można użyć pól wyszukiwania pod nagłówkiem kolumny lub menu **Filtry** z górnej części strony aby wyświetlić tylko interesujące nas podmioty. Na przykład, możesz szukać konkretnej wirtualnej maszyny lub wybrać widok tylko zarządzanych wirtualnych maszyn.

Sortowanie Wirtualnych Maszyn

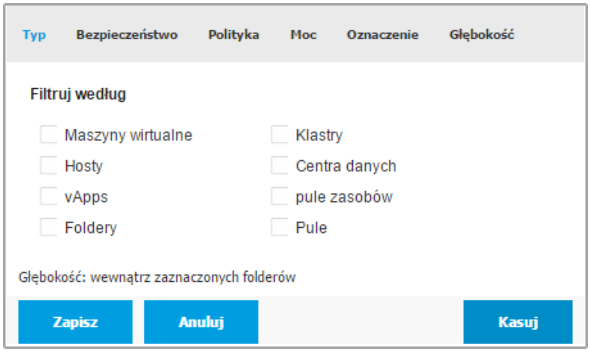
Aby posortować dane według konkretnej kolumny, naciśnij nagłówek kolumny. Na przykład, jeżeli chcesz ułożyć wirtualne maszyny po nazwie, naciśnij nagłówek **Nazwa**. Po ponownym kliknięciu wirtualne maszyny zostaną posortowane w odwrotnej kolejności.



Sortowanie komputerów

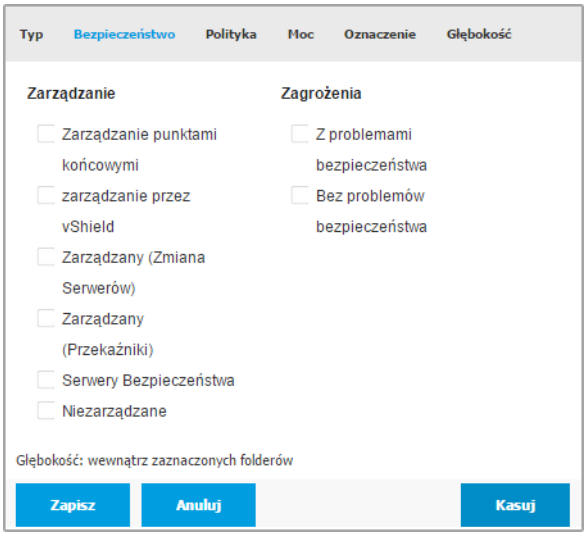
Filtrowanie Wirtualnych Maszyn

1. Wybierz pożądaną grupę z lewego panelu bocznego.
2. Kliknij menu **Filtry**z górnej bocznej strony obszaru panela sieciowego.
3. Wybierz kryteria filtrowania według:
   - **Typ**. Zaznacz rodzaje wirtualnych maszyn jakie mają być wyświetlane.



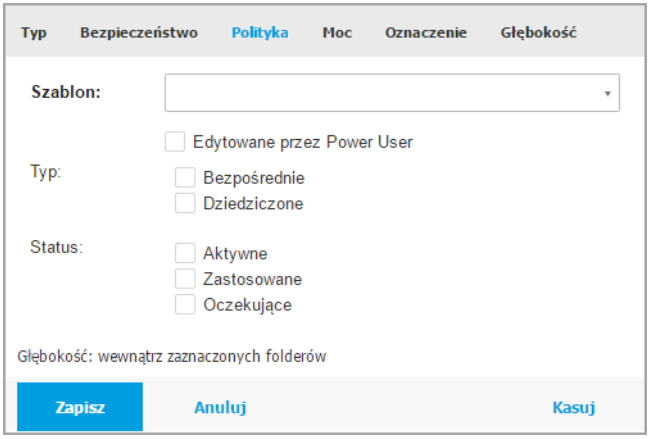
Wirtualne Maszyny - Filtrowane po Rodzaju

   - **Bezpieczeństwo**. Wybierz zarządzanie ochroną i/lub stan zabezpieczeń, aby przefiltrować obiekty sieciowe. Na przykład, można wybrać wyświetlanie tylko Security Server maszyn, albo można zobaczyć tylko punkty końcowe z kwestiami dotyczącymi bezpieczeństwa.



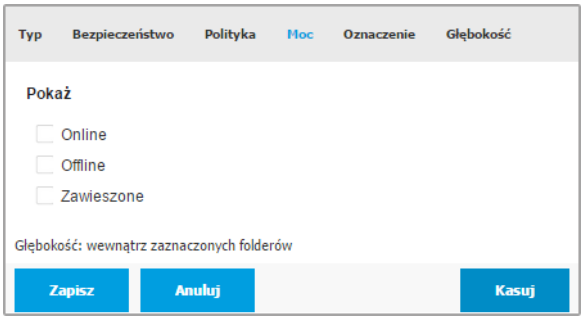
Wirtualne Maszyny - filtrowane po bezpieczeństwie

- **Polityka**. Wybierz szablon polityki jakim chcesz filtrować wirtualne maszyny, typ przypisania polityki (bezpośrednio lub dziedziczone), jak również status przypisania polityki (Aktywna, Przypisana lub w Toku).



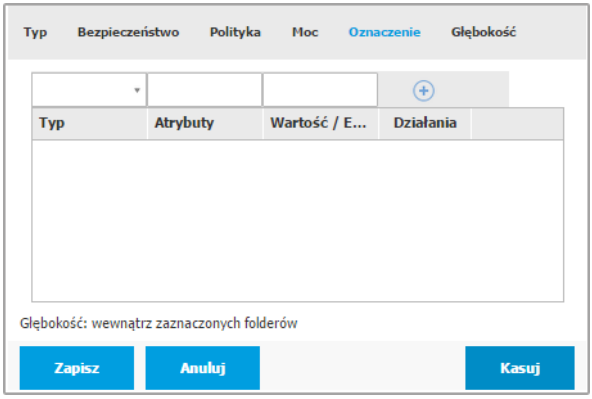
Wirtualne Maszyny - filtrowane po Polotyce

- **Moc**. Możesz wybrać pomiędzy maszynami wirtualnymi będącymi online, offline lub zawieszonymi.



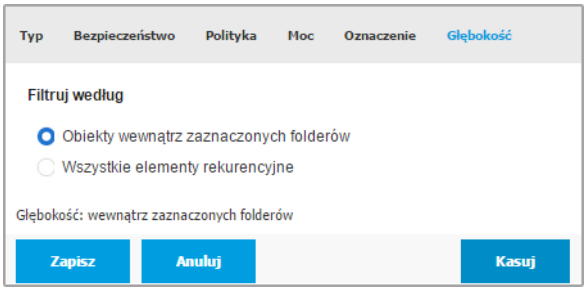
Wirtualne Maszyny - Filtrowanie po Zasilaniu

- **Etykiety**. Możesz wybrać aby odfiltrować wirtualne maszyny po etykiecie lub atrybutach jakie zdefiniowałeś w twoim środowisku wirtualizacji.



Wirtualne Maszyny - Filtrowane po Etykietach

- **Głębokość**. Podczas zarządzania strukturą drzewa sieci wirtualnych maszyn, wirtualne maszyny znajdujące się w podgrupach nie są wyświetlane domyślnie. Wybierz **Wszystkie elementy rekurencyjnie** aby zobaczyć wszystkie wirtualne maszyny zawarte w obecnej grupie i podgrupach.



Wirtualne Maszyny - Filtrowane po Głębokości

Notatka
Naciśnij **Reset** aby wyczyścuć filtr i wyświetlić wszystkie wirtualne maszyny.

4. Naciśnij **Zapisz** aby odfiltrować wirtualne maszyny według wybranych kryteriów.

Wyszukiwanie dla Maszyn Wirtualnych

1. Wybierz pożądany kontener z lewego panelu bocznego.
2. Podaj wyszukiwaną frazę w odpowiednim polu pod nagłówkami kolumn (nazwa, OS lub IP) z prawego panelu bocznego. Na przykład,w polu **IP** podaj adres IP wirtualnej maszyny, której szukasz. Tylko pasujące wirtualne maszyny pokażą się w tabeli.

   Wyczyść pole wyszukiwania aby wyświetlić pełną listę wirtualnych maszyn.

6.3.5. Działanie zadań na wirtualnych maszynach

Ze strony **Sieć**, możesz zdalnie uruchomić zadania administracyjne na wirtualnej maszynie.

Oto co możesz zrobić:

- „Skanowanie” (p. 127)
- „Zadania Uaktualnienia” (p. 138)
- „Skanowanie Exchange” (p. 140)
- „Zainstaluj” (p. 145)
- „Odinstaluj Klienta” (p. 149)
- „Aktualizacja” (p. 150)
- „Rekonfiguruj Klienta” (p. 151)

- „Przeszukiwanie sieci" (p. 152)
- „Wykrywanie Aplikacji" (p. 153)
- „Restartuj maszynę" (p. 154)
- „Zainstaluj Security Server" (p. 154)
- „Odinstaluj Security Server" (p. 157)
- „Aktualizuj Security Server" (p. 157)
- „Zainstaluj Pakiet Uzupełniający HVI" (p. 158)
- „Odinstaluj Pakiet Uzupełniający HVI" (p. 159)
- „Aktualizuj Pakiet Uzupełniający HVI" (p. 160)

Możesz wybrać aby stworzyć indywidualne zadania dla każdej maszyny wirtualnej lub dla grupy maszyn wirtualnych. Dla przykładu, możesz zdalnie zainstalować Bitdefender Endpoint Security Tools w grupie niezarządzanych maszyn wirtualnych. W późniejszym czasie, możesz stworzyć zadanie skanowania dla określonych maszyn wirtualnych z tej samej grupy.

Dla każdej maszyny wirtualnej możesz rozpocząć kompatybilne zadania. Dla przykładu, jeżeli wybierzesz niezarządzane maszyny wirtualne, możesz jedynie wybrać instalację agenta bezpieczeństwa, wszystkie pozostałe zadania będą nieaktywne.

Dla grupy, wybierane zadania będą stworzone tylko dla kompatybilnych maszyn wirtualnych. Jeżeli żadna maszyna wirtualna w grupie nie jest kompatybilny z wybranymi zadaniami, zostaniesz poinformowany, że zadanie nie może zostać utworzone.

Po utworzeniu zadania, od razu uruchomi się na maszynach wirtualnych będących online w sieci. Jeżeli maszyna wirtualna jest offline, zadanie rozpocznie się zaraz po podłączeniu online.

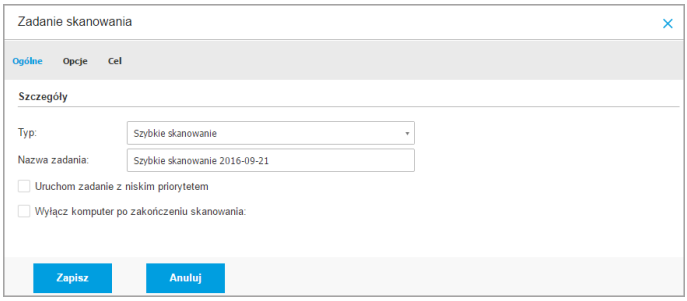
Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do „Przeglądanie i zarządzanie zadaniami" (p. 206).

Skanowanie

Aby uruchomić zadanie skanowania na kilku maszynach wirtualnych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.
4. Zaznacz pola odpowiadające obiektom które mają być zeskanowane.

5. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Skanowanie**. Wyświetlone zostanie okno konfiguracji.
6. Skonfiguruj opcje skanowania:
   - W zakładce **Ogólne** możesz wybrać rodzaj skanowania i podać nazwę zadania skanowania. Zadanie skanowania ma pomóc Ci zidentyfikować aktualne skanowanie na stronie **Zadania**.



Zadanie Skanowania Maszyn Wirtualnych - Ustawienia ogólnej konfiguracji

Wybierz rodzaj skanowania z menu **Rodzaj**:

– **Szybkie Skanowanie** jest wstępnie skonfigurowane, aby umożliwić skanowanie tylko najważniejszych lokalizacji systemu i nowych plików. Wykonanie szybkiego skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.

  Kiedy zostaje wykryte złośliwe oprogramowanie lub rootkity, Bitdefender automatycznie przeprowadza dezynfekcję. Jeśli z jakiegokolwiek powodu plik nie może zostać zdezynfekowany, zostaje przeniesiony do kwarantanny. Ten typ skanowania ignoruje podejrzane pliki.

– **Pełne Skanowanie**sprawdza cały system w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu, takiego jak wirusy, oprogramowanie typu spyware/adware, rootkity i inne.

  Bitdefender automatycznie próbuje zdezynfekować wykryte pliki zawierające złośliwe oprogramowanie. W przypadku, gdy nie można usunąć złośliwego oprogramowania, znajduje się ono w kwarantannie, gdzie nie może wyrządzić żadnej szkody. Podejrzane pliki są ignorowane.

Jeśli chcesz podjąć działania dotyczące podejrzanych plików lub inne domyślne akcje zainfekowanych plików, wybierz opcję uruchomienia skanowania niestandardowego.

– **Skanowanie Pamięci** sprawdza programy działające w pamięci maszyny wirtualnej.

– **Skanowanie Sieci** jest typem niestandardowego skanowania, pozwalającego na skanowanie dysków używając agenta bezpieczeństwa Bitdefender zainstalowanego na docelowych maszynach wirtualnych.

  W celu uruchomienia zadania skanowania sieciowego:

  - Musisz przypisać zadanie do jednego pojedynczego punktu końcowego w swojej sieci.
  - Musisz wprowadzić listy uwierzytelniające dla użytkowników kont z prawem odczytu/zapisu na docelowym dysku sieciowym, dla umożliwienia agentowi bezpieczeństwa dostanie się i podejmowanie czynności na tych dyskach sieciowych. Wymagane poświadczenia mogą być skonfigurowane w zakładce **Cel** nowego okna zadania.

– **Niestandardowe skanowanie**dopuszcza wybranie lokacji, które mają zostać przeskanowane i skonfigurować opcje skanowania.

Dla pamięci, sieci i niestandardowych skanów, masz następujące opcje:

– **Uruchom zadanie z niskim priorytetem**. Wybierz ten checkbox aby zmniejszyć priorytet procesu skanowania i pozwolić innym programom działać szybciej. Zwiększy to czas potrzebny na zakończenie skanowania.

> **Notatka**
> Ta opcja dotyczy tylko Bitdefender Endpoint Security Tools i Endpoint Security (agent legacy).

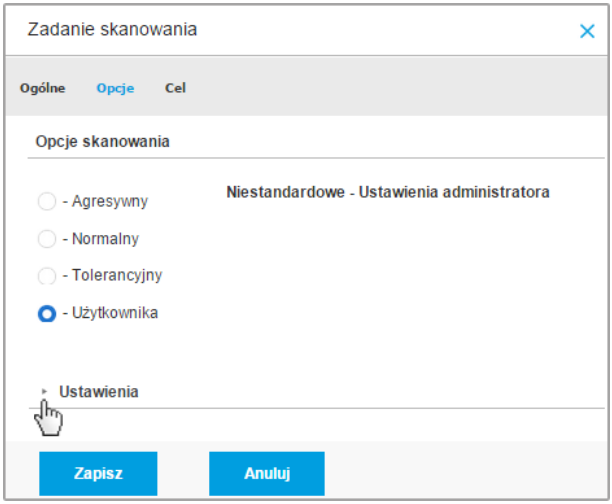
– **Wyłącz komputer po zakończeniu skanowania**. Wybierz ten checkbox, aby wyłaczyć twoją maszynę, jeśli nie zamierzasz z niej korzystać przez jakiś czas.

> **Notatka**
> Ta opcja dotyczy Bitdefender Endpoint Security Tools, Endpoint Security (agent legacy) i Endpoint Security for Mac.

Dla niestandardowego skanowania, skonfiguruj następujące ustawienia:

– Przejdź do zakładki **Opcje** aby ustawić opcje skanowania. Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

  Bazując na wybranym profilu, opcje skanowania w sekcji **Ustawienia** zostaną automatycznie skonfigurowane. Jednak, jeżeli chcesz, możesz skonfigurować je szczegółowo. Aby to zrobić, wybierz opcje **Niestandardowe** następnie rozwiń sekcję **Ustawienia**.



Zadanie Skanowania Maszyn Wirtualnych - Konfiguracja Niestandardowego Skanowania

Dostępne są następujące opcje:

- **Typy plików.** Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Możesz ustawić agenta bezpieczeństwa tak by skanował wszystkie pliki (niezależnie od rozszerzenia pliku), tylko pliki aplikacji lub określone rozszerzenia plików, które uważasz za potencjalnie niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.

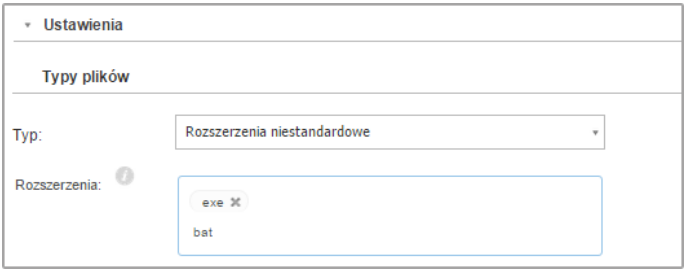
Notatka

Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji" (p. 516).

Jeżeli chcesz aby tylko określone rozszerzenia zostały przeskanowane, wybierz **Niestandardowe rozszerzenia** z menu wtedy podaj rozszerzenia w polu edycji, naciskając `Enter` po każdym rozszerzeniu.

WAŻNE

Agenty bezpieczeństwa Bitdefender zainstalowane na systemie operacyjnym Windows i Linux, skanują większość formatów .ISO, ale nie podejmują żadnych działań na nich.



Opcje zadania skanowania Maszyn Wirtualnych - Dodawanie niestandardowych rozszerzeń

- **Archiwa.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym. Jakkolwiek, zaleca się skanować archiwa w celu wykrycia i usunięcia potencjalnych zagrożeń, nawet jeśli nie są to zagrożenia bezpośrednie.

  WAŻNE

  Skanowanie zarchiwizowanych plików wydłuża ogólny czas skanowania i wymaga więcej zasobów systemowych.

- **Skanowanie wewnątrz archiwów.** Wybierz tę opcję tylko jeżeli chcesz sprawdzać pliki archiwów w poszukiwaniu malware. Jeżeli zdecydowałeś aby używać tej opcji, możesz skonfigurować poniższe opcje optymalizacji:
  - **Ogranicz rozmiar archiwum do (MB).** Możesz ustawić maksymalną akceptowalną wielkość archiwum do skanowania. Zaznacz odpowiadające pole wyboru i wpisz maksymalny rozmiar archiwum (w MB).
  - **Maksymalna głębokość archiwum (poziomy).** Zaznacz odpowiednie pole i wybierz maksymalną głębokość archiwum z menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.
- **Skanowanie archiwum e-mail.** Zaznacz tę opcję jeżeli chcesz włączyć skanowanie plików wiadomości e-mail i bazy e-mail, włączając formaty takie jak .eml, .msg, .pst, .dbx, .mbx, .tbb i inne.

  WAŻNE
  Skanowanie archiwum e-mail zużywa wiele zasobów i może mieć wpływ na wydajność systemu.

- **Inne.** Zaznacz odpowiednie pola, aby włączyć żądane opcje skanowania.
  - **Skanowanie sektorów startowych.** Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera kod maszyny wirtualnej, niezbędny do uruchomienia procesu ładowania systemu. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
  - **Skanowanie rejestru.** Włącz tę opcję, aby skanować klucze rejestru. Rejestr systemu Windows jest bazą danych przechowującą ustawienia konfiguracji i opcje dla komponentów systemu operacyjnego Windows oraz dla zainstalowanych aplikacji.
  - **Skanowanie w poszukiwaniu rootkitów.** Zaznacz tę opcję, aby skanować w poszukiwaniu rootkitów i ukrytych obiektów, które korzystają z tego rodzaju oprogramowania.

- **Skanuj w poszukiwaniu keyloggerów.** Zaznacz opcje skanowania dla oprogramowania keylogger. Keyloggery nie są złośliwymi aplikacjami z natury, ale mogą zostać wykorzystane w umyślnym celu. Haker może poznać ważne informacje z ukradzionych danych, takie jak numer i hasło do konta bankowego i użyć ich na własną korzyść.
- **Skanowanie pamięci.** Wybierz tę opcję, aby przeskanować programy działające w pamięci systemu.
- **Skanowanie ciasteczek.** Wybierz tę opcję, aby przeskanować ciasteczka zapisane przez przeglądarkę na maszynie wirtualnej.
- **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Potencjalnie nie chciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-suppored). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.
- **Skanowanie wymiennych woluminów.** Wybierz tę opcję aby przeskanować wymienny dysk przyłączony do maszyny wirtualnej.

- **Akcje.** W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:
  - **Gdy zostanie wykryty zainfekowany plik.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI). Agent bezpieczeństwa Bitdefender może normalnie usunąć złośliwy kod z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

Jeżeli zainfekowany plik został wykryty, agent bezpieczeństwa Bitdefender podejmie automatyczną próbę jego dezynfekcji. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.

WAŻNE
W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Przy wykryciu podejrzanego pliku .** Pliki są wykryte jako podejrzane przez analizę heurystyczną i inne technologie Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

  Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny. Pliki kwarantanny są wysyłane do analizy do Laboratorium Bitdefender w regularnych odstępach czasu. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

- **Gdy zostanie wykryty rootkit.** Rootkity stanowią specjalistyczne oprogramowanie wykorzystywane do ukrywania plików systemowych. Rootkity choć są nieszkodliwe, często są używane do ukrywania złośliwego oprogramowania lub intruza w systemie.

  Wykrywanie rootkitów i ukrywanie plików jest domyślnie ignorowane.

Gdy zostanie wykryty wirus na maszynie wirtualnej NSX w Security Server automatycznie oznacza maszynę wirtualną z tagiem bezpieczeństwa, pod warunkiem, że opcje zostały wybrane do vCenter Server integration.

W tym celu, NSX zawiera trzy znaczniki bezpieczeństwa, charakterystyczne dla stopnia nasilenia zagrożenia:

- `ANTI_VIRUS.VirusFound.threat=low`, stosowana na maszynie, gdy Bitdefender wyszukuje szkodliwe oprogramowanie niskiego ryzyka, które może usunąć.
- `ANTI_VIRUS.VirusFound.threat=medium`, stosowanie na maszynie jeżeli Bitdefender nie może usunąć zainfekowanych pliki, ale zamiast tego dezynfekuje je.
- `ANTI_VIRUS.VirusFound.threat=high`, zastosowanie na maszynie jeżeli Bitdefender nie może ani usunąć ani wyleczyć zainfekowanych pliki, ale blokuje dostęp do nich.

Można wyizolować zainfekowane maszyny przez utworzenie grup zabezpieczeń z dynamicznym członkowstwem w oparciu o znaczniki bezpieczeństwa.

WAŻNE

- Jeśli Bitdefender stwierdzi zagrożenia w maszynie o różnych poziomach (severity), będzie stosować wszystkie pasujące tagi.
- Znacznik bezpieczeństwa zostanie usunięty z maszyny dopiero po wykonaniu pełnego skanowania i odkażenia urządzenia.

Choć nie jest to polecane, możesz zmienić domyślne działania. Można tu wybrać osobną czynność dla każdej kategorii, a także określić drugą czynność, jaka ma zostać podjęta, jeśli pierwsza nie przyniesie skutku. Wybierz z odpowiedniego menu pierwszą i drugą czynność, jaka ma zostać zastosowana do każdego z wykrytych plików. Dostępne są następujące działania:

Dezynfekuj
Usuń złośliwy kod z zainfekowanych plików. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach.

Przenieś pliki do kwarantanny
Przenieś wykrytych plików z ich obecnego miejsca położenia do folderu kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami kwarantanny ze strony Kwarantanna w konsoli.

Usuń
Usuwa wykryte pliki z dysku, bez żadnego ostrzeżenia. Wskazane jest, aby unikać tego działania.

Ignoruj
Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania.

– Idź do zakładki **Cel** i dodaj lokacje które chciałbyś przeskanować na docelowych maszynach wirtualnych.

W sekcji **Cel skanowania** możesz dodać nowy filtr lub folder do przeskanowania:

a. Wybierz wcześniej zdefiniowaną lokalizacje z rozwijanego menu lub wprowadź **Określoną ścieżkę**, którą chciałbyś przeskanować.

b. W polu edycji określ ścieżkę do obiektów, które mają zostać przeskanowane.

- Jeżeli wybrałeś wcześniej zdefiniowana lokalizację, wypełnij ścieżkę jeśli potrzebujesz. Na przykład, aby przeskanować folder `Program Files` wystarczy wybrać odpowiednią ścieżkę z rozwijanego menu. Aby przeskanować konkretny folder z `Program Files`, musisz uzupełnić ścieżkę dodając backslash (\) i nazwę folderu.
- Jeżeli wybrałeś **Określona ścieżka**, podaj pełną ścieżkę do obiektu, który chcesz przeskanować. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich docelowych maszyn wirtualnych. Aby uzyskać więcej informacji dotyczących zmiennych systemowych, zapoznaj się z „Zmienne systemowe” (p. 517).

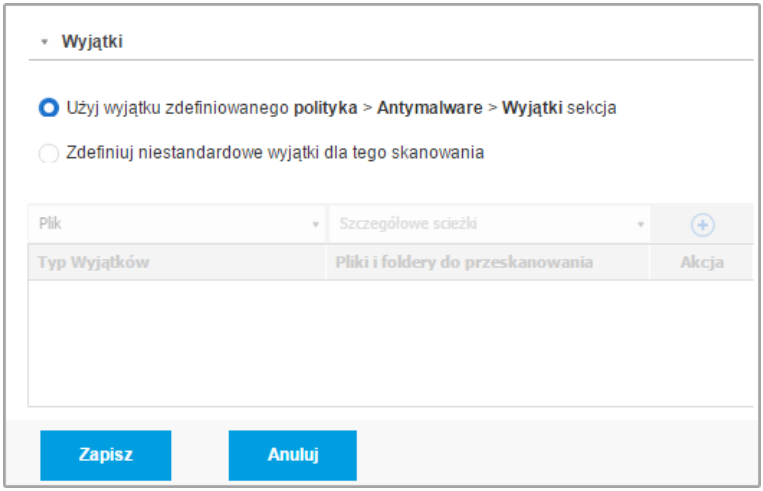
c. Naciśnij przycisk ⊕ **Dodaj**.

Aby edytować istniejącą lokalizację, kliknij ją. Aby usunąć lokalizację z listy, kliknij odpowiedni przycisk ⊗ **Usuń**.

W celu wykonania zadania skanowania sieciowego, musisz wprowadzić listy uwierzytelniające dla kont użytkowników posiadających prawo odczytu/zapisu na docelowych dyskach sieciowych, dla umożliwienia

agentowi bezpieczeństwa dostęp i podejmowanie czynności na dyskach sieciowych.

Kliknij sekcję **Wykluczenia** , jeśli chcesz zdefiniować wykluczenia celu.



Zadanie Skanowania Maszyn wirtualnych - Definiowanie wyjątków

Możesz korzystać z wykluczeń określonych przez politykę lub określić wyraźne wykluczenia dla bieżącego zadania skanowania. Aby uzyskać więcej informacji dotyczących wykluczeń, odwołaj się do „Wykluczenia” (p. 287).

7. Kliknij **Zapisz**, aby utworzyć zadanie skanowania. Pojawi się nowa wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Notatka
Aby zaplanować zadanie skanowania, idź do strony **Polityki**,wybierz politykę, do której przypisane są maszyny wirtualne, którymi jesteś zainteresowany i dodaj zadanie skanowania w sekcji **Antymalware >Na żądanie** Aby uzyskać więcej informacji, zapoznaj się z „Na żądanie” (p. 267).

Zadania Uaktualnienia

Zaleca się regularne sprawdzanie aktualizacji oprogramowania i stosowanie ich tak szybko, jak to możliwe. GravityZone automatyzuje ten proces za pomocą polityk bezpieczeństwa, ale jeśli potrzebujesz od razu zaktualizować oprogramowanie niektórych punktów końcowych, uruchom zadania w następującej kolejności:

1. Skanowanie Uaktualnień
2. Instalacja aktualizacji

Warunki wstępne

- Agent bezpieczeństwa z modułem Zarządzania Aktualizacjami jest zainstalowany na docelowych punktach końcowych.
- Aby zadania skanowania i instalacji zakończyły się powodzeniem, punkty komputery systemu Windows muszą spełniać następujące warunki:
  - **Zaufane Główne Urzędy Certyfikacji** przechowuje certyfikat **DigiCert Assured ID Root CA**.
  - **Pośrednie Urzędy Certyfikujące** obejmują **DigiCert SHA2 Assured ID Code Signing CA**.
  - Na punktach końcowych zainstalowane są aktualizacje dla Windows i Windows Server 2008 R2 wspomniane w tym artykule: Microsoft Security Advisory 3033929

Skanowanie Uaktualnień

Maszyny wirtualne z nieaktualnym oprogramowaniem są podatne na ataki. Zaleca się regularne sprawdzanie oprogramowania zainstalowanego na komputerach i aktualizowanie go tak szybko, jak to możliwe. Aby zeskanować maszyny wirtualne pod kątem brakujących aktualizacji:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Wybierz docelowe punkty końcowe.

5. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Skanowanie Aktualizacji**. Pojawi się nowe okno potwierdzające.
6. Kliknij **Tak**, aby potwierdzić zadanie skanowania.

   Kiedy zadanie się zakończy, GravityZone dodaje do Zasobów Aktualizacji wszystkie aktualizacje, których potrzebuje twoje oprogramowanie. Aby uzyskać więcej informacji, odwołaj się do „Inwentarz Aktualizacji" (p. 197).

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Notatka
Aby zaplanować skanowanie aktualizacji, edytuj polityki przypisane do docelowych komputerów i skonfiguruj ustawienia w sekcji **Zarządzanie Aktualizacjami**. Aby uzyskać więcej informacji, zapoznaj się z „Zarządzanie Aktualizacjami" (p. 334).

Instalacja aktualizacji

Aby zainstalować jedną lub więcej aktualizacji na docelowych maszynach wirtualnych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Instalacja Aktualizacji**.

   Wyświetlone zostanie okno konfiguracji. Tutaj możesz zobaczyć wszystkie aktualizacje, których brakuje w docelowych maszynach wirtualnych.
5. W razie potrzeby użyj opcji sortowania i filtrowania w górnej części tabeli, aby znaleźć określone aktualizacje.
6. Kliknij przycisk **Kolumny** po prawej stronie panelu, aby zobaczyć dodatkowe informacje.
7. Wybierz aktualizacje, które chcesz zainstalować.

   Niektóre aktualizacje są zależne od innych, W takim przypadku są one automatycznie wybierane jeśli mają aktualizaje.

Klikając na **CVEs** lub **Products** wyświetli się panel po lewej stronie. Panel zawiera dodatkowe informacje, takie jak CVE, które rozwiązuje aktualizacja, lub produkty, których dotyczy aktualizacja. Po zakończeniu czytania kliknij **Zamknij**, aby ukryć panel.

8. Wybierz opcję **Uruchom ponownie punkty końcowe po zainstalowaniu aktualizacji, jeśli jest to wymagane**, aby ponownie uruchomić punkty końcowe natychmiast po instalacji aktualizacji, jeśli wymagane jest ponowne uruchomienie systemu. Weź pod uwagę, że to działanie może zakłócić aktywność użytkownika.
9. Kliknąć **Instaluj**.

   Zadanie instalacji jest tworzone wraz z pod-zadaniami dla każdej docelowej maszyny wirtualnej.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Notatka

- Aby zaplanować wdrożnie aktualizacji, edytuj polityki przypisane do docelowych komputerów i skonfiguruj ustawienia w sekcji **Zarządzanie Aktualizacjami**. Aby uzyskać więcej informacji, zapoznaj się z „Zarządzanie Aktualizacjami" (p. 334).
- Możesz również zainstalować aktualizację ze strony **Inwentarz Aktualizacji**, zaczynając od aktualizacji, którą jesteś zainteresowany. W takim przypadku wybierz aktualizację z listy, kliknij przycisk **Zainstaluj** w górnej części tabeli i skonfiguruj szczegóły instalacji aktualizacji. Szczegółowe informacje znajdują się w „Instalowanie Aktualizacji" (p. 201).
- Po zainstalowaniu aktualizacji zalecamy wysłanie zadania Skanowanie Aktualizacji w celu dotarcia do punktów końcowych. Ta czynność uaktualni informacje o aktualizacji zapisane w GravityZone dla zarządzanych sieci.

Możesz odinstalować aktualizacje:

- Zdalnie, wysyłając zadanie odinstalowania aktualizacji z GravityZone.
- Lokalnie na maszynie. W takim przypadku musisz zalogować się jako administrator do punktu końcowego i ręcznie uruchomić dezinstalator.

Skanowanie Exchange

Możesz zdalnie skanować bazy danych Serwera Exchange poprzez uruchomienie zadania **Skanowanie Exchange**.

Aby być w stanie przeskanować bazę danych Exchange, musisz włączyć skanowanie na żądanie poprzez dostarcze uwierzytelnienia administratora Exchange. Aby uzyskać więcej informacji, odwołaj się do „Skanowanie Exchange Store” (p. 359).

Aby przeskanować bazę danych Serwera Exchange:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Z panela po lewej stronie, wybierz grupę zawierającą docelowy Serwer Exchange. Możesz odnaleźć serwer wyświetlony w panelu po prawej stronie.

   Notatka
   Optymalnie możesz zastosować filtry szybkiego odnajdywania docelowych serwerów:
   - Kliknij menu **Filtry** aby wybrać następujące opcje: **Zarządzane (Serwery Exchange)** z zakładki **Bezpieczeństwo** i **Wszystkie elementy rekurencyjne** z zakładki **Głębokość**.
   - Wprowadź nazwę hosta serwera lub adres IP w polach odpowiedniego nagłówka kolumny.

4. Wybierz pole wyboru Serwera Exchange którego bazę danych chcesz przeskanować.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Skanowanie Exchange**. Wyświetlone zostanie okno konfiguracji.
6. Skonfiguruj opcje skanowania:
   - **Ogólne.** Wprowadź sugestywną nazwę dla zadania.

     W przypadku dużych baz danych, zadanie skanowania może zająć dużo czasu i może mieć wpływ na wydajność serwera. W takich wypadkach, pole wyboru **Zatrzymaj skanowanie jeżeli zajmie to więcej niż** i wybierz dogodny przedział czasowy odpowiedniego menu.
   - **Cel.** Wybierz kontener i obiekty do skanowania. Możesz wybrać by skanowanie skrzynek pocztowych, publicznych folderów lub obu. Oprócz wiadomości e-mail, możesz skanować inne obiekty takie jak **Kontakty**, **Zadania**, **Spotkania** oraz **Elementy pocztowe**. Możesz ponadto ustawić następujące ograniczenia odnoszące się do skanowanej treści:
     – Tylko nieprzeczytane wiadomości
     – Tylko elementy z załącznikami
     – Tylko nowe pozycje, otrzymały określony przedział czasowy.

     Dla przykładu, możesz wybrać skanowanie tylko e-maili ze skrzyynek pocztowych użytkowników, które otrzymali w ciągu ostatnich siedmiu dni.

Zaznacz pole wyboru **Wykluczenia**, jeżeli chcesz zdefiniować skanowanie wyjątków. Aby utworzyć wyjątek, użyj pól z nagłówka tabeli w następujący sposób:

a. Wybierz typ repozytorium z menu.
b. Zależnie od rodzaju magazynu, określ obiekt jaki ma być wykluczony:

Typ repozytorium	Format obiektu
Skrzynka pocztowa	Adres e-mail
Folder publiczny	Ścieżka folderu, zaczynająca się od źródła
Baza danych	Tożsamość bazy danych

> **Notatka**
> By posiąść tożsamość bazy danych użyj polecenia shell Exchange:
> `Get-MailboxDatabase | fl name,identity`

Możesz dodać tylko jedną pozycję naraz. Jeżeli posiadasz kilka pozycji tego samego typu, musisz zdefiniować tyle zasad ile posiadasz pozycji.

c. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli by zapisać wyjątek i dodać go do listy.

Aby usunąć zasadę wyjątku z listy, kliknij odpowiadający mu przycisk ⊖ **Usuń**.

- **Opcje.** Skonfiguruj ustawienia skanowania dla wiadomości mailowych odpowiadającym zasadom:
  - **Przeskanowane typy plików.** Użyj tej opcji aby sprecyzować które typy plików chcesz przeskanować. Możesz ustalić skanowanie wszystkich plików (bez względu na ich rozszerzenie), samych plików aplikacji, lub określonego rozszerzenia, które uważasz za potencjalnie niebezpieczne. Skanowanie wszystkich plików zapewnia najlepszą ochronę, podczas gdy skanowanie jedynie aplikacji jest zalecane dla szybszego skanowania.

    > **Notatka**
    > Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji” (p. 516).

    Jeżeli chcesz skanować tylko pliki o konkretnym rozszerzeniu, masz dwie alternatywy:

- **Zadeklarowane rozszerzenia użytkownika**, tutaj musisz wprowadzić rozszerzenia które mają być skanowane.
- **Wszystkie pliki za wyjątkiem określonych rozszerzeń** tutaj należy podać rozszerzenia które mają zostać pominięte podczas skanowania.

– **Maksymalnym rozmiar załącznika / maila (MB).** zaznacz to pole wyboru i wprowadź wartość w odpowiednim polu aby ustawić maksymalny dopuszczalny rozmiar pliku załącznika lub długości treści maila, który ma być poddawany skanowaniu.
– **Maksymalna głębokość archiwum (poziomy).** Zaznacz pole wyboru i podaj maksymalną głębokość archiwum w odpowiednim polu. Im niższy poziom głębokości, tym większa wydajność i niższy stopień ochrony.
– **Sanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Zaznacz to pole wyboru by skanować w poszukiwaniu złośliwych i niechcianych aplikacji takich jak adware, który może instalować bez wiedzy użytkownika inne oprogramowanie,zmieniać działanie oprogramowania i obniżać wydajność systemu.

- **Akcje.** Możesz określić różne działania dla agenta bezpieczeństwa, aby je automatycznie podjął na plikach, w zależności od rodzaju detekcji.

  Rodzaj detekcji dzieli pliki na trzy kategorie:
  – **Pliki zainfekowane.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI).
  – **Podejrzane pliki.** Te pliki są wykryte jako podejrzane przez analizę heurystyczną i inne techonogię Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach.
  – **Nieskanowalne pliki.** Te pliki nie mogą być przeskanowane. Nieskanowalne pliki obejmują, ale nie ograniczają się do chronionych hasłem, zaszyfrowanych lub nadmiernie skompresowanych plików.

  Dla każdego rodzaju wykrycia, posiadasz domyślne lub główne działania oraz alternatywne działanie w przypadku awarii jednego z powyższych. Choć nie jest to zalecane, można zmienić ustawienia akcji w odpowiednim menu. Wybierz reakcję, która ma być podjęta:
  – **Dezynfekuj.** Usuwa złośliwy kod z zainfekowanego pliku i odbudowuje oryginalny plik. W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. Jest zalecane aby zawsze było to pierwsze działanie

wykonywane na zainfekowanych plikach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

- **Odrzuć / Usuń email.** Na serwerze z rolą Edge Transport, wykryty email jest odrzucany wraz z kodem błędu 550 SMTP. W każdym innym przypadku, wiadomość email jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Skasuj plik.** Kasuje załączniki w których wystąpiło zdarzenie bez wcześniejszego ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Plik zastępczy.** W miejsce skasowanego pliku umieszczany jest plik tekstowy który powiadamia użytkownika o podjętej czynności.
- **Przenieś plik do kwarantanny.** Przenosi wykryty plik do katalogu kwarantanny i umieszcza plik tekstowy który informuje użytkownika o podjętej czynności. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami w kwarantannie ze strony **Kwarantanna**

  Notatka
  Miej na uwadze, że kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni na partycji dysku twardego gdzie zainstalowano agenta. Rozmiar kwarantanny zależy od liczby elementów przechowywanych oraz ich wielkości.

- **Nie podejmuj działania.** Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania. Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny.
- Domyślnie, gdy email pasuje do zakresu reguł, jest przetwarzany wyłącznie ze zgodnymi zasadami, bez sprawdzania pod kątem wszelkich innych zasad. Jeśli chcesz kontynuować sprawdzanie pod kątem innych zasad, wyczyść pole wyboru **Jeżeli warunki reguł są dopasowane, wstrzymaj przetwarzanie kolejnych reguł**.

7. Kliknij **Zapisz**, aby utworzyć zadanie skanowania. Pojawi się nowa wiadomość potwierdzająca.
8. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Zainstaluj

Aby chronić maszyny wirtualne przy pomocy Security for Virtualized Environments, musisz zainstalować agenta bezpieczeństwa Bitdefender na każdym z nich. Agent bezpieczeństwa Bitdefender zarządza ochroną na maszynach wirtualnych. Komunikuje się również z Control Center aby otrzymać komendy administratora i wysłać wyniki przeprowadzonych działań. Po zainstalowaniu agenta bezpieczeństwa Bitdefender w sieci, automatycznie wykryje on niechronione maszyny wirtualne znajdujące się w tej sieci. Ochrona Security for Virtualized Environments może być zainstalowana na tych wirtualnych maszynach zdalnie z Control Center. Zdalna instalacja jest wykonywana w tle, bez wiedzy użytkownika.

W izolowanych sieciach, które nie mają bezpośredniej łączności z urządzeniem GravityZone, możesz zainstalować agenta bezpieczeństwa z rolą Relay. W tym wypadku, komunikacja pomiędzy urządzeniem GravityZone a pozostałymi agentami bezpieczeństwa będzie wykonywane poprzez agenta Relay, który będzie również pełnił rolę lokalnego serwera aktualizacji dla agentów bezpieczeństwa chroniących izolowane środowisko.

Notatka
Zaleca się by maszyna, na których instalujemy agentów Relay były zawsze włączone.

Ostrzeżenie
Przed instalacją, należy odinstalować istniejące oprogramowanie antymalware i zapory sieciowej z maszyn wirtualnych. Instalując ochronę Bitdefender na istniejące oprogramowanie bezpieczeństwa możemy wpłynąć na jego działanie i spowodować poważne problemy z pracą systemu. Windows Defender i Windows Firewall zostaną automatycznie wyłączone, gdy rozpocznie się instalacja.

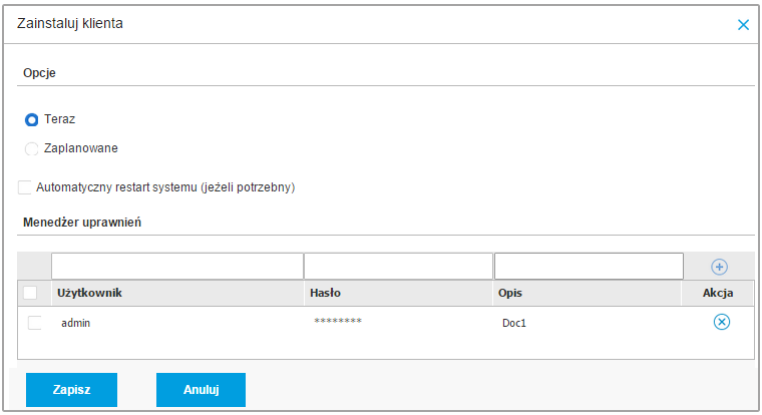
Aby zdalnie zainstalować ochronę Security for Virtualized Environments na jednym lub kilku maszynach wirtualnych:

1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz **Maszynę Wirtualną** z selektora widoku.
4. Wybierz pożądany kontener z lewego panelu bocznego. Jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.

Notatka
Opcjonalnie, możesz użyć filtrów w celu wyświetlenia jedynie niezarządzanych maszyn. Naciśnij menu **Filtry** i wybierz poniższe opcje: **Niezarządzane** z zakładki **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z zakładki **Głębokość**.

5. Wybierz podmioty (maszyny wirtualne, hosty, klastry lub grupy) na których chcesz zainstalować ochronę.
6. Kliknij przycisk **Zadania** z górnej strony tabelki i wybierz **Instaluj > BEST**.

   Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Bitdefender Endpoint Security Tools z menu zadań

7. W sekcji **Opcje** skonfiguruj czas instalacji:
   - **Teraz**, aby rozpocząć wdrożenie natychmiast.
   - **Zaplanowane**, aby ustawić przedział czasu na rozpoczęcie wdrożenia. W tym przypadku, wybierz przedział czasu jaki chcesz (godziny, dni lub tygodnie) i skonfiguruj go tak jak potrzebujesz.

     Notatka
     Na przykład, gdy określone operacje są wymagane na maszynach docelowych przed instalowaniem klienta (takie jak odinstalowanie innego oprogramowania albo ponowne uruchomienie systemu), możesz zaplanować zadanie wdrożenia aby uruchamiało się co 2 godziny. Zadanie rozpocznie się dla każdej maszyny docelowej w ciągu 2 godzin od udanego wdrożenia.

8. Jeśli chcesz, by docelowe punkty końcowe samoczynnie się uruchamiały, aby zakończyć instalację, wybierz **Automatyczny restart (w razie potrzeby)**.
9. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na docelowych punktach końcowych. Możesz dodać poświadczenia przez wpisanie użytkownika i hasła dla docelowego systemu operacyjnego.

   WAŻNE
   Dla Windows 8.1 musisz podać poświadczenia wbudowanego konta administratora lub konta administratora domeny. Aby nauczyć się więcej, odwołaj się do tego artykułu KB.

   Notatka
   Ostrzeżenie jest wyświetlane tak długo jak nie wybierzesz żadnych poświadczeń. Ten krok jest obowiązkowy, aby zdalnie zainstalować Bitdefender Endpoint Security Tools na punktach końcowych.

   Aby dodać wymagane poświadczenia OS:

   a. Podaj nazwę użytkownika i hasło dla konta administracyjnego dla docelowego systemu operacyjnego w odpowiednich polach z nagłówka tabeli poświadczeń. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto.

      Jeżeli maszyny znajdują się w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

      Użyj konwencji Windows podczas wprowadzania nazwy użytkownika konta

      - Dla maszyn Active Directory użyj tych składni: `username@domain.com` i `domain\username`. Aby upewnić się że wprowadzone poświadczenia będą działać, dodaj je w obu formach (`username@domain.com` i `domain\username`).
      - Dla maszyn z grupy roboczej, wystarczy wprowadzić tylko nazwę użytkownika, bez nazwy grupy roboczej.

   b. Kliknij przycisk ⊕ **Dodaj** . Konto jest dodane do listy poświadczeń.

      Notatka
      Określone poświadczenia, zostaną automatycznie zapisane w Menadżer Poświadczeń tak, by nie trzeba było wprowadzać ich następnym razem. Aby

uzyskać dostęp do Menadżera Poświadczeń, kliknij nazwę użytkownika w górnym prawym rogu konsoli.

WAŻNE
Jeżeli dostarczone poświadczenia są nieważne, instalacja klienta nie powiedzie się na odpowiednich punktach końcowych. Upewnij się, że zaktualizowałeś wprowadzone poświadczenia OS w Menedżerze Poświadczeń, gdy są one zmieniane na docelowych punktach końcowych.

c. Zaznacz pola odpowiadające kontom, które chcesz używać.

10. W sekcji **Wdrożeniowiec**, wybierz jednostkę, do której docelowa maszyna będzie się łączyła w celu instalacji i aktualizacji klienta:

- **Urządenie GravityZone**, gdy maszyny łączą się bezpośrednio do Urządenia GravityZone.

  W tym wypadku możemy również zdefiniować niestandardowy Serwer Komunikacyjny poprzez wprowadzenie jego adresu IP lub nazwy hosta, jeśli wymagane.

- **Endpoint Security Relay**, jeśli chcesz podłączyć komputery do klienta Relay zainstalowanego w sieci. Wszystkie maszyny z rolą Relay wykryte w Twojej sieci pokażą się w tabeli poniżej. Wybierz maszynę Relay. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego Relay.

  WAŻNE
  - Port 7074 musi być otwarty dla wdrożenia poprzez agenta Relay aby mógł działać.
  - Podczas wdrażania agenta za pośrednictwem Linux Relay muszą być spełnione następujące warunki:
    - Punkt końcowy Relay musi mieć zainstalowany pakiet Samba (`smbclient`) w wersji 4.1.0 lub nowszy i binarny/ wiersz poleceń `net` do wdrażania agentów Windows.

      Notatka
      Polecenie binarne/ `net` jest zwykle dostarczane razem z pakietami samba-client i/lub samba-common. W niektórych dystrybucjach Linuxa (takich jak CentOS 7.4) polecenie `net` jest instalowane tylko podczas instalowania pełnego pakietu

Samba (Common + Client + Server) Upewnij się, że Twój punkt końcowy Relay ma dostępne polecenie `net`.

- Docelowe punkty końcowe Windows muszą mieć włączone Zasoby Administracyjne i udostępnianie Sieciowe.
- Docelowe punkty końcowe Linux oraz Mac muszą mieć włączone SSH oraz wyłączony Firewall.

11. Musisz wybrać jeden pakiet instalacyjny dla aktualnego wdrożenia. Kliknij listę **Użyj pakietu** i wybierz pakiet instalacyjny, który chcesz. Możesz odnaleźć tutaj wszystkie paczki instalacyjne utworzone wcześniej dla twojej firmy.
12. Jeśli to potrzebne, można zmienić niektóre ustawienia wybranego pakietu instalacyjnego, klikając przycisk **Dostosuj** obok pola **Użycie pakietu**.

    Ustawienia pakietu instalacyjnego pojawią się poniżej i możesz wprowadzić zmiany, które potrzebujesz. Aby dowiedzieć się więcej o edycji pakietów instalacyjnych, zapoznaj się z Instrukcją instalacji GravityZone.

    Ostrzeżenie
    Pamiętaj że moduły Zapory Sieciowej są dostępne tylko dla wspieranych stacji roboczych Windows.

    Jeśli chcesz zapisać zmiany jako nowy pakiet, wybierz opcję **Zapisz jako pakiet** umieszczoną na dole listy ustawień pakietów, a następnie wpisz nazwę dla nowego pakietu instalacyjnego.
13. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

Odinstaluj Klienta

Aby zdalnie odinstalować ochronę Bitdefender:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie jednostki z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Zaznacz pola wyboru dla maszyn wirtualnych z których chcesz odinstalować agentów bezpieczeństwa Bitdefender.
5. Kliknij przycisk **Zadania** z bocznej strony tabeli i wybierz **Odinstaluj klienta**.

6. Konfiguracja okna jest wyświetlana w celu umożliwienia ustawienia następujących opcji:
   - Możesz zdecydować się na przechowywanie elementów podlegających kwarantannie na komputerze klienta.
   - Dla środowisk integracji vShield, musisz wybrać wymagane poświadczenia dla każdej maszyny, w innym wypadku odinstalowanie nie powiedzie się. Wybierz **Użyj poświadczeń dla integracji vShield**, po czym sprawdź wszystkie właściwe poświadczenia w tabeli Menadżera Poświadczeń wyświetlonej poniżej.
7. Naciśnij **Zapisz** aby utworzyć zadanie. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Notatka
Jeżeli chcesz przeinstalować ochronę, upewnij się czy zrestartowałeś wcześniej komputer.

Aktualizacja

Sprawdzaj okresowo status zarządzanych maszyn wirtualnych. Jeżeli zauważysz maszyny wirtualne z problemami bezpieczeństwa, kliknij ich nazwę, aby wyświetlić stronę **Informacje**. Aby uzyskać więcej informacji, odwołaj się do „Stan bezpieczeństwa” (p. 110).

Nieaktualni klienci lub przestarzała zawartość zabezpieczeń stanowią problemy z bezpieczeństwem. W tych wypadkach, musisz uruchomić aktualizację dla określonych maszyn wirtualnych. To zadanie dla maszyn wirtualnych może zostać wykonane lokalnie lub zdalnie z Control Center.

Aby zdalnie zaktualizować klienta i zawartość zabezpieczeń na zarządzanych maszynach wirtualnych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie jednostki z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.

4. Wybierz pola wyboru dla maszyn wirtualnych, na których chcesz uruchomić klienta aktualizacji.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Aktualizacja**. Wyświetlone zostanie okno konfiguracji.
6. Możesz wybrać aktualizację tylko produktu, tylko zawartości zabezpieczeń lub obu.
7. Dla systemu operacyjnego Linux i maszyn zintegrowanych z vShield, obowiązkowym jest wybranie odpowiednich poświadczeń. Zaznacz opcję **Użyj poświadczeń dla integracji Linux i vShield**, po czym wybierz właściwe poświadczenia z tabeli Menadżera Poświadczeń wyświetlonej poniżej.
8. Naciśnij **Aktualizuj** aby uruchomić zadanie. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Rekonfiguruj Klienta

Moduły ochrony agentów bezpieczeństwa, ich role i moduły skanowania są wstępnie skonfigurowane wewnątrz paczki instalacyjnej. Po zainstalowaniu agenta bezpieczeństwa w swojej sieci, można w każdym momencie zmienić wstępne ustawienia poprzez przesłanie zdalnego zadania **Przekonfiguruj Klienta** do pożądanego i zarządzanego punktu końcowego.

Ostrzeżenie
Należy pamiętać, że zadanie **Rekonfiguracji Klienta** nadpisuje wszystkie ustawienia instalacyjne, a żadne z początkowych ustawień nie zostaną zapisane. Podczas wykonywania zadania, upewnij się, że przekonfigurowałeś wszystkie ustawienia instalacyjne dla docelowego punktu końcowego.

Aby zmienić ustawienia instalacji dla jednego lub kilku maszyn wirtualnych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie jednostki z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.

4. Zaznacz pola wyboru maszyn wirtualnych, dla których chcesz zmienić ustawienia instalacyjne.
5. Kliknij przycisk **Zadania** w górnej części tabeli i wybierz **Rekonfiguracja klienta**.
6. W sekcji **Ogólne**, skonfiguruj kiedy zadanie ma być uruchamiane:
   - **Teraz**, aby uruchomić natychmiast.
   - **Zaplanowane**, aby ustawić częstotliwość powtórzeń zadania. W tym przypadku, wybierz przedział czasu jaki chcesz (godziny, dni lub tygodnie) i skonfiguruj go tak jak potrzebujesz.

     Notatka
     Na przykład, gdy inne ważne procesy są również wymagane do uruchomienia na docelowej maszynie, możesz zaplanować zadanie było wykonywane co każde 2 godziny. Zadanie rozpocznie się na każdej docelowej maszyny co 2 godziny do momentu pomyślnego wykonania.

7. Konfiguruj moduły, role i tryby skanowania dla docelowego punktu końcowego. Aby uzyskać więcej informacji zapoznaj się z Instrukcją Instalacyjną GravityZone.

   Ostrzeżenie
   - Zostaną zainstalowane tylko obsługiwane moduły dla każdego z systemów operacyjnych.

     Pamiętaj że moduły Zapory Sieciowej są dostępne tylko dla wspieranych stacji roboczych Windows.
   - Bitdefender Tools (agent dziedziczony) wspiera tylko Centralne Skanowanie.

8. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Przeszukiwanie sieci

Network discovery jest wykonywany automatycznie jedynie za pośrednictwem agenta bezpieczeństwa w raz z rolą Relay Jeżeli nie posiadasz zainstalowanego agenta Relay w swojej sieci, możesz ręcznie przesłać zadanie network discovery z poziomu chronionego punktu końcowego.

Aby uruchomić zadanie wykrywania sieci:

WAŻNE
Jeśli korzystając z Relaya na Linuxie do wykrycia pozostałych punktów końcowych z systemem Mac lub Linux, musisz zainstalować Sambę na punktach końcowych lub dołączyć je poprzez Active Directory korzystając z DHCP. W ten sposób NetBIOS zostanie na nie automatycznie skonfigurowany.

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie jednostki z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Wybierz pola wyboru dla maszyn, na których chcesz dokonać network discovery.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Network Discovery**.
6. Pojawi się nowa wiadomość potwierdzająca. Naciśnij **Tak**.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Wykrywanie Aplikacji

Aby wykryć aplikacje w twojej sieci:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie maszyny wirtualne z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Zaznacz wirtualne maszyny na których chcesz wykonać wykrywanie aplikacji.
5. Kliknij przycisk **Zadania** na górnej stronie tabeli i wybierz **Wykrywanie Aplikacji**.

Notatka
Bitdefender Endpoint Security Tools musi być zainstalowany z Kontrolą Aplikacji i aktywowany na zaznaczonych wirtualnych maszynach. W innym przypadku, zadanie będzie wyszarzone. Kiedy wybrana grupa zawiera jednocześnie aktywne i nieaktywne cele, zadanie wyślę tylko do aktywnych punktów końcowych.

6. Kliknij **Tak** w oknie potwierdzenia, aby kontynuować.

Wykryte aplikacje i procesy są wyświetlone na stronie **Sieć > Magazyn Aplikacji**. Aby uzyskać więcej informacji, zapoznaj się z „Magazyn Aplikacji" (p. 192).

Notatka
Zadanie **Wykrywanie Aplikacji** może zająć chwilę, w zależności od ilości zainstalowanych aplikacji. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami" (p. 206).

Restartuj maszynę

Możesz zdalnie uruchomić ponownie wybrane zarządzane maszyny wirtualne.

Notatka
Sprawdź strony **Sieć > Zadania** przed ponownym uruchomieniem maszyn wirtualnych. Uprzednio stworzone zadania mogą w dalszym ciągu być przetwarzane na docelowych maszynach.

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie jednostki z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Zaznacz pola wyboru dla maszyn wirtualnych, które chcesz ponownie uruchomić.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Zrestartuj maszynę**.
6. Wybierz opcje harmonogramu restartu:
   - Wybierz **Zrestartuj teraz** aby natychmiast uruchomić komputery ponownie.
   - Wybierz **Ponowne Uruchamianie włączone** i użyj pola poniżej do zaplanowania restartu komputera danego dnia o określonej porze.
7. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z Zadania Przeglądania i Zarządzania.

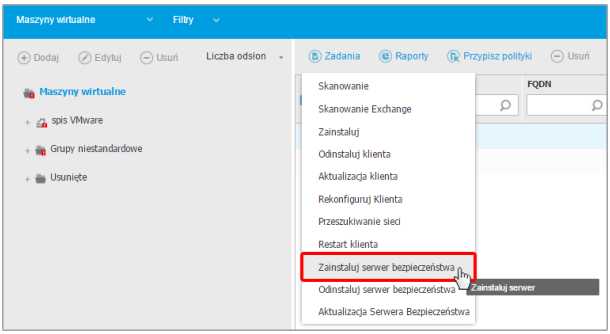
Zainstaluj Security Server

Aby zainstalować Security Server w twoim środowisku wirtualnym:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Przeglądaj zasoby Nutanix, VMware lub Citrix i wybierz pole wyboru odpowiadające wybranym hostom lub kontenerom (Nutanix Prism, serwer vCenter, XenServer lub centrum danych). Dla szybkiej selekcji, możesz bezpośrednio wybrać główny kontener (Nutanix Inventory, VMware Inventory lub Citrix Inventory). Będziesz mógł wybrać hosty indywidualnie z kreatora instalacji.

   Notatka
   Nie możesz wybrać hostów z różnych folderów.

4. Kliknij przycisk **Zadania** w górnej części tabeli i wybierz **Zainstaluj Security Server** z menu. Okno **Instalacja Security Server** zostało wyświetlone.



Instalowanie Security Server z menu zadań

5. Wszystkie hosty wykryte w wybranym kontenerze pojawią się na liście. Wybierz hosty na których chcesz zainstalować Security Server.
6. Wybierz ustawienia konfiguracji jakich chcesz używać.

   WAŻNE
   Korzystanie z ustawień wspólnych podczas wdrażania wieloplatformowego Security Server jednocześnie wymaga hostów udostępniających tą sama ilość pamięci, których adresy IP są przypisane do serwerów DHCP i będą częścią tej samej sieci.

7. Kliknij **Dalej**.
8. Dostarcz odpowiednie poświadczenia VMware vShield dla każdej maszyny vCenter.
9. Podaj sugestywną nazwę dla Security Server.
10. Dla środowisk VMware wybierz kontener, w którym chcesz uwzględnić Security Server z menu **Wdrażaj Kontener**.
11. Wybierz dysk docelowy.
12. Wybierz rodzaj dysku rezerwowego. Jest zalecane aby wdrożyć urządzenie używając dysku rezerwowego.

    WAŻNE
    Jeżeli używasz małego dysku rezerwowego i miejsce na dysku się skończyło, Security Server zamrozi się, w konsekwencji host pozostanie niechroniony.

13. Skonfiguruj pamięć i zasoby procesora alokacji na podstawie wskaźnika konsolidacji VM na hoście. Wybierz **Niskie**, **Średnie** lub **Wysokie** aby załadować zalecane ustawienia alokacji zasobów lub **Ręczne** do konfiguracji zasobów ręcznej alokacji.
14. Należy ustawić hasło administratora dla konsoli Security Server. Ustaw hasło administracyjne nadpisując domyślne hasło ("sve").
15. Ustaw strefę czasową urządzenia.
16. Wybierz typ konfiguracji sieci z sieci Bitdefender. Adres IP Security Server nie może się zmienić w czasie gdy jest używany przez Linuksowych agentów do komunikacji.

    Jeśli zdecydujesz się wybrać DHCP, upewnij się, że skonfigurowałeś serwer DHCP, aby zarezerwował adres IP dla urządzenia.

    Jeżeli wybierzesz statyczne, musisz podać adres IP, maska subnet, bramę i informacje DNS.
17. Wybierz sieć vShield i podaj poświadczenia vShield. Domyślna etykieta dla sieci vShield to `vmservice-vshield-pg`.
18. Naciśnij **Zapisz** aby utworzyć zadanie. Pojawi się nowa wiadomość potwierdzająca.

WAŻNE

- Pakiety Security Server nie są domyślnie dołączone do urządzenia GravityZone. W zależności od ustawień dokonanych przez głównego administratora , pakiety Security Server są niezbędne dla twojego środowiska, które zostanie pobrane gdy rozpocznie się zadanie instalacji Security Server lub administrator zostanie powiadomiony o brakującym obrazi i instalacja się nie rozpocznie. Jeżeli brakuje pakietu, główny administrator powinien ręcznie pobrać go aby instalacja była możliwa.
- Instalowanie Security Server na Nutanix za pomocą zdalnego zadania może się nie powieść, gdy klaster Element Prism jest zarejestrowany w Prism Central lub z innego powodu. W takich sytuacjach zaleca się ręczne wdrożenie Security Server. Więcej szczegółów znajdziesz w tym artykule KB.

19. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Odinstaluj Security Server

Aby odinstalować Security Server:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz centrum danych lub folder zawierający host na którym Security Server jest zainstalowany.
4. Zaznacz pole zawierające host na którym Security Server jest zainstalowany.
5. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Odinstaluj Security Server**.
6. Wprowadź poświadczenia vShield i kliknij **Tak** aby utworzyć zadanie.
7. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

Aktualizuj Security Server

Aby zaktualizować Security Server:

1. Przejdź do strony **Sieć**.

2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Zaznacz host na którym ma być zainstalowany Security Server.

   Aby łatwo zlokalizować Security Server, możesz użyć menu **Filtry** według poniższych:

   - Przejdź do zakładki **Bezpieczeństwo** i wybierz tylko **Serwer bezpieczeństwa**.
   - Przejdź do zakładki **Głębokość** i wybierz **Wszystkie elementy rekursywanie**.

   Notatka
   Jeżeli używasz narzędzia zarządzania wirtualizacją, które nie jest obecnie zintegrowane z Control Center, Security Server zostanie umieszczony w **Grupy Niestandardowe**.
   Aby uzyskać więcej informacji na temat wspieranych platform wirtualizacji zapoznaj się z Podręcznikiem Instalacyjnym GravityZone.

4. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Aktualizacje Security Server**.
5. Czynności należy potwierdzić, klikając **Tak**.
6. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „Przeglądanie i zarządzanie zadaniami” (p. 206).

WAŻNE
Zaleca się skorzystać z tej metody, aby zaktualizować Security Server przez NSX, w przeciwnym razie kwarantanny zapisane na urządzeniu zostaną usunięte.

Zainstaluj Pakiet Uzupełniający HVI

Aby chronić maszyny wirtualne z HVI musisz zainstalować pakiet uzupełniający na hoście. Rolą tego pakietu jest zapewnienie komunikacji między hypervisor'em i Security Server zainstalowanym na hoście. Po zainstalowaniu HVI chroni maszyny wirtualne, które mają włączony HVI w polityce.

WAŻNE

- HVI chroni wyłącznie maszyny wirtualne na hypervisor'ach Citrix Xen.
- Nie musisz odinstalowywać istniejącego agenta bezpieczeństwa z maszyn wirtualnych.

Aby zainstalować pakiet uzupełniający na hoście:

1. Przejdź do strony **Konfiguracja > Aktualizacja**.
2. Wybierz Pakiet Uzupełniający HVI z listy **Komponenty** i kliknij przycisk **Pobierz** w górnej części tabeli.
3. Przejdź do strony **Sieć** i wybierz **Maszyny Wirtualne** z selektora widoków.
4. Wybierz **Serwer** z menu **Widoki** w lewym panelu.
5. Wybierz jeden lub więcej hostów Xen z inwentaryzacji sieci. Możesz łatwo zobaczyć dostępne hosty zaznaczając opcję **Wpisz > Hosty** z menu **Filtry**.
6. Kliknij przycisk **Zadania** po prawej stronie panelu i wybierz **Zainstaluj Pakiet Uzupełniający HVI**. Otwiera się okno instalacyjne.
7. Zaplanuj kiedy zadanie instalacyjne powinno się rozpocząć. Możesz wybrać czy uruchomić zadanie natychmiast po zapisaniu zadania, czy w określonym czasie. W przypadku, gdy instalacja nie może zostać wykonana w określonym czasie, zadanie automatycznie powtarza się zgodnie z ustawieniami powtarzania. Na przykład, jeśli zaznaczyłeś więcej hostów i jeden host nie jest dostępny, gdy pakiet jest zaplanowany do instalacji, zadanie zostanie uruchomione ponownie w określonym czasie.
8. Host musi zostać zrestartowany, aby zastosować zmiany i zakończyć instalację. Jeśli chcesz restartować hosta bez nadzoru, zaznacz **Automatyczny restart(jeśli potrzebny)**.
9. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**.

Odinstaluj Pakiet Uzupełniający HVI

Aby odinstalować pakiet uzupełniający z hostów:

1. Przejdź do strony **Sieć** i wybierz **Maszyny Wirtualne** z selektora widoków.
2. Wybierz **Serwer** z menu **Widoki** w lewym panelu.
3. Wybierz jeden lub więcej hostów Xen z inwentaryzacji sieci. Możesz łatwo zobaczyć dostępne hosty zaznaczając opcję **Wpisz > Hosty** z menu **Filtry**.
4. Kliknij przycisk **Zadania** po prawej stronie panelu i wybierz **Zainstaluj Pakiet Uzupełniający HVI**. Otwiera się okno konfiguracji.

5. Zaplanuj czas usunięcia pakietu. Możesz wybrać czy uruchomić zadanie natychmiast po zapisaniu zadania, czy w określonym czasie. W przypadku, gdy deinstalacja nie może zostać wykonana w określonym czasie, zadanie automatycznie powtarza się zgodnie z ustawieniami powtarzania. Na przykład, jeśli zaznaczyłeś więcej hostów i jeden host nie jest dostępny, gdy pakiet jest zaplanowany do deinstalacji, zadanie zostanie uruchomione ponownie w określonym czasie.
6. Host musi się zresetować aby ukończyć usuwanie. Jeśli chcesz restartować hosta bez nadzoru, zaznacz **Automatyczny restart(jeśli potrzebny)**.
7. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**.

Aktualizuj Pakiet Uzupełniający HVI

Aby aktualizować pakiet uzupełniający z hostów:

1. Zainstaluj najnowszy dostępny Pakiet Uzupełniający HVI.

   Aby uzyskać więcej informacji, odwołaj się do „Zainstaluj Pakiet Uzupełniający HVI” (p. 158).
2. Przejdź do strony **Sieć**.
3. Wybierz **Maszynę Wirtualną** z selektora widoku.
4. Wybierz **Serwer** z menu **Widoki** w lewym panelu.
5. Wybierz jeden lub więcej hostów Xen z inwentaryzacji sieci.

   Możesz łatwo zobaczyć dostępne hosty zaznaczając opcję **Wpisz > Hosty** z menu **Filtry**.
6. Kliknij przycisk **Zadania** po prawej stronie panelu i wybierz **Zainstaluj Pakiet Uzupełniający HVI**. Otwiera się okno konfiguracji.
7. Zaplanuj czas aktualizacji pakietu. Możesz wybrać czy uruchomić zadanie natychmiast po zapisaniu zadania, czy w określonym czasie.

   W przypadku, gdy aktualizacja nie może zostać wykonana w określonym czasie, zadanie automatycznie powtarza się zgodnie z ustawieniami powtarzania. Na przykład, jeśli zaznaczyłeś więcej hostów i jeden host nie jest dostępny, gdy pakiet jest zaplanowany do aktualizacji, zadanie zostanie uruchomione ponownie w określonym czasie.

8. Zaznacz **Automatycznie uruchom ponownie (jeśli trzeba)** jeśli chcesz ponownie uruchomić hosta bez nadzoru. W przeciwnym wypadku musisz ręcznie zrestartować hosta aby zastosować aktualizacje.
9. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

Możesz również śledzić status zadania na stronie **Sieć > Zadania**.

Wstaw Narzędzie Niestandardowe

Aby wstrzyknąć narzędzia do wnętrza systemu operacyjnego:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
4. Zaznacz pola wyboru docelowych punktów końcowych.
5. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Wstrzyknij Narzędzie Niestandardowe**. Wyświetlono okno konfiguracji.
6. Z rozwijanego menu wybierz wszystkie narzędzia, które chcesz wstrzyknąć. Dla każdego wybranego narzędzia zostanie wyświetlona sekcja z jego ustawieniami.

   Narzędzia te zostały wcześniej przesłane do GravityZone. Jeśli nie znajdziesz odpowiedniego narzędzia na liście, przejdź do **Centrum Zarządzania Narzędziami** i dodaj go z tego poziomu. Aby uzyskać więcej informacji, zapoznaj się z „Iniekcja Narzędzi Niestandardowych z HVI” (p. 483).
7. Dla każdego narzędzia wyświetlonego w oknie:
   a. Kliknij nazwę narzędzia, aby zobaczyć lub ukryć jego sekcje.
   b. Wpisz wiersz polecenia narzędzia, wraz z wszystkimi potrzebnymi parametrami wejściowymi, podobnie jak w Wierszu Polecenia lub w Terminalu. Na przykład:

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

      W przypadku Narzędzi Naprawczych BD można wybrać tylko działanie naprawcze i działanie zaradcze kopii zapasowych z obu rozwijanych menu.
   c. Wskaż lokalizację, z której serwer Security Server powinien zbierać dzienniki:

- **stdout**. Zaznacz to pole wyboru, aby przechwycić dzienniki ze standardowego kanału komunikacyjnego.
- **Plik wyjściowy**. Zaznacz to pole wyboru, aby zebrać plik dziennika zapisany w punkcie końcowym. W tym przypadku należy wprowadzić ścieżkę, na której Security Server może odnaleźć plik. Możesz używać ścieżek bezwzględnych lub zmiennych systemowych.

  Tutaj masz dodatkową opcję: **Usuń pliki dziennika z Gościa po ich przesłaniu**. Zaznacz pliki, których nie potrzebujesz w punkcie końcowym.

8. Jeśli chcesz przenieść plik dzienników z Security Server do innej lokalizacji, musisz podać ścieżkę do miejsca docelowego i dane uwierzytelniające.
9. Czasami narzędzie może wymagać dłuższego czasu niż oczekiwano, aby zakończyć pracę lub może przestać reagować. Aby uniknąć awarii w takich sytuacjach, w sekcji **Konfiguracja Bezpieczeństwa** wybierz, po upływie jakiego czasu Security Server powinien automatycznie zakończyć proces.
10. Kliknij **Zapisz**.

    Stan zadania można zobaczyć na stronie **Zadania**. Aby uzyskać więcej informacji, możesz też sprawdzić raport **status wstrzyknięcia zewnętrznego HVI**.

6.3.6. Tworzenie szybkich raportów

Możesz wybrać żeby stworzyć błyskawiczne raporty na temat zarządzanych wirtualnych maszyn począwszy od strony **Sieć**:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie maszyny wirtualne z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Filtruj zawartość wybranych grup tylko zarządzanych przez wirtualne maszyny.
5. Zaznacz pola odpowiadające wirtualnym maszynom które chcesz żeby były zawarte w raporcie.
6. Kliknij przycisk **Raport** w górnej części tabeli i wybierz rodzaj raportu z menu. Aby uzyskać więcej informacji, odwołaj się do „Komputer i Raporty Wirtualnej Maszyny” (p. 416).

7. Konfiguracja opcji raportu. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie raportów” (p. 435)
8. Kliknij **Wygeneruj**. Raport jest natychmiast wyświetlony. Czas wymagany do utworzenia raportów uzależniony jest od liczby wybranych maszyn wirtualnych.

6.3.7. Przypisywanie polityk

Możesz zarządzać ustawieniami bezpieczeństwa na maszynach wirtualnych używając polityk.

Na stronie **Sieć** możesz zobaczyć zmiany i przypisane polityki dla każdej maszyny wirtualnej lub grupy maszyn wirtualnych.

Notatka
Ustawienia bezpieczeństwa są dostępne wyłącznie dla zarządzanych maszyn wirtualnych. Aby ułatwić przeglądanie i zarządzanie ustawieniami bezpieczeństwa, możesz filtrować inwentarz sieci jedynie przez zarządzane maszyny wirtualne.

Aby wyświetlić ustawienia zabezpieczeń stosowanych w danej maszyny wirtualnej:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie maszyny wirtualne z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Naciśnij nazwę wirtualnej maszyny, która Cię interesuje. Pojawi się okno informacyjne.
5. W zakładce **Ogólne**, w sekcji **Polityki**, kliknij nazwę obecnej polityki, aby zobaczyć jej ustawienia.
6. Możesz zmienić ustawienia bezpieczeństwa jakie potrzebujesz, pod warunkiem, że właściciel polityki zezwala użytkownikom na wprowadzenie zmian w tej polityce. Pamiętaj, że wszystkie wprowadzone zmiany będą miały wpływ na wszystkie maszyny wirtualne przypisane do tej samej polityki.

   Aby uzyskać informacje na temat ustawień polityk maszyn wirtualnych, zapoznaj się z„Polityki Bezpieczeństwa” (p. 218)

Aby przypisać politykę do wirtualnej maszyny lub grupy maszyn wirtualnych:

1. Przejdź do strony **Sieć**.

2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie maszyny wirtualne z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
4. Wybierz pole wyboru pożądanej jednostki. Możesz wybrać jeden z kilku obiektów tego samego rodzaju tylko tego samego poziomu.
5. Kliknij przycisk **Przypisz Polityki** w górnej części tabeli.
6. Dokonaj niezbędnych ustawień w oknie **Przypisanie polityki**.

   Aby uzyskać więcej informacji, odwołaj się do „Przypisywanie polityk” (p. 222).

Ostrzeżenie
W przypadku polityk z włączoną funkcją [HVI_ LONG], maszyny docelowe mogą wymagać ponownego uruchomienia komputera po przypisaniu polityki. Maszyny w tym stanie są oznaczone w zakładce **Sieci** z ikoną **Do czasu ponownego uruchomienia**.

6.3.8. Korzystanie z Menedżera Odzyskiwania dla Zaszyfrowanych Woluminów

Gdy użytkownicy zapomną swoich haseł szyfrowania i nie mogą uzyskać dostępu do zaszyfrowanych dysków, możesz im pomóc odzyskując klucze ze strony **Sieć**

Aby pobrać klucz odzyskiwania:

1. Przejdź do strony **Sieć**.
2. Kliknij **Menedżer Odzyskiwania** w pasku narzędzi po lewej stronie. Pojawi się nowe okno.
3. W sekcji **Identyfikator** wprowadź następujące dane:
   a. ID klucza odzyskiwania zaszyfrowanego woluminu. ID klucza odzyskiwania jest ciągiem cyfr i liczb dostępnym na punkcie końcowym na ekranie odzyskiwania Bitlockera.

      Na Windows, ID klucza odzyskiwania jest ciągiem cyfr i liczb dostępnym na punkcie końcowym na ekranie odzyskiwania Bitlockera.

      Możesz także użyć opcji **Odzyskiwanie** w zakładce **Ochrona** we właściwościach maszyny wirtualnej aby automatycznie wprowadzić ID

klucza odzyskiwania, zarówno dla punktów końcowych z Windows jak i macOS.

b. Hasło do twojego konta GravityZone.

4. Kliknij **Ujawnij**. Okno się rozwija.

   W **Informacjach o Woluminie** znajdziesz następujące dane:

   a. Nazwa woluminu

   b. Typ woluminu (rozruchowy lub nierozruchowy).

   c. Nazwa punktu końcowego (wymieniona w Zasobach Sieci)

   d. Klucz Odzyskiwania. Na Windows, klucz odzyskiwania jest hasłem automatycznie generowanym podczas szyfrowania woluminu. Dla Mac, klucz odzyskiwania jest jednocześnie hasłem użytkownika.

5. Wyślij klucz odzyskiwania do użytkownika.

Szczegółowe informacje o szyfrowaniu i odszyfrowywaniu woluminów przy użyciu GravityZone znajdują się w „Szyfrowanie” (p. 381).

6.3.9. Czyszczenie Licencji

W ekwipunku Active Directory, vCenter(bez vShielda, NSX lub HVI) i Xen Server, możesz z łatwością zwolnić miejsca w licencji użyte przez maszyny wirtualne gdzie agent bezpieczeństwa został usunięty bez korzystania z deinstalatora.

Po tym jak to zrobisz, maszyny które są celem, stają się nie zarządzane w panelu Sieci.

Aby zwolnić miejsce w licencji:

1. Przejdź do strony **Sieć**.
2. Zaznacz **Komputery i Maszyny Wirtualne** lub **Maszyny Wirtualne** z selektora widoku
3. Wybierz pożądaną grupę z lewego panelu. Wszystkie maszyny wirtualne zostaną wyświetlone po prawej stronie tabeli.
4. Zaznacz maszynę wirtualną, z której chcesz usunąć licencje.
5. Kliknij przycisk ⊖ **Wyczyść licencję** w górnej części tabeli.
6. Kliknij **Tak** w oknie potwierdzenia, aby kontynuować.

6.4. Urządzenia mobilne

Aby zarządzać bezpieczeństwem dla urządzeń mobilnych używanych w twojej firmie, musisz w pierwszej kolejności połączyć je z konkretnymi użytkownikami w Control Center, nastepnie zainstalować i aktywować aplikację GravityZone Mobile Client na każdym z nich.

Urządzenia przenośne mogą być własnością przedsiębiorstwa lub osoby prywatnej. Możesz zainstalować i aktywować GravityZone Mobile Client na każdym urządzeniu przenośnym, następnie przekazać do odpowiedniego użytkownika. Użytkownicy mogą również sami instalować i aktywować GravityZone Mobile Client według instrukcji wysłanych na maila. Aby uzyskać więcej informacji zapoznaj się z Instrukcją Instalacyjną GravityZone.

Aby zobaczyć urządzenia przenośne użytkownika przypisane do twojego konta, przejdź do sekcji **Sieć** i wybierz **Komputery** z selektora usług. Strona **Sieć** wyświetla dostępne grupy użytkowników w lewym panelu i odpowiednich użytkowników i urządzeń w prawym panelu.

Jeżeli integracja z Active Directory jest skonfigurowana, możesz dodać urządzenia przenośne do istniejących użytkowników Active Directory. Możesz również stworzyć użytkowników w **Grupa Niestandardowa** i dodać urządzenie przenośne do nich.

Możesz przełączyć widok prawego bocznego panelu na **Użytkownicy** lub na **Urządzenia** za pomocą zakładki **Widok** z menu **Filtry** znajdującego się w górnej części tabeli. Widok **Użytkownicy** pozwala na zarządzanie użytkownikami w Control Center, takimi jak dodawanie użytkowników i urządzeń mobilnych przez sprawdzanie numerów urządzeń od każdego użytkownika. Wyświetl **Urządzenie** aby łatwo zarządzać i sprawdzać szczegóły każdego urządzenia przenośnego w Control Center.

Możesz zarządzać użytkownikami i urządzeniami przenośnymi w Control Center poprzez:

- Dodaj niestandardowych użytkowników.
- Dodaj urządzenia mobilne do użytkowników.
- Organizuj niestandardowych użytkowników w grupy
- Filtru i wyszukuj użytkowników i urządzenia
- Sprawdzaj użytkownika lub status urządzenia i szczegóły
- Uruchom zadanie na urządzeniach mobilnych
- Utwórz szybkie raporty urządzeń mobilnych
- Sprawdź i zmień ustawienia bezpieczeństwa urządzeń.
- Synchronizuj inwentarz Control Center z Active Directory

- Usuń użytkowników i urządzenia mobilne

6.4.1. Dodawanie niestandardowych użytkowników.

Jeżeli integracja z Active Directory jest skonfigurowana, możesz dodać urządzenia przenośne do istniejących użytkowników Active Directory.

W sytuacji gdy nie ma przynależności do Active Directory, musisz najpierw stworzyć niestandardowego użytkownika w celu oznaczenia właścicieli do identyfikacji urządzeń przenośnych.

Istnieją dwa sposoby tworzenia użytkowników niestandardowych. Możesz dodawać je pojedynczo lub zaimportować plik CSV.

Dodaj niestandardowego użytkownika:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektora usług
3. Kliknij menu **Filtry** z górnej strony tabeli i przejdź do zakładki **Widok**. Upewnij się, że opcja **Użytkownik** została wybrana.
4. W panelu po lewej stronie **Niestandardowe Grupy**.
5. Kliknij przycisk **Dodaj użytkownika** z górnej strony tabelki. Wyświetlone zostanie okno konfiguracji.
6. Określ szczegóły wymaganego użytkownika:
   - sugestywna nazwa użytkownika (np. pełna nazwa użytkownika)
   - Adres e-mail użytkownika

   WAŻNE
   - Upewnij się, że podano poprawny adres e-mail. Użytkownik dostanie instrukcje instalacyjne na maila, po dodaniu urządzenia.
   - Każdy adres e-mail może być połączony tylko z jednym użytkownikiem.

7. Kliknij **OK**.

Aby zaimportować użytkowników urządzeń mobilnych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektora usług

3. Kliknij menu **Filtry** z górnej strony tabeli i przejdź do zakładki **Widok**. Upewnij się, że opcja **Użytkownik** została wybrana.
4. W panelu po lewej stronie **Niestandardowe Grupy**.
5. Kliknij **Importuj użytkowników**. Otworzy się nowe okno.
6. Wybierz plik CSV i kliknij **Importuj**. Okno zostanie zamknięte, a tabela wypełni się zaimportowanymi użytkownikami.

> **Notatka**
> W przypadku wystąpienia błędów, wyświetlany jest komunikat, a tabela jest wypełniana tylko ważnymi użytkownikami. Istniejący użytkownicy są pomijani.

Następnie możesz Stworzyć grupy użytkowników w **Grupy Niestandardowe**.

Polityka i zadania przypisane do użytkownika zostaną zastosowane do wszystkich urządzeń należących do wybranego użytkownika.

6.4.2. Dodawanie urządzeń przenośnych do użytkowników

Użytkownik może mieć nieskończoną liczbę urządzeń przenośnych. Możesz dodać urządzenie do jednego lub większej ilości użytkowników, ale tylko jedno urządzenie dla każdego użytkownika w danym czasie.

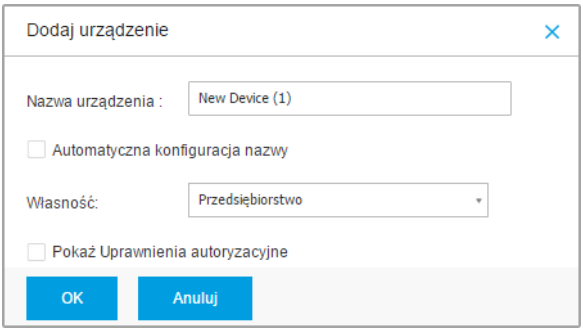
Dodawanie urządzenia do pojedynczego użytkownika

Aby dodać urządzenie do konkretnego użytkownika:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Zlokalizuj użytkownika wewnątrz grupy **Active Directory** lub w **Grupy Niestandardowe** i zaznacz odpowiednie pole w prawym panelu bocznym.

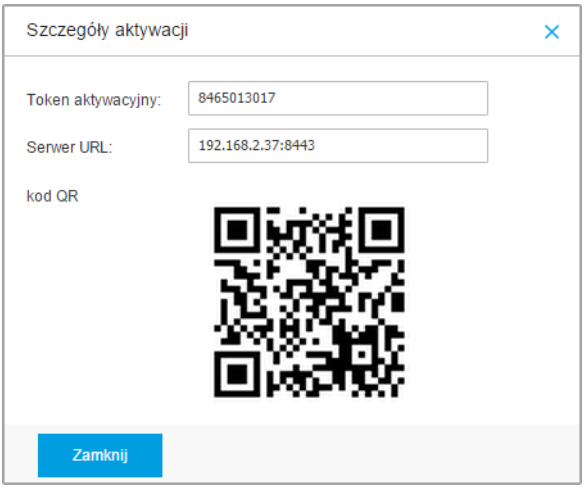
> **Notatka**
> **Filtry** muszą być ustawione w **Użytkownicy** w zakładce **Wyświetl**.

4. Kliknij przycisk **Dodaj Urządzenie** z górnej strony tabeli. Wyświetlone zostanie okno konfiguracji.



Dodaj urządzenie mobilne do użytkownika.

5. Konfiguruj szczegóły urządzenia przenośnego:
   a. Podaj sugestywną nazwę dla urządzenia.
   b. Użyj opcji **Automatyczna konfiguracja nazwy** jeśli chcesz aby nazwa była automatycznie generowana. kiedy dodajesz urządzenia ma wygenerowaną nazwę. Kiedy urządzenie jest włączone, automatycznie zmienia nazwę z odpowiednimi informacjami producenta i modelu.
   c. Wybierz rodzaj własności urządzenia (Enterprise lub Personal). Możesz w każdej chwili odfiltrować urządzenia przenośne po właścicielu i zarządzać nimi według swoich potrzeb.
   d. Zaznacz opcje **Pokaż poświadczenia aktywacyjne** jeżeli instalujesz GravityZone Mobile Client na urządzeniu użytkownika.
6. Naciśnij **OK** aby dodać nowe urządzenie. Użytkownik niezwłocznie dostanie wiadomość e-mail z instrukcjami dotyczącymi instalacji i szczegółami aktywacji do konfiguracji urządzenia przenośnego. Szczegóły aktywacyjne zawierają token aktywacyjny i adres serwera komunikacyjnego (i odpowiedni QR kod).
7. Jeżeli wybrałeś opcje **Wyświetl poświadczenia aktywacji** pojawi się okna **Szczegóły Aktywacji**, pokazując unikalny token, adres serwera komunikacji i odpowiedni kod QR dla nowych urządzeń.



Szczegóły aktywacji urządzenia przenośnego

Po instalacji GravityZone Mobile Client, gdy pojawi się monit aby aktywować urządzenie, naciśnij token aktywacyjny i adres serwera komunikacji lub zeskanuj kod QR.

Dodawanie urządzeń do wielu użytkowników

Dodaj urządzenie przenośne do wybranych użytkowników i grup:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Ulokuj użytkowników lub grupy w folderze **Active Directory** lub **Grupy Niestandardowe** i zaznacz odpowiednie pole w prawym panelu.

> **Notatka**
> **Filtry** muszą być ustawione w **Użytkownicy** w zakładce **Wyświetl**.

4. Naciśnij przycisk **Dodaj urządzenie** po prawej stronie tabeli. W tym przypadku, musisz zdefiniować w oknie konfiguracyjnym wyłącznie własność urządzenia.

   Jeżeli będą użytkownicy z nieokreślonym adresem e-mail, zostaniesz niezwłocznie powiadomiony. Lista odpowiednich użytkowników będzie dostępna w obszarze **Powiadomienia** w Control Center.

Urządzenia przenośne stworzone przez wielokrotną selekcje mają domyslną nazwę rodzajową w Control Center. Kiedy urządzenie jest włączone, automatycznie zmienia nazwę z odpowiednimi informacjami producenta i modelu.

5. Naciśnij **OK** aby dodać nowe urządzenia. Użytkownicy niezwłocznie dostaną wiadomość e-mail z instrukcjami dotyczącymi instalacji i szczegółami aktywacji do konfiguracji urządzenia przenośnego. Szczegóły aktywacyjne zawierają token aktywacyjny i adres serwera komunikacyjnego (i odpowiedni QR kod).

Możesz sprawdzić liczbę przypisanych urządzeń do każdego użytkownika w prawym panelu, w kolumnie **Urządzenia**.

6.4.3. Organizowanie niestandardowych użytkowników w grupy

Możesz zobaczyć dostępne grupy użytkowników w lewym panelu strony **Siec**.

Użytkownicy Active Directory są zgrupowani w **Active Directory**. Nie możesz edytować grup Active Directory. Możesz tylko wyświetlić i dodać urządzenia dla danych użytkowników.

Możesz umieścić użytkowników nie należących do Active Directory do **Grupy Niestandardowe**, możesz stworzyć i zorganizować grupy jak chcesz. Główną zaletą jest to, że możesz korzystać z polityk grupy w celu spełnienia różnych wymogów bezpieczeństwa.

W **Niestandardowe Grupy** możesz utworzyć, usunąć, zmienić nazwę i przesunąć grupy użytkowników w ramach zdefiniowanej niestandardowej struktury drzewa.

WAŻNE
Proszę zwrócić uwagę na następujące:

- Grupa może zawierać zarówno użytkowników jak i inne grupy.
- Kiedy wybierasz grupę w lewym panelu, możesz zobaczyć wszystkich użytkowników z wyjątkiem tych umieszczonych w podgrupach. Aby zobaczyć wszystkich użytkowników zawartych w grupie i swoich podgrupach kliknij menu **Filtry** zlokalizowane z górnej strony tabeli i wybierz **Wszystkie elementy rekurencyjnie** w sekcji **Głębokość**.

Tworzenie grup

Aby utworzyć niestandardową grupę:

1. Wybierz **Niestandardowe Grupy** w lewym panelu.

2. Naciśnij przycisk ⊕ **Dodaj grupę** u góry lewego panelu bocznego.
3. Podaj sugestywna nazwę dla grupy i naciśnij **OK**. Nowa grupa wyświetli się w **Grupy Niestandardowe**.

Zmienianie nazw grup

Aby zmienić nazwę niestandardowej grupy:

1. Wybierz grupę z lewego panelu bocznego.
2. Naciśnij przycisk ✎ **Edytuj grupę** u góry lewego panelu bocznego.
3. Wprowadź nową nazwę w odpowiednim polu.
4. Kliknij **OK**, aby potwierdzić.

Przesuwanie grup i uzytkowników

Możesz przesunąć grupy i użytkowników gdziekolwiek wewnątrz hierarchii **Niestandardowe Grupy**. Aby przesunąć grupę lub użytkownika, przeciągnij i upuść go do nowej lokacji.

Notatka

Ten wpis został przeniesiony, odziedziczy ustawienia polityki nowej grupy macierzystej, chyba że dziedziczona polityka została wyłączona i inne licencje zostały przypisane do niego.

Usuwanie grup

Grupa nie może zostać usunięta jeżeli należy do niej przynajmniej jeden użytkownik. Przenieś wszystkich użytkowników z grupy, którą chcesz usunąć do innej grupy. Jeżeli grupa zawiera podgrupy, możesz przenieść wszystkie podgrupy, a nie indywidualnych użytkowników.

Aby usunąć grupę:

1. Wybierz pustą grupę.
2. Naciśnij przycisk ⊗ **Usuń grupę** u góry lewego panelu bocznego. Czynności należy potwierdzić, klikając **Tak**.

6.4.4. Sprawdzanie Statusu Urządzeń Mobilnych

Każde urządzenie mobilne jest reprezentowane na stronie sieci jako ikona określająca swój typ i status.

Odnieś się do „Typy obiektów sieciowych i statusy” (p. 514) dla listy ze wszystkimi dostępnymi typami ikon i statusów.

Urządzenia przenośne, mogą mieć następujące statusy zarządzania:

- **Zarządzane (Aktywne)**, kiedy wszystkie warunki są spełnione:
  - GravityZone Mobile Client jest aktywny na urządzeniu.
  - GravityZone Mobile Client został zsynchronizowany z Control Center w ciągu ostatnich 48 godzin.
- **Zarządzane (Bezczynne)**, kiedy wszystkie warunki są spełnione:
  - GravityZone Mobile Client jest aktywny na urządzeniu.
  - GravityZone Mobile Client nie został zsynchronizowany z Control Center w przeciągu ponad 48 godzin.
- **Niezarządzane**, w poniższych sytuacjach:
  - GravityZone Mobile Client nie został jeszcze zainstalowany i aktywowany na urządzeniu przenośnym.
  - GravityZone Mobile Client został odinstalowany z urządzenia przenośnego (tylko dla urządzeń Android).
  - Profil MDM Bitdefender został usunięty z urządzenia przenośnego (tylko dla urządzeń iOS).

Aby sprawdzić status zarządzania urządzeń:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. W lewym panelu, wybierz grupę, która Cie interesuje.
4. Kliknij menu **Filtry** zlokalizowane z górnej strony tabeli i dokonaj następujących ustawień:
   a. Przejdź do zakładki **zobacz** i wybierz **Urządzenie**.
   b. Przejdź do zakładki **Bezpieczeństwo** i wybierz status jaki Cie interesuje w sekcji **Zarządzanie**. Możesz wybrać jeden lub kilka kryteriów filtrów w tym samym czasie.
   c. Możesz dodatkowo wybrać, żeby zobaczyć wszystkie urzadzenia rekursywnie, przez wybieranie odpowiednich opcji w zakładce **Głębokość**.

d. Kliknij **Zapisz**.

Wszystkie urządzenia mobilne przypisane do wybranych kryteriów wyświetlą się w tabeli.

Możesz wygenerować raport stanu synchronizacji urządzenia na jednym albo kilku urządzeniach przenośnych. Ten raport zawiera szczegółowe informacje o stanie synchronizacji każdego wybranego urządzenia, w tym datę i czas ostatniej synchronizacji. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie szybkich raportów" (p. 188)

6.4.5. Skompilowane i nieskompilowane urządzenia przenośne

Aplikacja GravityZone Mobile Client zostanie aktywowana na urządzeniu przenośnym, Control Center sprawdzi czy odpowiednie urządzenie spelnia wszystkie wymogi jakościowe. Urządzenia przenośne, mogą mieć następujące statusy bezpieczeństwa:

- **Pomiń kwestie bezpieczeństwa** , kiedy wszystkie wymagania są spełnione.
- **Z kwestiami Bezpieczeństwa**, kiedy przynajmniej jeden z wymogów nie jest spełniony. Kiedy urządzenie jest niezgodne, uzytkownik jest proszony, aby rozwiązać problem zgodności. Użytkownik musi wykonać wymaganych zmian w określonym czasie, w przeciwnym razie zostanie zastosowana akcja dla urządzeń niezgodnych, zdefiniowana w polityce która zostanie zastosowana.

  Aby uzyskać więcej informacji o niezgodnych działaniach i kryteriach, odwołaj się do „Zgodność" (p. 396).

Aby sprawdzić status zgodności urządzeń:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. W lewym panelu, wybierz grupę, która Cie interesuje.
4. Kliknij menu **Filtry** zlokalizowane z górnej strony tabeli i dokonaj następujących ustawień:
   a. Przejdź do zakładki **zobacz** i wybierz **Urządzenie**.
   b. Przejdź do zakładki **Bezpieczeństwo** i wybierz status jaki Cie interesuje w sekcji **Kwestie Bezpieczeństwa**. Możesz wybrać jeden lub kilka kryteriów filtrów w tym samym czasie.

c. Możesz dodatkowo wybrać, żeby zobaczyć wszystkie urzadzenia rekursywnie, przez wybieranie odpowiednich opcji w zakładce **Głębokość**.

d. Kliknij **Zapisz**.

Wszystkie urządzenia mobilne przypisane do wybranych kryteriów wyświetlą się w tabeli.

5. Możesz zobaczyć współczynnik zgodności urządzenia dla każdego użytkownika:

a. Kliknij menu **Filtry** zlokalizowane w górnej części tabeli i wybierz **Użytkowników** z kategorii **Widok**. Wszyscy użytkownicy wybranej grupy zostaną wyświetleni w tabeli.

b. Naciśnij kolumne **Zgodnośc** aby zobaczyć jak wiele urządzeń jest zgodnych wśród wszystkich urządzeń posiadanych przez użytkownika.

Możesz wygenerować raport stanu zgodności urządzenia na jednym albo kilku urządzeniach przenośnych. Ten raport dostarcza szczegółowych informacji na temat stanu zgodności z każdym wybranym urządzeniu, w tym nieprzestrzegania powodu zgodności. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie szybkich raportów” (p. 188)

6.4.6. Sprawdzanie szczegółów Użytkownik i urządzeń przenośnych

Możesz uzyskac szczegółowe informacje o każdym użytkowniku urządzenia przenośnego na stornie **Sieć**.

Sprawdzanie szczegółów użytkownika

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz żądaną grupę w lewym panelu bocznym.
4. Kliknij menu **Filtry** zlokalizowane w górnej części tabeli, przejdź do zakładki **Widok** i wybierz **Użytkownicy**. Aby rekursywnie wyświetlić użytkowników, przejdź do zakładki **Głębia** i wybierz **Wszystkie elementy rekursywnie**. Kliknij **Zapisz**. Wszyscy użytkownicy wybranej grupy zostaną wyświetleni w tabeli.
5. Sprawdź informacje wyświetlane w kolumnach tabeli dla każdego użytkownika:
   - **Nazwa**. Nazwa użytkownika.

- **urządzenia**. Liczba urządzeń przypisanych do użytkownika. Naciśnij liczbę aby zmienić wyświetlanie **Urządzeń** i wyświetlanie tylko określonych urządzeń.
- **Zgodność**. Stosunek całości zgodnych urządzeń do wszystkich urzadzeń przpisanych do użytkownika. Naciśnij pierwszą wartość aby zmienić wyświetlanie **Urządzeń** i wyświetlanie tylko zgodnych urządzeń.

6. Naciśnij nazwę użytkownika, który Cię interesuje. Pojawi się okno konfiguracji, gdzie możesz zobaczyć i edytować nazwę użytkownika i adres e-mail.

Sprawdzanie Szczegółów Urządzenia

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz żądaną grupę w lewym panelu bocznym.
4. Kliknij menu **Filtry** zlokalizowane z górnej strony tabeli, przejdź do zakładki **Widok** i wybierz **Urządzenia**. Kliknij **Zapisz**. Wszystkie urządzenia należące do użytkowników wybranej grupy zostaną wyświetleni w tabeli.
5. Sprawdź informacje wyświetlane w kolumnach tabeli dla każdego urządzenia:
   - **Nazwa**. Nazwa urządzenia.
   - **Użytkownik**. Nazwa użytkownika zarządzającego określonym urządzeniem.
   - **System operacyjny**. System operacyjny określonego urządzenia
6. Naciśnij nazwę urządzenia żeby wyświetlić więcej szczegółów. Pojawi się okno **Szczegóły Urządzenia Przenośnego**, gdzie będziesz mógł zaznaczyć informacje zgrupowane w zakładkach **Przegląd** i **Szczegóły**:
   - **Ogólne**.
     - **Nazwa**. Nazwa określona podczas dodawania urządzenia w Control Center.
     - **Użytkownik**. Nazwa właściciela urządzenia.
     - **Grupa**. Grupa macierzysta urządzenia przenośnego w zasobach sieci.
     - **System operacyjny**. System operacyjny urządzenia przenośnego.
     - **Własność**. Rodzaj własności urządzenia przenośnego (Enterprise lub Personal).

- **Bezpieczeństwo**.
  - **Wersja programu**. Wersja aplikacji GravityZone Mobile Client zainstalowana na urządzeniu, wykrywa tylko po rejestracji
  - **Polityka**. Polityka aktualnie przypisana do urządzenia przenośnego. Naciśnij nazwę polityki przechodząc do określonej strony **Polityka** i sprawdź ustawienia bezpieczeństwa.

    WAŻNE

    Domyślnie, tylko użytkownik, który stworzył politykę może ją modyfikować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**. Zmiany wprowadzone do polityki będą dotyczyć wszystkich urządzeń przypisanych do odpowiedniej polityki. Aby uzyskać więcej informacji, odwołaj się do „Przypisywanie polityk" (p. 189).

  - **Status licencji**. Informacje o licencji dla określinego urządzenia.
  - **Status zgodności**. Status zgodności jest dostępny dla zarządzanych urządzeń przenośnych. Urządzenie przenośne może być zgodne lub nie.

    Notatka

    Dla nie zgodnych urządzeń przenośnych, ikona powiadomień ! jest wyświetlana. Sprawdź ikonę podpowiedzi aby zobaczyć powód niezgodności.
    Aby uzyskać więcej informacji o zgodności urządzeń mobilnych, odwołaj się do „Zgodność" (p. 396).

  - **Aktywność Malware (ostatnie 24 godziny)** Szybki przegląd zależny od ilości wykrytych malware na danym urządzeniu bieżącego dnia.
  - **hasło blokady**. Unikalne hasło zostanie automatycznie utworzone przy rejestracji urządzenia, które jest używane przez zdalne zabezpieczenie urządzenia (tylko dla urządzeń Android)
  - **Status Szyfrowania**. Niektóre urządzenia z Android 3.0 lub nowszym wspierają funkcję szyfrowania. Sprawdź status szyfrowania w na stronie szczegółów urządzeniu aby znaleźć czy określone urządzenie wspiera funkcję szyfrowania. Jeżeli szyfrowanie będzie wymagane przez politykę na urządzeniu, musisz zobaczyć stan aktywacji szyfrowania.

- **Szczegóły aktywacji**
  - **Kod aktywacyjny**. Unikalny token aktywacyjny przypisany do urządzenia.
  - Adres serwera komunikacyjnego.
  - **kod QR**. Unikalny kod QR zawierający token aktywacyjny i adres serwera komunikacyjnego.
- **Sprzęt komputerowy**. Możesz zobaczyć tutaj informacje sprzętowe urządzenia, dostępne tylko dla zarządzanych (aktywnych) urządzeń. Informacje sprzętowe są sprawdzane co 12 godzin i aktualizowane gdy pojawią się zmiany.

  WAŻNE
  Rozpoczynając od Androida 10, GravityZone Mobile Client nie ma dostępu numeru seryjnego, IMEI, IMSI i adresu MAC urządzenia. Ta restrykcja prowadzi do następujących sytuacji:
  - Jeżeli urządzenie mobilne z zainstalowanym GravityZone Mobile Client zostanie zaktualizowane ze starszej wersji Androida do Androida 10, Control Center wyświetli prawidłowe szczegóły urządzenia. Przed aktualizacją, urządzenia musi mieć najnowszą wersję GravityZone Mobile Client.
  - Jeżeli GravityZone Mobile Client zostanie zainstalowany na urządzeniu z Android 10, Control Center wyświetli niedokładne informacje o urządzeniu w powodu ograniczeń nałożonych przez system operacyjny.

- **Sieć**. Możesz zobaczyć tutaj informacje łączności sieciowej, dostępne tylko dla zarządzanych (aktywnych) urządzeń.

6.4.7. Sortowanie, Filtrowanie i Wyszukiwanie Urządzeń Mobilnych

Tabela zasobów urządzeń przenośnych może obejmować kilka stron, w zależności od liczby użytkowników lub urządzeń (domyślnie na jednej stronie wyświetlanych jest tylko 10 wpisów). Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

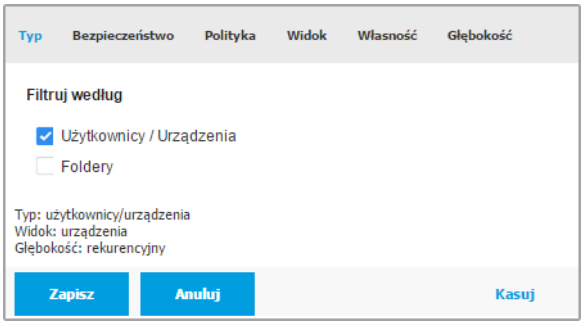
Jeżeli jest zbyt dużo wpisów, możesz użyć opcji filtru aby wyświetlić tylko wpisy, które Cię interesują. Dla przykładu, możesz szukać określonych urządzeń mobilnych lub zobaczyć tylko zarządzane urządzenia.

Sortowanie listy urządzeń mobilnych

Aby posortować dane według określonych kolumn, naciśnij na nagłówek kolumny. Dla przykładu, jeżeli chcesz uporządkować urządzenia według nazwy, kliknij nagłówek **Nazwa**. Jeżeli klikniesz ponownie nagłówek, urządzenia będą wyświetlone w odwrotnej kolejności.

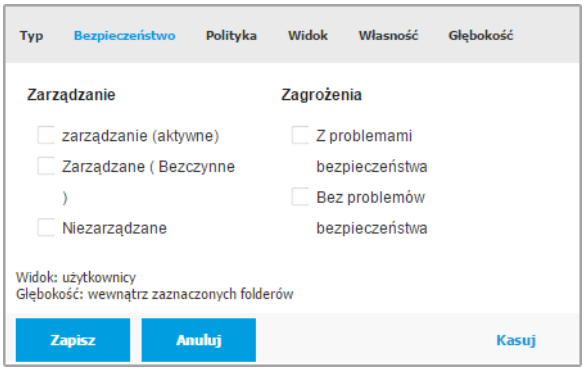
Filtrowanie listy urządzeń mobilnych

1. Wybierz pożądaną grupę z lewego panelu bocznego.
2. Kliknij menu **Filtry**z górnej bocznej strony obszaru panela sieciowego.
3. Wybierz kryteria filtrowania według:
   - **Typ**. Wybierz typ podmiotów, które chcesz wyświetlić (Użytkownicy/Urządzenia i Foldery).



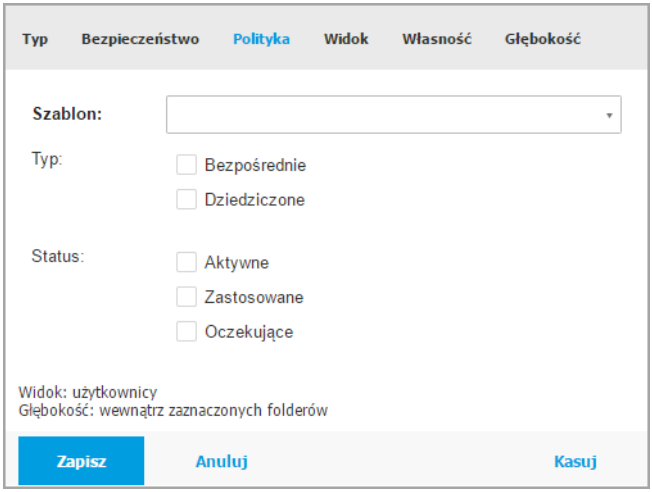
Urządzenia przenośne - Filtruj po Rodzaju

   - **Bezpieczeństwo**. Wybierz aby wyświetlić komputery zarządzane i stan bezpieczeństwa.



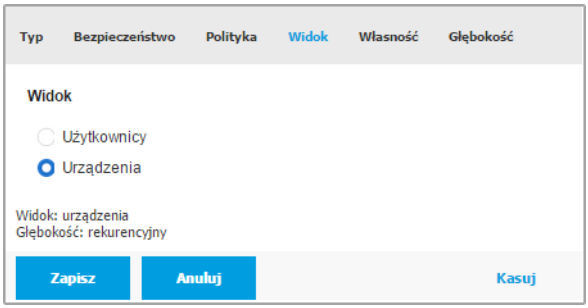
Urządzenia przenośne - Filtruj po Bezpieczeństwie

- **Polityka**. Wybierz szablon polityki jakim chcesz filtrować urządzenia mobilne, rodzaj przypisania typu polityki (Bezpośrednia lub Dziedziczona), jak również status przypisanej polityki (Aktywna, Przypisana lub w Toku).



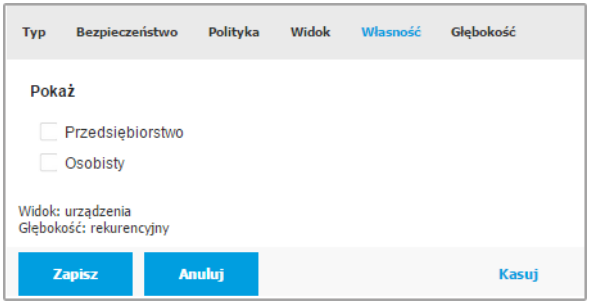
Urządzenia Przenośne - Filtrowanie po Polityce

- **Widok**. wybierz **Użytkownicy** aby wyświetlić tylko użytkowników w wybranej grupie. Wybierz **Urządzenia** aby wyświetlić tylko urządzenia w wybranej grupie.



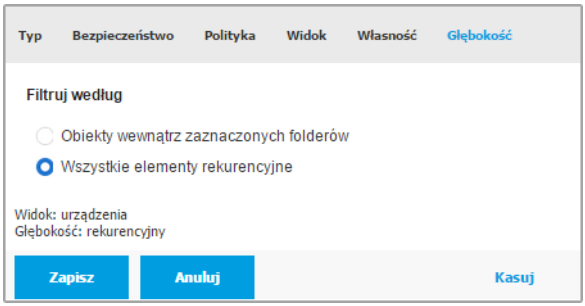
Urządzenia przenośne - Filtrowanie po wyświetlaniu

- **Własność**. Możesz odfiltrować urządzenia mobilne według właściciela wybierając wyświetlenie urządzeń **Przedsiębiorstwo** lub urządzeń **Osobiste**. Atrybut własności określony jest szczegółowo w urządzeniach mobilnych.



Urządzenia Przenośne - Filtrowanie po Właścicielu

- **Głębokość**. Gdy zarządzamy siecią o strukturze drzewa, urządzenia mobilne lub użytkownicy ulokowani w podgrupach nie są wyświetlani podczas wybierania grup źródłowych. Wybierz **Wszystkie elementy rekurencyjnie** aby zobaczyć wszystkie podmioty zawarte w obecnej grupie i jej podgrupach.



Urządzenia Przenośne - Filtrowanie po Głębokości

4. Naciśnij **Zapisz**, aby filtrować listę urządzeń mobilnych według wybranych kryteriów.

   Filtr pozostaje aktywny na stronie **Sieć** dopóki się nie wylogujesz lub nie zrestartujesz filtru.

Wyszukiwanie dla Urządzeń Mobilnych

Prawy panel tabeli zawiera szczegółowe informacje o użytkownikach i urządzeniach mobilnych. Możesz użyc dostepnych kategorii w każdej kolumnie do filtrowania zawartości.

1. Wybierz żądaną grupę w lewym panelu bocznym.
2. Przełącz do wybranego widoku (Użytkownicy i Urządzenia Mobilne) używając **Filtrów** menu z górnej strony obszaru okienka sieciowego.
3. Szukaj pożądanych podmiotów stosując pola wyszukiwarki pod każdym nagłówkiem kolumny z prawej strony panela:
   - Wprowadź pożądany termin wyszukiwania w odpowiednim polu wyszukiwania.

     Dla przykładu, przełącz widok **Urządzenia** i wprowadź nazwę użytkownika, którego szukasz w polu **Użytkownik**. Tylko pasujące urządzenia przenośne pokażą się w tabeli.
   - Wybierz pożądane atrybuty, które chcesz wyszukać w odpowiednim polu rozwijanej listy.

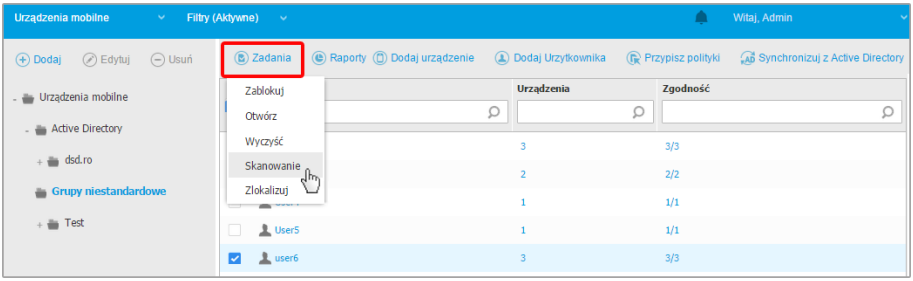
Dla przykładu, przełącz do widoku **Urządzenia**, kliknij z listy pole **System operacyjny** i wybierz **Android** aby wyświetlić tylko urządzenia mobilne z Android.

Notatka
Aby wyczyścić kryterium wyszukiwania i zobaczyć wszystkie wpisy, umieść kursor myszy nad odpowiednim polem i kliknij ikonę ×.

6.4.8. Uruchomienie zadania na urządzeniach mobilnych

Ze strony **Sieć**, możesz zdalnie uruchomić szereg zadań administracyjnych dla urządzeń mobilnych. Oto co możesz zrobić:

- „Zablokuj” (p. 184)
- „Wyczyść” (p. 185)
- „Skanowanie” (p. 186)
- „Zlokalizuj” (p. 187)



Zadania urządzeń przenośnych

Aby uruchomić zdalne zadania na urządzeniach mobilnych, pewne warunki wstępne muszą zostać spełnione. Dla uzyskania większej ilości informacji, zapoznaj się z rozdziałem Wymaganiami Instalacyjnymi z Podręcznika Instalacji GravityZone.

Możesz wybrać aby stworzyć indywidualne zadania dla każdego urządzenia przenośnego, dla każdego użytkownika lub dla grup użytkowników. Na przykład, możesz zdalnie skanować w poszukiwaniu malware urządzenia przenośne grup lub użytkowników. Możesz również uruchomić lokalizacje zadania dla konkretnego urządzenia przenośnego.

Zasoby sieciowe mogą zawierać aktywne, bezczynne lub niezarządzane urządzenia przenośne. Po utworzeniu zadań, od razu uruchomią się na aktywnych urządzeniach przenośnych. Dla bezczynnych urządzeń, zadania rozpoczną się jak tylko wrócą online. Zadania nie zostaną stworzone dla niezarządzanych urządzeń przenośnych. Powiadomienia informujące, że zadanie nie może zostac utworzone wyświetlą się w tym przypadku.

Możesz zobaczyć i zarządzać zadaniami na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do „Przeglądanie i zarządzanie zadaniami” (p. 206).

Zablokuj

Zadanie Blokada, niezwłocznie zablokuje ekran docelowego urządzenia przenośnego Zachowanie zadania Blokada jest uzależnione od systemu operacyjnego:

- Zadanie blokowania dla urządzeń z systemem Android (7.0 lub wyższym) wymusi hasło ustawione w konsoli GravityZone tylko wtedy, gdy na urządzeniu nie skonfigurowano zabezpieczenia blokady. W przeciwnym razie, do zabezpieczenia urządzenia zostaną użyte istniejące opcje blokady ekranu, takie jak Wzór, PIN, Hasło, Odcisk linii papilarnych lub Inteligentna blokada.

  Notatka

  - Hasło blokady ekranu wygenerowane przez Control Center jest wyświetlane w oknie Szczegóły Urządzenia Przenośnego.
  - Zadanie odblokowywania nie jest już dostępne dla urządzeń z systemem Android (7,0 lub wyższym). Zamiast tego, użytkownicy mogą ręcznie odblokować swoje urządzenia. Musisz się najpierw upewnić, ze te urządzenia obsługują wymagania złożoności dla hasła.
  - Z powodu technicznych ograniczeń, zadanie Zablokuj jest niedostępne na Android 11.

- Na iOS, jeżeli urządzenie ma zablokowany ekran hasłem, użytkownik jest proszony o odblokowanie.

Aby zdalnie zablokować urządzenia przenośne:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz pożądaną grupę z lewego panelu bocznego.

4. Kliknij menu **Filtry** z górnej strony obszaru panelu sieciowego i wybierz **Użytkownicy** z kategorii **Widok**. Kliknij **Zapisz**. Wszyscy użytkownicy wybranej grupy zostaną wyświetleni w tabeli.
5. Zaznacz pola wyboru odpowiadające użytkownikom, którymi jesteś zainteresowany. Możesz wybrać jednego lub kilku użytkowników w tym samym czasie.
6. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Zablokuj**.
7. Czynności należy potwierdzić, klikając **Tak**. Wiadomość poinformuje Cię, czy zadanie zostało stworzone.
8. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do „Przeglądanie i zarządzanie zadaniami” (p. 206).

Wyczyść

Zadanie **Wyczyść** przywraca urządzenie przenośne do ustawień fabrycznych. Uruchom to zadanie zdalnie aby usunąć wszystkie wrażliwe informacje i aplikacje wgrane na docelowym urządzeniu przenośnym.

Ostrzeżenie

Ostrożnie używaj zadania **Wyczyść**. Sprawdź właściciela urządzenia docelowego (jeżeli chcesz uniknąć wycierania osobistych urządzeń przenośnie) i upewnij się, że na pewno chcesz wyczyścić wybrane urządzenia. Raz wysłane, zadanie **Wyczyść** nie może zostać odwołane.

Notatka

Z powodu technicznych ograniczeń, zadanie Wyczyść jest niedostępne na Android 11.

Aby zdalnie wyczyścić urządzenie przenośne:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz pożądaną grupę z lewego panelu bocznego.
4. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**. Kliknij **Zapisz**. Wszystkie urządzenia w wybranej grupie są wyświetlane w tabeli.

Notatka
Możesz również wybrać **Wszystkie przedmioty rekursywnie** w sekcji **Głębia** aby zobaczyć wszystkie urządzenia w bieżącej grupie.

5. Zaznacz pola odpowiadające urządzeniom które chcesz wyczyścić.
6. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Wyczyść**.
7. Czynności należy potwierdzić, klikając **Tak**. Wiadomość poinformuje Cię, czy zadanie zostało stworzone.
8. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do „Przeglądanie i zarządzanie zadaniami” (p. 206).

Skanowanie

Zadanie **Skanowanie** pozwala sprawdzić wybrane urządzenia przenośne czy nie posiadają malware. Użytkownik urządzenia jest powiadomiony o wykrytym malware i poproszony o usunięcie. Skanowanie odbywa się w chmurze, dlatego urządzenie musi mieć dostęp do internetu.

Notatka
Zdalne skanowanie nie działa na urządzeniach iOS (ograniczenie platformy).

Aby zdalnie skanować urządzenie przenośne:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz pożądaną grupę z lewego panelu bocznego.
4. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**. Kliknij **Zapisz**. Wszystkie urządzenia w wybranej grupie są wyświetlane w tabeli.

   Notatka
   Możesz również wybrać **Wszystkie przedmioty rekursywnie** w sekcji **Głębia** aby zobaczyć wszystkie urządzenia w bieżącej grupie.
   Aby wyświetlić tylko urządzenia Android w wybranych grupach, idź do nagłówka kolumny **OS** w prawym panelu i wybierz **Android** z odpowiedniego pola listy.

5. Zaznacz pola odpowiadające urządzeniom które mają być zeskanowane.

6. Kliknij przycisk **Zadania** z górnej części tabeli i wybierz **Skanowanie**.
7. Czynności należy potwierdzić, klikając **Tak**. Wiadomość poinformuje Cię, czy zadanie zostało stworzone.
8. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Raport skanowania jest dostępny gdy zadanie zostanie skończone. Naciśnij odpowiednią ikonę w kolumnie **Raporty** aby natychmiastowo wygenerować raport.

   Aby uzyskać więcej informacji, odwołaj się do „Przeglądanie i zarządzanie zadaniami” (p. 206).

Zlokalizuj

Zadanie Zlokalizuj otwiera mapę pokazującą lokalizację wybranych urządzeń. Możesz zlokalizować jedno lub kilka urządzeń w tym samym czasie.

Dla zadania przeznaczonego do pracy, lokalizacja usług musi być włączona na urządzeniach przenośnych.

Aby zlokalizować urządzenia przenośne:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz pożądaną grupę z lewego panelu bocznego.
4. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**. Kliknij **Zapisz**. Wszystkie urządzenia w wybranej grupie są wyświetlane w tabeli.

   Notatka
   Możesz również wybrać **Wszystkie przedmioty rekursywnie** spod sekcji **Głębia** aby zobaczyć wszystkie urządzenia w obecnej grupie.

5. Zaznacz pola odpowiadające urządzeniom które chcesz zlokalizować.
6. Kliknij przycisk **Zadania** z górnej strony tabeli i wybierz **Lokalizuj**.
7. Okno **Lokalizacja** otworzy się, wyświetlając poniższe informacje:
   - Mapa pokazująca pozycje wybranych urządzeń przenośnych. Urządzenie nie jest zsynchronizowane, mapa wyświetli ostatnią znaną lokalizacje.

- Tabela wyświetla szczegóły wybranych urządzeń (nazwa, użytkownik, czas i data ostatniej synchronizacji). Aby zobaczyć mapę lokacji danego urządzenia na liście w tabeli, wybierz jego pole. Mapa wskaże natychmiast lokalizację odpowiedniego urządzenia.
- Opcja **Automatyczne Odświeżanie** automatycznie aktualizuje lokalizacje wybranych urządzeń przenośnych po 10 sekundach.

8. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do „Przeglądanie i zarządzanie zadaniami" (p. 206).

6.4.9. Tworzenie szybkich raportów

Możesz wybrać żeby tworzyć raporty błyskawiczne dla urządzeń przenośnych zaczynając ze strony **Sieć**:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Wybierz pożądaną grupę z lewego panelu.
4. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**. Możesz również wybrać opcje Zarządzane z zakładki **Bezpieczeństwo**, aby filtrować wybrane grupy jedynie zarządzanych urządzeń. Kliknij **Zapisz**. Wszystkie urządzenia spełniające kryteria filtra z wybranej grupy są wyświetlane w tabeli.
5. Wybierz pola wyboru odpowiadających urządzeniom mobilnym, które nas interesują. Możesz wybrać jedno lub kilka urządzeń w tym samym czasie.
6. Kliknij przycisk **Raport** w górnej części tabeli i wybierz rodzaj raportu z menu. Aby uzyskać więcej informacji, odwołaj się do „Raporty Urządzenia Przenośnego" (p. 433)
7. Konfiguracja opcji raportu. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie raportów" (p. 435)
8. Kliknij **Wygeneruj**. Raport jest natychmiast wyświetlony. Czas wymagany do utworzenia raportów uzależniony jest od liczby wybranych urządzeń przenośnych.

6.4.10. Przypisywanie polityk

Możesz zarządzać ustawieniami bezpieczeństwa dla urządzeń mobilnych używając polityk.

W sekcji **Sieć** możesz zobaczyć zmiany i przypisane polityki dla urządzeń przenośnych przypisanych do twojego konta.

Możesz przypisać polityki dla grup, użytkowników lub konkretnych urządzeń przenośnych.

Notatka

Polityka przypisana do użytkownika dotyczy wszystkich urządzeń należących do użytkownika. Aby uzyskać więcej informacji, odwołaj się do „Przypisywanie Polityk Lokalnych" (p. 222).

Zobacz ustawienia bezpieczeństwa przypisane do urządzenia przenośnego:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**. Kliknij **Zapisz**. Wszystkie urządzenia należące do użytkowników wybranej grupy zostaną wyświetleni w tabeli.
4. Naciśnij nazwę urządzenia przenośnego, które cię interesuje. Pojawi się okno szczegóły.
5. W sekcji **Bezpieczeństwo** ze strony **Przegląd**, kliknij nazwę aktualnie przypisanej polityki w celu wyświetlenia jej ustawień.
6. Możesz zmienić ustawienia bezpieczeństwa jeżeli potrzebujesz. Należy pamiętać, że wszystkie zmiany jakie wprowadzisz będą miały również zastosowanie do wszystkich innych urządzeń, na których jest aktywna polityka.

   Aby uzyskać więcej informacji, odwołaj się do „Polityki Urządzenia Przenośnego" (p. 390)

Aby przypisać politykę do urządzenia przenośnego:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. W lewym panelu, wybierz grupę, która Cie interesuje.

4. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**. Kliknij **Zapisz**. Wszystkie urządzenia należące do użytkowników wybranej grupy zostaną wyświetleni w tabeli.
5. W prawym panelu, wybierz pole urządzenia przenośnego, które Cię interesuje.
6. Kliknij przycisk **Przypisz polityki** w górnej części tabeli.
7. Dokonaj niezbędnych ustawień w oknie **Przypisanie polityki**. Aby uzyskać więcej informacji, odwołaj się do „Przypisywanie Polityk Lokalnych” (p. 222).

6.4.11. Synchronizowanie z Active Directory.

Zasoby sieci są automatycznie synchronizowane z Active Directory w przedziałach czasu określonych w sekcji konfiguracyjnej Control Center. Aby uzyskać więcej informacji, zapoznaj się z rozdziałem Instalacja i Konfiguracja GravityZone w Przewodniku Instalacyjnym GravityZone.

Aby ręcznie zsynchronizować obecnie wyświetlanych użytkowników z Active Directory:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Naciśnij przycisk **Synchronizuj z Active directory** z górnej strony tabeli.
4. Czynności należy potwierdzić, klikając **Tak**.

> **Notatka**
> Dla duzych sieci Active directory, synchronizacja może zajać więcej czasu.

6.4.12. Usuwanie użytkowników i urządzeń przenosnych

Jeśli w zasobach sieciowych znajdują się nieaktualni użytkownicy lub urządzenia przenośne, zaleca się ich usunięcie.

Usuwanie urządzeń przenośnych z zasobów sieciowych

Kiedy usuwasz urządzenie z Control Center:

- GravityZone Mobile Client jest odłączony, ale nie usunięty z urządzenia.

- Dla urządzeń iOS, Profil MDM jest usunięty. Jeśli urządzenie nie jest podłączone do Internetu, Profil MDM pozostaje zainstalowany do czasu dostępności nowego połączenia.
- Wszystkie logi połączone z usuniętym urządzeniem pozostaną nadal dostępne.
- Nie wpłynie to na twoje osobiste informacje i zainstalowane aplikacje.

Ostrzeżenie

- Nie można przywrócić usuniętych urządzeń przenośnych.
- Jeżeli przypadkowo usunąłeś zablokowane urządzenie, musisz zrestartować urządzenie do ustawień fabrycznych, to je odblokuje.

Aby usunąć urządzenie przenośne:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. W lewym panelu, wybierz grupę, która Cie interesuje.
4. Kliknij menu **Filtry** z górnej stron obszaru panelu sieciowego i wybierz **Urządzenia** z kategorii **Widok**.
5. Kliknij **Zapisz**.
6. Zaznacz pola opowiadające urządzeniom przenośnym, jakie chcesz usunąć.
7. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Czynności należy potwierdzić, klikając **Tak**.

Usuwanie użytkowników z zasobów sieci

Użytkownicy przypisani do urządzeń przenośnych nie mogą zostać usunięci. Najpierw możesz usunąć odpowiednie urządzenie przenośne.

Notatka
Możesz usunąć użytkowników tylko z niestandardowych grup.

Aby usunąć użytkownika:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. W lewym panelu, wybierz grupę, która Cie interesuje.

4. Kliknij menu **Filtry** z górnej strony obszaru panelu sieciowego i wybierz **Użytkownicy** z kategorii **Widok**.
5. Kliknij **Zapisz**.
6. Zaznacz pola odpowiadające użytkownikom którzy mają zostać usunięci.
7. Naciśnij przycisk **Usuń** po prawej stronie tabeli. Czynności należy potwierdzić, klikając **Tak**.

6.5. Magazyn Aplikacji

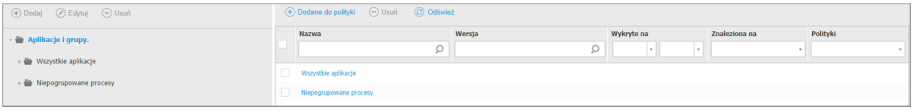
Możesz wyświetlić wszystkie aplikację wykryte w sieci przez zadanie **Wykrywanie Aplikacji**, w sekcji **Aplikacje i grupy**. Aby uzyskać więcej informacji, zapoznaj się z „Wykrywanie Aplikacji” (p. 100).

Aplikacje i procesy są automatycznie dodawane w folderze **Aplikacje i grupy** po lewej stronie panelu.

Możesz porządkować aplikacje i procesy w niestandardowe grupy.

Wszystkie aplikacje/procesy w wybranym folderze są wyświetlone w tabeli po prawej stronie panelu. Możesz wyszukiwać po nazwie, wersji, wydawcy/autorze, aktualizatorze, lokalizacji i polityce.

Aby przeglądać najnowsze informacje w tabeli, kliknij przycisk **Odśwież** z górnej części tabeli. Może być potrzebne abyś spędził więcej czasu na tej stronie.



Magazyn Aplikacji

WAŻNE
Nowe aplikacje wykryte za każdym razem jak uruchomisz zadanie **Wykrywania Aplikacji** zostaną automatycznie umiejscowione w folderze **Niepogrupowane Aplikacje** Procesy, które nie są powiązane ze specyficznymi aplikacjami, są umiejscowione w folderze **Niepogrupowane Procesy**.

Drzewo Aplikacje i Grupy

Aby dodać niestandardową grupę do drzewa **Aplikacje i grupy**:

1. Wybierz **Wszystkie aplikacje** folder.

2. Kliknij przycisk ⊕ **Dodaj** w górnej części drzewa.
3. Wpisz nazwę w nowym oknie.
4. Kliknij **OK** aby utworzyć nową grupę.
5. Wybierz **niepogrupowane aplikacje** folder. Wszystkie aplikacje zebrane w wybranym folderze są wyświetlone w prawej części panelu w tabeli.
6. Wybierz upragnione aplikacje z prawej strony panelu. Chwyć i upuść wybrane elementy z prawej strony panelu i przenieś je do niestandardowych grup z lewej strony.

Aby dodać niestandardową aplikację:

1. Wybierz folder docelowy pod **Wszystkie aplikacje**
2. Kliknij przycisk ⊕ **Dodaj** w górnej części drzewa.
3. Wpisz nazwę w nowym oknie.
4. Kliknij **OK** aby utworzyć niestandardową aplikacje.
5. Możesz dodać procesy powiązane do nowej niestandardowej aplikacji z folderu **Niepogrupowane Procesy**, lub z innych folderów wyświetlonych w drzewie **Aplikacje i grupy** Po tym jak wybierzesz folder, wszystkie procesy są wyświetlone w tabeli po prawej stronie panelu.
6. Wybierz upragnione procesy z tabeli po prawej stronie. Chwyć i upuść zaznaczone elementy w panelu po lewej stronie, aby przenieść je to niestandardowej aplikacji.

Notatka
Aplikacja może być częścią tylko jednej grupy.

Aby edytować folder lub nazwę aplikacji:

1. Zaznacz to na drzewie **Aplikacje i grupy**.
2. Kliknij przycisk ✎ **Edytuj** w górnej części drzewa.
3. Zmień nazwę na jaką chcesz.
4. Kliknij **OK**.

Możesz przesunąć grupy i aplikacje gdziekolwiek wewnątrz hierarchii **Aplikacje i grupy**. Aby przesunąć grupę lub aplikacje, przeciągnij i upuść je z obecnej do nowej lokacji.

Aby usunąć niestandardowy folder lub aplikacje, zaznacz je na drzewie**Aplikacje i grupy** i potem kliknij przycisk ⊖ **Usuń** w górnej części drzewa.

Dodając Aplikacje do Polityk

Aby dodać aplikacje lub proces do reguły bezpośrednio z Magazynu Aplikacji:

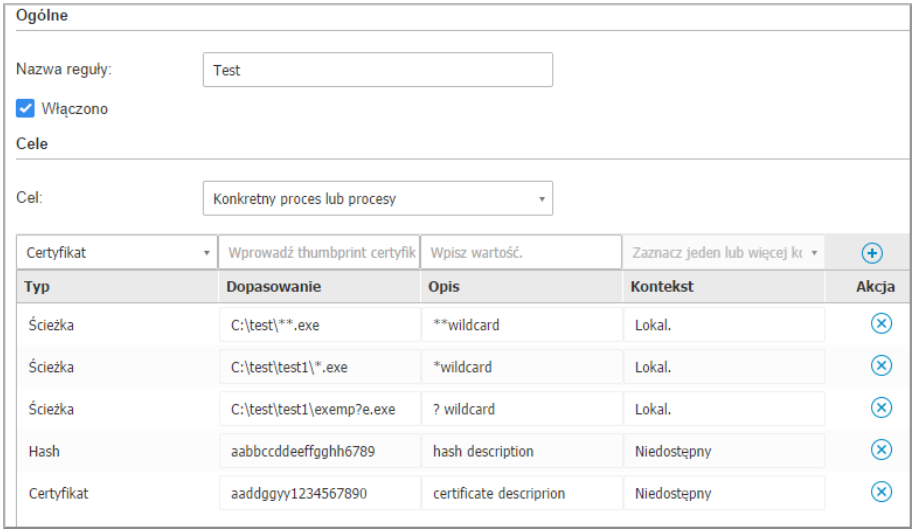
1. Wybierz pożądany folder z drzewa **Aplikacje i grupy**. Zawartość folderu jest wylistowana po prawej stronie panelu.
2. Zaznacz procesy lub aplikacje, które potrzebujesz z panelu po prawej stronie.
3. Kliknij przycisk ⊕ **Dodaj politykę** aby otworzyć okno konfiguracyjne.
4. W sekcji **Zastosuj regułę do tych polityk** wprowadź nazwę istniejącej polityki. Użyj wyszukiwarki aby znaleźć nazwę polityki lub nazwę właściciela.
5. W sekcji **Szczegóły reguły** wprowadź **nazwa reguły**.
6. Zaznacz pole wyboru **Włączone** aby aktywować regułę.
7. Typ docelowy jest automatycznie rozpoznawany. W razie potrzeby edytować istniejące kryteria:
   - **Specyficzny proces lub procesy**, aby określić proces, który jest dozwolony lub zabroniony przed startem. Możesz autoryzować po ścieżce, hash lub certyfikat. Warunki wewnątrz reguły są dopasowane na podstawie bramki logicznej AND
     - Aby autoryzować aplikację z określonej ścieżki:
       a. Zaznacz **Ścieżka** w kolumnie **Typ**. Określ ścieżkę do obiektu. Możesz podać bezwzględną lub względną ścieżkę i używać symboli wieloznacznych. Symbol gwiazdki (*) dopasowuje dowolny plik wewnątrz katalogu. Podwójna gwiazdka (**) pasuje do wszystkich plików i katalogów w określonym katalogu. Znak zapytania (?) zastępuje dokładnie jeden znak. Można także dodać opis do identyfikacji procesu.
       b. Z listy rozwijalnej **Wybierz jedno lub kilka kontekstów** można wybierać spośród lokalnych, CD-ROM, usuwalne i sieć. Możesz zablokować aplikacje uruchamiane z przenośnego dysku, lub zezwolić jeśli aplikacja jest wykonywana lokalnie.

– Aby autoryzować aplikacje oparte na HASHu, wybierz **Hash** w kolumnie **Typ** i wpisz wymaganą wartość. Można także dodać opis do identyfikacji procesu.

> **WAŻNE**
> Aby wygenerować wartość HASH, pobierz narzędzie Fingerprint. Aby uzyskać więcej informacji, odwołaj się do „Narzędzia Kontroli Aplikacji” (p. 519)

– Aby autoryzować w oparciu o certyfikat, zaznacz **Certyfikat** i kolumnie **Typ** i wpisz thumbprint certyfikatu. Można także dodać opis do identyfikacji procesu.

> **WAŻNE**
> Aby uzyskać thumbprint certyfikatu, pobierz narzędzie Thumbprint. Aby uzyskać więcej informacji, odwołaj się do „Narzędzia Kontroli Aplikacji” (p. 519)



Reguły aplikacji

Kliknij ⊕**Dodaj**, aby dodać regułę. Nowo utworzona reguła będzie mieć najwyższy priorytet w tej polityce.

- **Magazyn aplikacji lub grup**, aby dodać grupę lub aplikacje wykrytą w twojej sieci. Możesz wyświetlić aplikacje uruchomione w twojej sieci na stronie **Sieć > Magazyn Aplikacji**

  Wstaw aplikację lub nazwę grupy w polu, rozdzielając je przecinkami. Funkcja automatycznego uzupełniania wyświetla propozycje podczas pisania.

8. Zaznacz pole wyboru **Dołącz podprocesu** aby zastosować regułę do zrodzonych procesów podrzędnych.

   Ostrzeżenie
   Podczas ustawiania reguł dla aplikacji przeglądarki, zaleca się, aby wyłączyć tą opcję, aby uniknąć zagrożenia bezpieczeństwa.

9. Opcjonalnie można również określić wyjątki od zasady rozpoczęcia procesu. Dodawanie operacji jest podobne do tej jednej opisanej w poprzednich krokach.
10. W sekcji **Uprawnienia** wybierz czy zezwalasz czy odmawiasz uruchomić reguły.
11. Naciśnij **Zapisz** aby zastosować zmiany.

Aby usunąć aplikację lub proces:

1. Wybierz pożądany folder z drzewa **Aplikacje i grupy**.
2. Zaznacz procesy lub aplikacje, które potrzebujesz z panelu po prawej stronie.
3. Kliknij przycisk ⊖ **Usuń** .

Aktualizatory

Musisz zdefiniować aktualizatory dla aplikacji wykrytych w Twojej sieci.

Ostrzeżenie
Jeśli nie przypiszesz aktualizatorów, aplikacje z Białej Listy nie będą mogły się aktualizować.

Aby przypisać aktualizator:

1. Wybierz pożądany folder z drzewa **Aplikacje i grupy**. Zawartość folderu jest wylistowana po prawej stronie panelu.
2. Po prawej stronie panelu, wybierz plik, który chcesz użyć jako aktualizator.

3. Kliknij przycisk **Przypisz aktualizatory**.
4. Kliknij **Tak**, aby potwierdzić zadanie. Aktualizatory są oznaczone specyficzną ikoną:

Aktualizator

Aby usunąć aktualizator:

1. Wybierz pożądany folder z drzewa **Aplikacje i grupy**. Zawartość folderu jest wylistowana po prawej stronie panelu.
2. W panelu po prawej, zaznacz aktualizator, który chcesz usunąć.
3. Kliknij przycisk **Usuń aktualizatory**.
4. Kliknij **Tak**, aby potwierdzić.

6.6. Inwentarz Aktualizacji

GravityZone odkrywa aktualizacje potrzebne Twojemu oprogramowaniu poprzez **Skanowanie Aktualizacji**, a następnie dodaje je do inwentarza aktualizacji.

Na stronie **Inwentarz Aktualizacji** wyświetlane są wszystkie aktualizacje wykryte dla oprogramowania zainstalowanego na twoich punktach końcowych i zapewniasz kilka działań, które możesz wykonać na tych aktualizacjach.

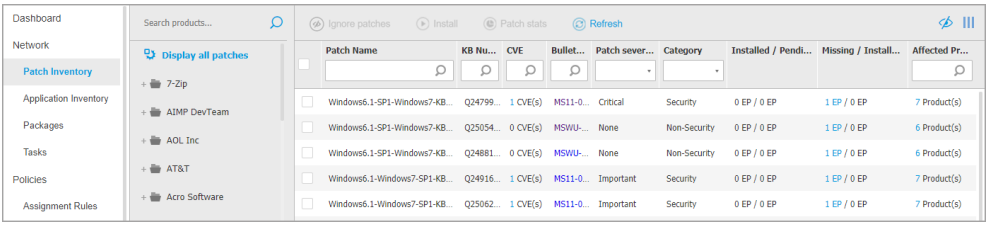
Korzystaj z Inwentarza Aktualizacji zawsze, gdy musisz niezwłocznie wdrożyć określone aktualizacje. Ta alternatywa pozwala łatwo rozwiązać niektóre problemy, o których wiesz. Na przykład, przeczytałeś artykuł dotyczący luki w oprogramowaniu i znasz identyfikator CVE. Możesz przeszukać inwentarz pod kątem aktualizacji adresujących CVE, a następnie sprawdzić, które punkty końcowe powinny zostać zaktualizowane.

Aby uzyskać dostęp do Inwentarza Aktualizacji, kliknij opcję **Sieć > Inwentarz Aktualizacji** w menu głównym Control Center.

Strona jest zorganizowana w dwóch panelach:

- W lewym panelu wyświetlane są produkty oprogramowania zainstalowane w sieci, pogrupowane według dostawców.

- Prawy panel wyświetla tabelę z dostępnymi aktualizacjami i szczegółami na ich temat.



Inwentarz Aktualizacji

Następnie dowiesz się jak korzystać z zasobów. Oto co możesz zrobić:

- Zobacz szczegóły aktualizacji
- Wyszukaj i filtruj aktualizacje
- Zignoruj uaktualnienia
- Zainstaluj aktualizacje
- Odinstaluj aktualizacje
- Stwórz statystyki aktualizacji

6.6.1. Przeglądanie Szczegółów Aktualizacji

Tabela aktualizacji zawiera informacje ułatwiające identyfikację aktualizacji, ocenę ich ważności, przeglądanie stanu instalacji i jej zakresu. Szczegóły opisane są tutaj:

- **Nazwa aktualizacji.** Jest to nazwa pliku wykonywalnego zawierającego aktualizację.
- **Numer KB.** Ta liczba identyfikuje artykuł KB, który ogłasza wydanie aktualizacji.
- **CVE.** Jest to liczba podatności CVE adresowanych przez aktualizację. Kliknięcie numeru wyświetli listę identyfikatorów CVE.
- **Identyfikator biuletynu.** Jest to identyfikator biuletynu zabezpieczeń wystawionego przez dostawcę. Ten identyfikator łączy się z artykułem opisującym aktualizacę i zawierającym szczegóły instalacji.

- **Waga aktualizacji.** Ta ocena informuje o znaczeniu poprawki względem szkód, którym przeciwdziała.
- **Kategoria.** W zależności od rodzaju problemów, które rozwiązują, aktualizacje są grupowane na dwie kategorie: bezpieczeństwo i niezwiązane z bezpieczeństwem. To pole informuje, do której kategorii należy aktualizacja.
- **Zainstalowana / Oczekuje na instalację.** Te liczby pokazują, ile punktów końcowych ma zainstalowaną aktualizację, a ile z nich czeka na jej zainstalowanie. Liczby prowadzą do listy tych punktów końcowych.
- **Brakujące / Instalacja nieudane.** Te liczby pokazują, ile punktów końcowych nie ma zainstalowanej aktualizacji, a w ilu instalacja nie powiodła się. Liczby prowadzą do listy tych punktów końcowych.
- **Produkty, których dotyczy problem.** Jest to liczba produktów, dla których została wydana aktualizacja. Liczba łączy się z listą produktów oprogramowania.
- **Usuwalne** Jeśli chcesz przywrócić aktualizację, musisz najpierw sprawdzić, czy aktualizację można odinstalować. Użyj tego filtra, aby dowiedzieć się, które aktualizacje można usunąć (przywrócić). Aby uzyskać więcej informacji, patrz Odinstaluj aktualizacje .

Aby dostosować szczegóły polityki wyświetlane w tabeli:

1. Kliknij przycisk III **Kolumny** z prawej strony Akcja Pasek narzędzi.
2. Wybierz kolumny, które chcesz zobaczyć.
3. Naciśnij przycisk **Reset** aby przywrócić domyślny widok kolumn.

Gdy jesteś na stronie, procesy GravityZone działające w tle mogą wpływać na bazę danych. Aby przeglądać najnowsze informacje w tabeli, kliknij przycisk **Odśwież** z górnej części tabeli.

GravityZone przegląda raz w tygodniu listę dostępnych aktualizacji i usuwa te, które nie mają już zastosowania, ponieważ nie istnieją już powiązane aplikacje lub punkty końcowe.

GravityZone codziennie przegląda i usuwa aktualizacje niedostępne na liście, chociaż mogą być obecne na niektórych punktach końcowych.

6.6.2. Wyszukiwanie i Filtrowanie Aktualizacji

Domyślnie Control Center wyświetla wszystkie dostępne aktualizacjie dla twojego oprogramowania. GravityZone oferuje kilka opcji szybkiego wyszukiwania potrzebnych aktualizacji.

Filtrowanie aktualizacji według produktu

1. Zlokalizuj produkt w lewym panelu bocznym.

   Możesz to zrobić przewijając listę, aby znaleźć jej dostawcę, lub wpisując jej nazwę w polu wyszukiwania w górnej części panelu.

2. Kliknij nazwę dostawcy, aby rozwinąć listę i wyświetlić jej produkty.
3. Wybierz produkt, aby wyświetlić dostępne aktualizacje, lub usuń zaznaczenie, aby ukryć je ukryć.
4. Powtórz poprzednie kroki dla produktów, które Cię interesują.

Jeśli chcesz ponownie zobaczyć aktualizacje dla wszystkich produktów, kliknij przycisk **Wyświetl wszystkie aktualizacje** w górnej części lewego panelu bocznego.

Filtrowanie poprawek według ich użyteczności

aktualizacja staje się zbędna, gdy na przykład, na punkcie końcowym została już wdrożona nowsza wersja. Jako że inwentarz może zawierać w danym momencie takie aktualizacje, GravityZone pozwala je zignorować. Wybierz te aktualizacje, a następnie kliknij przycisk **Ignoruj aktualizacje** w górnej części tabeli.

Control Center wyświetla ignorowane aktualizacje w innym widoku. Kliknij przycisk **Zarządzane/Ignorowane** po prawej stronie Paska Narzędzi Działań, aby przełączać widoki:

- - aby wyświetlić ignorowane aktualizacje
- - aby wyświetlić zarządzane aktualizacje.

Filtrowanie aktualizacji według szczegółów.

Użyj wyszukiwania, aby filtrować aktualizacje według konkretnych kryteriów lub według znanych szczegółów. Wprowadź wyszukiwane hasła w polach wyszukiwania w górnej części tabeli aktualizacji. Pasujące aktualizacje są wyświetlane w tabeli podczas pisania lub po dokonanym wyborze.

Wyczyszczenie pól wyszukiwania zresetuje wyszukiwanie.

6.6.3. Ignorowanie Aktualizacji

Być może będzie potrzebne wykluczenie niektórych poprawek z inwentarza aktualizacji, jeśli nie planujesz ich instalować na swoich punktach końcowych, za pomocą polecenia **Ignoruj poprawki**.

Zignorowana aktualizacja zostanie wykluczona z zadań automatycznych aktualizacji i raportów o aktualizacjach i nie będzie liczona jako brakująca aktualizacja.

aby ignorować aktualizację:

1. Na stronie **Inwentarz Aktualizacji** wybierz jedną lub kilka aktualizacji, które chcesz zignorować.
2. Kliknij przycisk **Ignoruj Aktualizacje** z górnej strony tabeli.

   Pojawi się okno konfiguracji, w którym można wyświetlić szczegóły dotyczące wybranych poprawek wraz z aktualizacjami podrzędnymi.
3. Kliknij **Ignoruj**. Aktualizacja zostanie usunięta z listy inwentarza aktualizacji.

Możesz znaleźć ignorowane aktualizacje w określonym widoku i podjąć na nich działania:

- Kliknij **Wyświetl ignorowane aktualizacje** w prawym górnym rogu tabeli. Zostanie wyświetlona lista wszystkich ignorowanych aktualizacji.
- Możesz uzyskać więcej informacji o ignorowanej aktualizacji, generując raport statystyk aktualizacji. Wybierz zignorowaną aktualizację i kliknij przycisk **Statystyki aktualizacji** u góry tabeli. Aby uzyskać więcej informacji, przejdź do „Tworzenie Statystyk Aktualicazji” (p. 205).
- Aby przywrócić zignorowane aktualizacje, zaznacz je i kliknij **Przywróć aktualizacje** w górnej części tabeli.

  Pojawi się okno konfiguracji, w którym można wyświetlić szczegółowe informacje o wybranych aktualizacjach.

  Kliknij przycisk **Przywróć**, aby wysłać aktualizację do inwentarza.

6.6.4. Instalowanie Aktualizacji

Aby zainstalować aktualizacje z Inwentarza Aktualizacji:

1. Idź do **Sieć > Inwentarz Aktualizacji**.
2. Zlokalizuj aktualizacje, które chcesz zainstalować. Jeśli to konieczne, użyj opcji filtrowania, aby szybko je znaleźć.

3. Wybierz aktualizacje, a następnie kliknij przycisk **Instaluj** w górnej części tabeli. Pojawi się okno konfiguracji, w którym możesz edytować szczegóły instalacji aktualizacji.

   Wyświetlone zostaną wybrane aktualizacje oraz aktualizacje podrzędne.

   - Wybierz docelową grupę punktów końcowych:
   - **Jeżeli to jest konieczne, zrestartuj punkt końcowy po instalacji aktualizacji**. Ta opcja spowoduje zrestartowanie punktów końcowych natychmiast po zainstalowaniu aktualizacji, jeśli wymagane jest ponowne uruchomienie systemu. Weź pod uwagę, że to działanie może zakłócić aktywność użytkownika.

     Pozostawienie tej opcji wyłączonej oznacza, że jeśli wymagane jest ponowne uruchomienie systemu na docelowych punktach końcowych, będą one wyświetlać ikonę oczekującego statusu restartu w inwentarzu sieciowym GravityZone. W takim przypadku masz następujące opcje:

     – Wysyłaj zadanie **Uruchom ponownie urządzenie** do oczekujących na restart punktów końcowych w dowolnym momencie. Szczegółowe informacje znajdują się w „Restartuj maszynę” (p. 99).

     – Skonfiguruj aktywną politykę, aby powiadomić użytkownika końcowego, że konieczne jest ponowne uruchomienie. Aby to zrobić, uzyskaj dostęp do aktywnej polityki na docelowym punkcie końcowym, przejdź do **Ogólne > Powiadomienia** i włącz opcję **Powiadomienie o ponownym uruchomieniu punktu końcowego**. W takim przypadku użytkownik będzie otrzymywać wyskakujące okienko za każdym razem, gdy konieczne będzie ponowne uruchomienie z powodu zmian wprowadzonych przez określone komponenty GravityZone (w tym przypadku Zarządzanie Aktualizacjami). Wyskakujące okno umożliwia odłożenie ponownego uruchomienia komputera. Jeśli użytkownik zdecyduje się odłożyć, powiadomienie o ponownym uruchomieniu będzie okresowo wyświetlane na ekranie, aż do ponownego uruchomienia systemu lub do upływu czasu ustawionego przez administratora firmy.

       Aby uzyskać więcej informacji, odwołaj się do „Powiadomienie o Restarcie Punktu Końcowego” (p. 240).

4. Kliknąć **Instaluj**.

   Zadanie instalacji jest tworzone wraz z pod-zadaniami dla każdego docelowego punktu końcowego.

Notatka

- Możesz również zainstalować aktualizację ze strony **Sieć**, zaczynając od określonych punktów końcowych, którymi chcesz zarządzać. W takim przypadku wybierz punkty końcowe z inwentarza sieci, kliknij przycisk **Zadania** w górnej części tabeli i wybierz opcję **Instalacja Aktualizacji**. Aby uzyskać więcej informacji, odwołaj się do „Instalacja aktualizacji" (p. 83).
- Po zainstalowaniu aktualizacji zalecamy wysłanie zadania Skanowanie Aktualizacji w celu dotarcia do punktów końcowych. Ta czynność uaktualni informacje o aktualizacji zapisane w GravityZone dla zarządzanych sieci.

6.6.5. Odinstalowywanie Aktualizacji

Może być konieczne usunięcie aktualizacji, które spowodowały awarię na docelowych punktach końcowych. GravityZone zapewnia funkcję wycofywania aktualizacji zainstalowanych w twojej sieci, co przywraca oprogramowanie do poprzedniego stanu przed zastosowaniem aktualizacji.

Funkcja odinstalowywania jest dostępna tylko w przypadku usuwalnych aktualizacji. Inwentaryzacja aktualizacji GravityZone zawiera kolumnę **Usuwalne**, w której możesz filtrować aktualizacje usuwając je.

Notatka
Atrybut usuwalności zależy od tego, w jaki sposób aktualizacja została wydana przez producenta lub zmian wprowadzonych przez aktualizację do oprogramowania. W przypadku aktualizacji, których nie można usunąć, może być konieczna ponowna instalacja oprogramowania.

Aby odinstalować aktualizację:

1. Idź do **Sieć > Inwentarz Aktualizacji**.
2. Wybierz aktualizacje, którą chcesz odinstalować. Aby wyszukać określoną aktualizację, użyj filtrów dostępnych w kolumnach, takich jak numer KB lub CVE. Użyj kolumny **Usuwalne**, aby wyświetlić tylko dostępne aktualizacje, które można odinstalować.

   Notatka
   Możesz odinstalować tylko jedną łaktualizację na raz dla jednego lub kilku punktów końcowych.

3. Kliknij przycisk ⊗ **Odinstaluj** z górnej części tabeli. Pojawi się okno konfiguracji, w którym możesz edytować szczegóły zadania deinstalacji.

   - **Nazwa zadania**. Możesz edytować domyślną nazwę zadania deinstalacji aktualizacji. W ten sposób łatwiej będzie zidentyfikować zadanie na stronie **Zadania**.
   - **Dodaj aktualizację do listy ignorowanych aktualizacji**. Najprawdopodobniej nie potrzebujesz już aktualizacji, którą chcesz odinstalować. Ta opcja automatycznie dodaje aktualizację do listy ignorowanych po jej odinstalowaniu.
   - **Jeżeli to jest konieczne, zrestartuj punkt końcowy po odinstalowaniu aktualizacji**. Ta opcja spowoduje zrestartowanie punktów końcowych natychmiast po odinstalowaniu aktualizacji, jeśli wymagane jest ponowne uruchomienie systemu. Weź pod uwagę, że to działanie może zakłócić aktywność użytkownika.

     Pozostawienie tej opcji wyłączonej oznacza, że jeśli wymagane jest ponowne uruchomienie systemu na docelowych punktach końcowych, będą one wyświetlać ikonę oczekującego statusu restartu w inwentarzu sieciowym GravityZone. W takim przypadku masz następujące opcje:

     – Wysyłaj zadanie **Uruchom ponownie urządzenie** do oczekujących na restart punktów końcowych w dowolnym momencie. Szczegółowe informacje znajdują się w „Restartuj maszynę” (p. 99).

     – Skonfiguruj aktywną politykę, aby powiadomić użytkownika końcowego, że konieczne jest ponowne uruchomienie. Aby to zrobić, uzyskaj dostęp do aktywnej polityki na docelowym punkcie końcowym, przejdź do **Ogólne > Powiadomienia** i włącz opcję **Powiadomienie o ponownym uruchomieniu punktu końcowego**. W takim przypadku użytkownik będzie otrzymywać wyskakujące okienko za każdym razem, gdy konieczne będzie ponowne uruchomienie z powodu zmian wprowadzonych przez określone komponenty GravityZone (w tym przypadku Zarządzanie Aktualizacjami). Wyskakujące okno umożliwia odłożenie ponownego uruchomienia komputera. Jeśli użytkownik zdecyduje się odłożyć, powiadomienie o ponownym uruchomieniu będzie okresowo wyświetlane na ekranie, aż do ponownego uruchomienia systemu lub do upłynięcia czasu ustawionego w polu Administratora firmy.

       Aby uzyskać więcej informacji, odwołaj się do „Powiadomienie o Restarcie Punktu Końcowego” (p. 240).

- W tabeli **Przywracanie** wybierz punkty końcowe, na których chcesz odinstalować aktualizację.

  Możesz wybrać jeden lub kilka punktów końcowych z sieci. Użyj dostępnych filtrów, aby zlokalizować punkt końcowy.

  Notatka
  Tabela wyświetla tylko punkty końcowe, w których zainstalowana jest wybrana aktualizacja.

4. Kliknij **Potwierdź**. Zadanie **Odinstalowywanie Aktualizacji** zostanie utworzone i wysłane do docelowych punktów końcowych.

   Raport **Odinstalowanie Aktualizacji** jest generowany automatycznie dla każdego ukończonego zadania deinstalacji aktualizacji, dostarczając szczegółowych informacji o aktualizacji, docelowych punktach końcowych i stanie zadania deinstalacji aktualizacji.

Notatka
Po odinstalowaniu aktualizacji zalecamy wysłanie zadania Skanowanie Aktualizacji w celu dotarcia do punktów końcowych. Ta czynność uaktualni informacje o aktualizacji zapisane w GravityZone dla zarządzanych sieci.

6.6.6. Tworzenie Statystyk Aktualicazji

Jeśli potrzebujesz szczegółowych informacji o statusie określonej aktualizacji dla wszystkich punktów końcowych, użyj funkcji **Statystyki Aktualizacji**, która generuje natychmiastowy raport dla wybranej aktualizacji:

1. Na stronie **Inwentarz aktualizacji** wybierz aktualizację z prawego panelu.
2. Kliknij przycisk **Status aktualizacji** w górnej części tabeli.

   Pojawi się raport statystyk aktualizacji, zawierający szczegóły statusu aktualizacji, w tym:

   - Wykres kołowy, pokazujący odsetek zainstalowanych, zakończonych niepowodzeniem, brakujących i oczekujących aktualizacji dla punktów końcowych, które zgłosiły aktualizację.
   - Tabelę wyświetlającą następujące informacje:
     - **Nazwa**, **FQDN**, **IP** i **OS** każdego punktu końcowego, który zgłosił aktualizację.

- **Ostatnia Kontrola**: czas ostatniego sprawdzenia aktualizacji na punkcie końcowym.
- **Status Aktualizacji**: zainstalowana, nieudana, brakująca lub ignorowana.

Notatka
Funkcja statystyki aktualizacji jest dostępna zarówno dla aktualizacji zarządzanych, jak i ignorowanych.

6.7. Przeglądanie i zarządzanie zadaniami

Strona **Sieć > Zadania** pozwoli Ci zobaczyć i zarządzać wszystkimi zadaniami jakie stworzyłeś.

Gdy stworzyłeś zadanie dla jednego lub kilku obiektów sieciowych, możesz zobaczyć je w tabeli zadań.

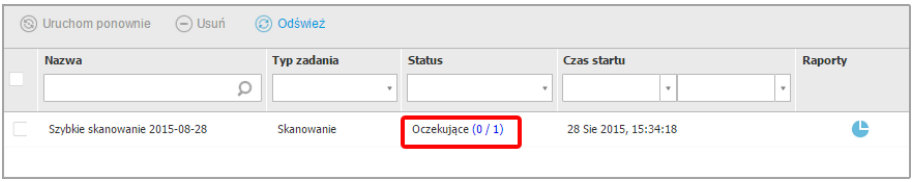
Możesz zrobić poniższe punkty ze strony **Sieć > Zadania**:

- Sprawdź status zadania
- Zobacz raporty zadań
- Restartuj zadania
- Zatrzymaj zadania skanowania Exchange
- Usuń zadania

6.7.1. Sprawdzanie statusu zadania

Za każdym razem jak tworzysz zadanie dla kilku obiektów sieci, możesz chcieć sprawdzić postęp i dostać powiadomienie gdy wystąpi błąd.

Przejdź do strony **Sieć > Zadania** i sprawdź kolumnę **Status** dla każdego zadania jakie Cię interesuje. Możesz sprawdzić status głównego zadania i możesz uzyskać szczegółowe informacje o każdym pod zadaniu.



Strona Zadań

- **Sprawdzanie statusu zadania głównego**

Główne zadanie dotyczy działań rozpoczętych na obiektach sieciowych (takich jak instalacja klienta lub skanowanie) i zawiera pewną liczbę pod zadań, jedno dla każdego wybranego obiektu sieciowego. Na przykład, główne zadanie instalacyjne stworzone dla ośmiu komputerów zawiera osiem pod zadań. Liczby w nawiasach stanowią ilość zakończony pod zadań. Na przykład, (2/8) znaczy, że dwa z ośmiu pod zadań jest ukończonych.

Status głównego zadania może być:

- **Oczekuje**, gdy żadne z pod-zadań się jeszcze nie zostało rozpoczęte, lub gdy zostanie przekroczona liczba jednoczesnych wdrożeń. Maksymalna liczba jednoczesnych wdrożeń może być ustawiona w menu **Konfiguracja**. Aby uzyskać więcej informacji zapoznaj się z Instrukcją Instalacyjną GravityZone.
- **W trakcie**, kiedy wszystkie pod zadania są uruchomione. Status głównego zadania pozostaje jako W Trakcie tak długo aż nie skończy się ostatnie pod zadanie.
- **Zakończone**, kiedy wszystkie pod zadania są zakończone(powodzeniem lub niepowodzeniem). W przypadku nieudanych pod zadań, pojawi się symbol ostrzegawczy.

- **Sprawdzanie statusu pod zadań**

  Przejdź do zadania, które Cię interesuje i wejdź w dostępny link w kolumnie **Status** aby otworzyć okno **Status**. Możesz zobaczyć listę obiektów sieci z przypisanymi zadaniami głównymi i statusem pod zadań. Status pod zadań może być:

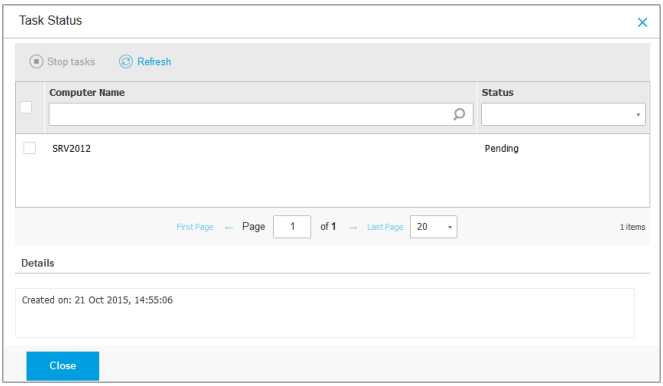
  - **W Trakcie**, kiedy pod zadania nadal działają.

    Dodatkowo, dla zadań skanowania na żądanie Exchange, można również wyświetlić status ukończenia.

  - **Zakończone**, kiedy pod zadania są zakończone sukcesem.
  - **Oczekujące**, kiedy pod zadania jeszcze się nie rozpoczęły. Może się to zdarzyć w następujących sytuacjach:
    - pod zadania czekają w kolejce.
    - Nie ma problemów z połączeniem Control Center i obiektów sieci docelowej.
    - Docelowe urządzenie jest w stanie spoczynku (offline), w przypadku urządzeń przenośnych. Zadanie zostanie uruchomione na urządzeniach docelowych gdy tylko pojawią się online.

- **Nie powiodło się**, kiedy pod zadania nie mogły się rozpocząć albo zostały zatrzymane przez błędy, takie jak niepoprawne uwierzytelnienie poświadczeń i za mała ilość pamięci.
- **Zatrzymywanie**, gdy skanowanie na żądanie trwa zbyt długo, aby sie skończyło i wybrałeś, aby je zatrzymać.

Aby zobaczyć szczegóły każdego pod zadania, wybierz je i sprawdź sekcje **Szczegóły** na dole tabeli.



Szczegóły statusu zadania

Możesz uzyskać informację na temat:

- Data i czas rozpoczęcia zadania.
- Data i czas końca zadania.
- Opis napotkanych błędów.

6.7.2. Przeglądanie raportów zadania

Na stronie **Sieć > Zadania** masz opcje żeby zobaczyć raporty zadań szybkiego skanowania.

1. Przejdź do strony **Sieć > Zadania**.
2. Wybierz żądany obiekt sieciowy z selektora widoku.
3. Zaznacz pole wyboru odpowiadające rodzajom skanowania zadań, którymi jesteś zainteresowany.

4. Naciśnij odpowiedni przycisk z kolumny **Raporty**. Poczekaj, aż zostanie wyświetlony raport. Aby uzyskać więcej informacji, odwołaj się do „Używanie raportów” (p. 415).

6.7.3. Restartowanie Zadań

Z różnych powodów, zadania instalacji klienta, dezinstalacji lub aktualizacji może nie zostać ukończona. Możesz wybrać czy uruchomić ponownie nieudane zadania zamiast tworzyć nowe, według następujących kroków:

1. Przejdź do strony **Sieć > Zadania**.
2. Wybierz żądany obiekt sieciowy z selektora widoku.
3. Wybierz pola wyboru odpowiadające nieudanym zadaniom.
4. Kliknij przycisk **Uruchom ponownie** z górnej części tabeli. Wybrane zadania zostaną uruchomione ponownie i status zadań zostanie zmieniony na **Ponawianie**.

Notatka
Dla zadań z wieloma pod zadaniami, opcja **Uruchom ponownie** jest dostępna jedynie wtedy gdy wszystkie pod zadania zostaną ukończone i tylko nieudane pod zadania będą wykonywane.

6.7.4. Zatrzymywanie zadań skanowania Exchange

Skanowanie Exchange Store może zająć dużo czasu. Jeśli z jakiegoś powodu chcesz przerwać skanowanie na żądanie Exchange, wykonaj kroki opisane tutaj:

1. Przejdź do strony **Sieć > Zadania**.
2. Wybierz żądany widok sieci z selektora widoku.
3. Kliknij link w kolumnie **Status**, aby otworzyć okno **Status Zadania**.
4. Zaznacz pole wyboru odpowiadające podzadaniom w toku lub uruchomionym, które chcesz zatrzymać.
5. Kliknij przycisk **Zatrzymaj zadania** w górnej części tabeli. Musisz potwierdzić tę czynność poprzez kliknięcie **Tak**.

Notatka
Możesz także przerwać skanowanie na żądanie Exchange Store z obszaru zdarzeń Bitdefender Endpoint Security Tools.

6.7.5. Usuwanie zadań

GravityZone automatycznie usuwa oczekujące zadania po 2 dniach i zakończone zadania po 30 dniach. Jeśli wciąż masz dużo zadań, jest zalecane usuwanie tych już niepotrzebnych, aby zapobiec zagraceniu listy.

1. Przejdź do strony **Sieć > Zadania**.
2. Wybierz żądany obiekt sieciowy z selektora widoku.
3. Zaznacz pola odpowiadające zadaniom które mają zostać usunięte.
4. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Czynności należy potwierdzić, klikając **Tak**.

> **Ostrzeżenie**
> Usuwanie oczekujących zadań, również anuluje zadanie.
> Jeżeli realizowane właśnie zadanie zostanie usunięte, wszystkie oczekujące pod zadania zostaną anulowane. W tym przypadku, wszystkie pod zadania nie zostaną ukończone.

6.8. Usuwanie punktów końcowych z zasobów sieci

Inwentarz sieci zawiera domyślnie folder **Usunięty**, wyznaczony do przechowywania punktów końcowych, którymi nie planujemy zarządzać.

Działanie **Usuń** niesie za sobą następujące efekty:

- Po usunięciu niezarządzanych punktów końcowych, są one przenoszone bezpośrednio do folderu **Usunięte**.
- Gdy zostaną usunięte zarządzane punkty końcowe:
  - Stworzono zadanie odinstalowania klienta
  - Zwolniono miejsce w licencji
  - Punkty końcowe są przeniesione do folderu **Usunięte**.

By usunąć punkty końcowe z zasobów sieci:

1. Przejdź do strony **Sieć**.
2. Wybierz odpowiedni widok sieci z selektor widoku.
3. Wybierz **Niestandardowe Grupy** z lewego panelu. Wszystkie punkty końcowe dostępne w tej grupie są wyświetlane w prawym panelu bocznym.

Notatka
Możesz usunąć tylko punkty końcowe wyświetlane pod **Grupy niestandardowe**, które zostały wykryte spoza którejkolwiek zintegrowanej infrastruktury sieci.

4. W prawym panelu, wybierz pole punktu końcowego, który chcesz usunąć.
5. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Czynności należy potwierdzić, klikając **Tak**.

   Jeśli usunięty punkt końcowy jest zarządzany, zadanie **Odinstaluj klienta** zostanie utworzone na stronie **Zadania**, a agent bezpieczeństwa zostanie odinstalowany z punktu końcowego, zwalniając jedną pozycję licencji.
6. Punkt końcowy jest przeniesiony do folderu **Usunięte**.

Możesz w każdym momencie przenieść punkty końcowe z folderu **Usunięte** do **Grypy Niestandardowe** przy użyciu funkcji przeciągnij i upuść.

Notatka
- Jeśli chcesz trwale wykluczyć niektóre punkty końcowe z zarządzania, musisz je zachować w folderze **Usunięte**.
- Jeśli usuniesz punkty końcowe z folderu **Usunięte**, zostaną one całkowicie usunięte z bazy danych GravityZone. Jednak wykluczone punkty końcowe, które są w trybie online, zostaną wykryte przy następnym zadaniu wykrywania sieci i pojawią się w Zasobach Sieciowych jako nowe punkty końcowe.

6.9. Konfiguracja Ustawień Sieciowych

Na stronie **Konfiguracja > Ustawienia Sieci**, możesz skonfigurować ustawienia związane z Inwentarzem Sieci, takie jak: zapisywanie filtrów, zachowanie ostatnio przeglądanej lokalizacji, tworzenie i zarządzanie zaplanowanymi regułami usuwania nieużywanych maszyn wirtualnych.

Opcje są podzielone na następujące sekcje:

- Ustawienia zasobów sieciowych
- Czyszczenie maszyn offline

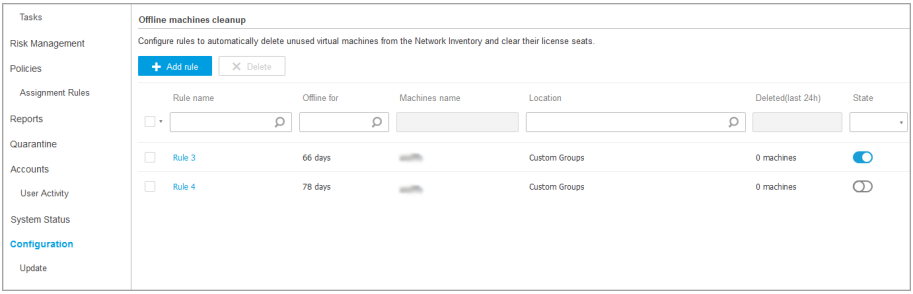
6.9.1. Ustawienia Inwentarza Sieci

W sekcji **Ustawienia Inwentarza Sieci**, dostępne są następujące opcje:

- **Zapisz filtry Zasobów Sieciowych**. Zaznacz to pole wyboru, aby zapisać filtry w **Sieci** między sesjami Control Center.
- **Zapamiętaj ostatnio przeglądaną lokalizację w Zasobach Sieciowych, dopóki się nie wyloguję**. Zaznacz te pole by zapisać ostatnią lokalizację przed opuszczeniem strony **Sieci**. Lokalizacja nie zapisuje się pomiędzy sesjami.
- **Unikaj duplikatów sklonowanych punktów końcowych**. Zaznacz tę opcję aby uruchomić nowy rodzaj obiektów sieciowych w GravityZone zwany złote obrazy. W ten sposób możesz odróżnić źródłowe punkty końcowe od ich klonów. Następnie należy oznaczyć każdy klonowany punkt końcowy w następujący sposób:
  1. Przejdź do strony **Sieć**.
  2. Zaznacz punkt końcowy, który chcesz sklonować.
  3. Wybierz z menu kontekstowego **Oznacz jako Złoty Obraz**.

6.9.2. Czyszczenie Maszyn Offline

W sekcji **Czyszczenie maszyn offline**, możesz skonfigurować zaplanowane reguły automatycznego usuwania nieużywanych maszyn wirtualnych z Zasobów Sieci.



Konfiguracja - Ustawienia Sieci - Czyszczenie maszyn offline

Tworzenie reguł

Aby utworzyć regułę czyszczenia:

1. W sekcji **Czyszczenie maszyn offline**, kliknij przycisk **Dodaj regułę**.
2. Na stronie konfiguracji:
   a. Wprowadź nazwę reguły.

b. Wybierz godzinę codziennego czyszczenia.

c. Zdefiniuj kryteria czyszczenia:

- Ile dni maszyny były offline (od 1 do 90).
- Wzór nazwy, który można zastosować dla jednej lub wielu maszyn wirutalnych.

  Na przykład użyj `maszyna_1`, aby usunąć maszynę o tej nazwie. Alternatywnie, dodaj `maszyna_*`, aby usunąć wszystkie maszyny, których nazwa zaczyna się na `maszyna_`.

  W tym polu rozróżniana jest wielkość liter i akceptowane są tylko litery, cyfry i znaki specjalne gwiazdka (*), znak podkreślenia (_), myślnik (-). Nazwa nie może zaczynać się gwiazdką (*).

d. Wybierz docelowe grupy punktów końcowych w Zasobach Sieci gdzie zastosować regułę.

3. Kliknij **Zapisz**.

Wyświetlanie Reguł i Zarządzanie nimi

Sekcja **Ustawienia Sieci > Czyszczenie maszyn offline** umożliwia przeglądanie wszystkich utworzonych reguł. Dedykowana tabela zawiera następujące informacje:

- Nazwa reguły.
- Liczba dni, po których maszyny przełączyły się w tryb offline.
- Wzór nazw maszyn.
- Lokalizacja w Zasobach Sieciowych.
- Liczba maszyn usuniętych w ciągu ostatnich 24 godzin.
- Stan: Włączony, wyłączony lub niepoprawny.

> **Notatka**
> Reguła jest nieprawidłowa gdy cele są w różnych przyczyn nieprawidłowe. Na przykład, wirtualne maszyny zostały usunięte lub nie masz do niej dostępu.

Nowo utworzona reguła jest domyślnie włączona. W każdej chwili możesz włączyć i wyłączyć reguły używając przełącznika Włączona/Wyłączona w kolumnie **Stan**.

W razie potrzeby użyj opcji sortowania i filtrowania w górnej części tabeli, aby znaleźć określone reguły.

Aby zmodyfikować regułę:

1. Kliknij nazwę reguły.
2. Na stronie konfiguracji edytuj szczegóły reguły.
3. Kliknij **Zapisz**.

Aby usunąć jedną lub więcej reguł:

1. Użyj pól wyboru, aby wybrać jedną lub więcej reguł.
2. Kliknij przycisk **Usuń** w górnej części tabeli.

6.10. Konfigurowanie Ustawień Security Server

Security Server korzysta z mechanizmu buforowania aby zdeduplikować skanowanie antymalware, optymalizując proces. Kolejnym krokiem optymalizacji skanowania jest współdzielenie tej pamięci z innymi Security Server

Współdzielenie pamięci podręcznej działa tylko pomiędzy serwerami Security Server tego samego typu. Przykładowo Security Server Multi-Platform będzie współdzielił pamięć tylko z innym Security Server Multi-Platform, a nie z Security Server for NSX.

Aby włączyć i skonfigurować dzielenie pamięci:

1. Przejdź do **Konfiguracja > Security Server Ustawienia**.
2. Zaznacz okienko **Security Server Współdzielnie Pamięci**.
3. Wybierz zakres udostępniania:
   - Wszystkie dostępne Security Server.

     Używanie tej opcji jest zalecane jeśli wszystkie Security Server są w tej samej sieci.
   - Security Server dostępne na liście przydziałów.

     Używaj tej opcji gdy Security Server są w różnych sieciach i współdzielenie pamięci może wygenerować dużo ruchu.
4. Przy ograniczaniu zakresu, utwórz grupę Security Server. Wybierz Security Server z rozwijanej listy i kliknij **Dodaj**.

   Tylko Security Server w tabeli będą współdzielić pamięć.

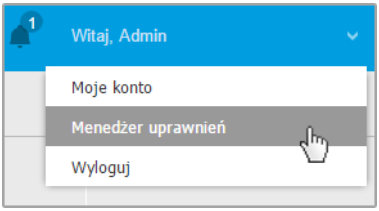
Notatka
Security Server dla NSX-T i NSX_V wymieniają informacje tylko wewnątrz tego samego serwera vCenter.

5. Kliknij **Zapisz**.

6.11. Manager uprawnień

Menadżer Poświadczeń pomaga definiować poświadczenia wymagane podczas dostępu do zasobów Serwera vCenter i do zdalnego uwierzytelniania na rożnych systemach operacyjnych w twojej sieci.

Aby otworzyć Menadżera Poświadczeń, kliknij nazwę użytkownika w górnym prawym rogu strony i wybierz **Menadżer Poświadczeń**.



Menu menadżera poświadczeń

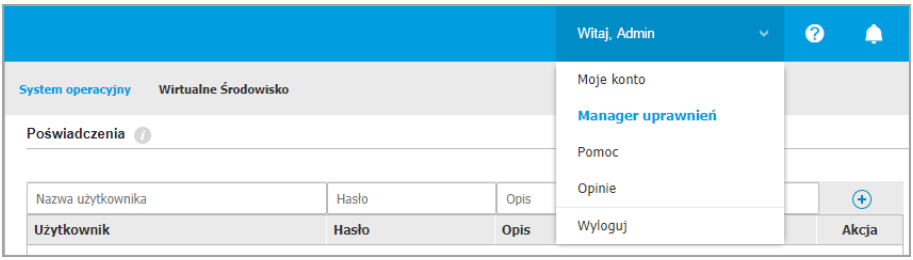
Okno **Menadżer poświadczeń** zawiera dwie zakładki:

- System Operacyjny
- Wirtualne środowisko

6.11.1. System Operacyjny

Z zakładki **System Operacyjny** możesz zarządzać poświadczeniami administratora wymaganymi do zdalnego uwierzytelniania podczas zadań instalacji wysyłanych do komputerów i maszyn wirtualnych w twojej sieci.

Aby dodać zestaw poświadczeń:



Manager uprawnień

1. Wprowadź nazwę użytkownika i hasło konta administratora dla każdego docelowego systemu operacyjnego w odpowiednim polu z górnej strony nagłówka tabeli. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto. Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

   Użyj konwencji Windows podczas wprowadzania nazwy użytkownika konta

   - Dla maszyn Active Directory użyj tych składni: `username@domain.com` i `domain\username`. Aby upewnić się że wprowadzone poświadczenia będą działać, dodaj je w obu formach (`username@domain.com` i `domain\username`).
   - Dla maszyn z grupy roboczej, wystarczy wprowadzić tylko nazwę użytkownika, bez nazwy grupy roboczej.

2. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli. Nowe ustawienia poświadczeń zostały dodane do tabeli.

> **Notatka**
> Jeżeli nie określiłeś poświadczeń uwierzytelniania, będziesz musiał podać je podczas uruchamiania zadania instalacyjnego. Określone poświadczenia, zostaną zapisane automatycznie w menadżerze poświadczeń, więc nie będziesz musiał wprowadzać ich ponownie następnym razem.

6.11.2. Wirtualne środowisko

W zakładce Środowisko Wirtualne, możesz zarządzać uwierzytelnianiem poświadczeń dla dostępnych systemów serwera zwirtualizowanego.

Aby mieć dostęp do zwirtualizowanej infrastruktury zintegrowanej z Control Center musisz podać swoje poświadczenia użytkownika dla każdego dostępnego systemu serwera wirtualizacji. Control Center używa twoich poświadczeń, aby połączyć z wirtualną infrastrukturą, pokazywanie tylko zasobów do których masz dostęp (jak określono w serwerze zwirtualizowanym).

Aby określić poświadczenia wymagane do połączenia się z serwerem zwirtualizowanym:

1. Wybierz serwer z odpowiedniego menu.

   Notatka
   Jeżeli menu jest niedostępne, albo nie została jeszcze skonfigurowana integracja lub wszystkie niezbędne poświadczenia zostały już skonfigurowane.

2. Podaj swoją nazwę użytkownika, hasło i sugestywny opis.
3. Kliknij przycisk ⊕ **Dodaj** . Nowe ustawienia poświadczeń zostały dodane do tabeli.

   Notatka
   Jeżeli nie skonfigurowałeś poświadczeń uwierzytelnienia w Menadżerze poświadczeń, będziesz musiał podać je podczas próby przeglądania spisu dowolnego systemu serwera zwirtualizowanego. Po wprowadzeniu swoich poświadczeń, zostaną one zapisane w Menadżerze Poświadczeń tak, by nie było potrzeby wprowadzania ich ponownie.

   WAŻNE
   Za każdym razem, gdy zmienisz hasło użytkownika serwera zwirtualizowanego, pamiętaj aby uaktualnić je w Menadżerze Poświadczeń.

6.11.3. Usuwanie Poświadczeń z Menadżera Poświadczeń

aby usunąć nieaktualne poświadczenia z Menadżera Poświadczeń:

1. Wskaż wiersz w tabeli zawierający dane uwierzytelniające, które chcesz usunąć.
2. Kliknij przycisk ⊗**Usuń** po prawej stronie odpowiedniego wiersza w tabeli. Wybrane konto zostanie usunięte.

7. POLITYKI BEZPIECZEŃSTWA

Po zainstalowaniu ochrony Bitdefender może być skonfigurowana i zarządzana z Control Center używając polityk bezpieczeństwa. Szczegóły ustawień polityki bezpieczeństwa zostaną dostosowane do zasobu obiektów sieci docelowej (komputery, maszyny wirtualne lub urządzenia mobilne).

Natychmiast po instalacji, zasobom obiektów sieciowych zostanie przypisana domyślna polityka, która jest wstępnie skonfigurowana z zalecanymi ustawieniami ochrony. Integracja NSX jest włączona, kiedy kolejne trzy domyślne zasady zabezpieczeń dla NSX są dostępne, po jednym dla każdego poziomu zabezpieczeń: pobłażliwy, normalny i agresywny. Zasady te są wstępnie skonfigurowane z zalecanymi ustawieniami zabezpieczeń. Nie możesz modyfikować ani usuwać domyślnych polityk.

Możesz utworzyć tak wiele polityk bazujących na wymaganiach bezpieczeństwa ile potrzebujesz, dla każdego rodzaju zarządzanych obiektów sieciowych.

To jest to co potrzebujesz, żeby wiedzieć o politykach:

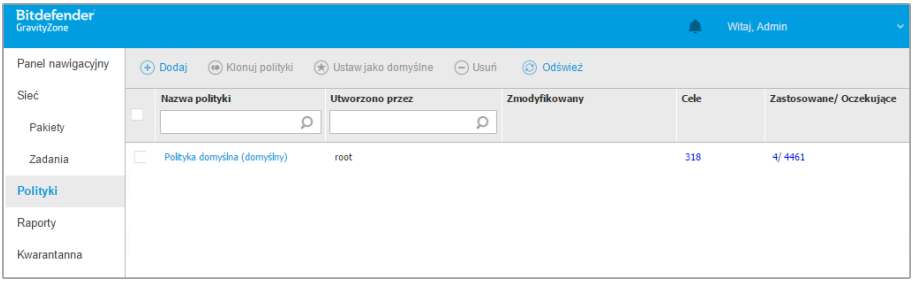
- Polityki są tworzone na stronie **Polityki** i przypisane do obiektów sieciowych ze strony **Sieć**.
- Polityki mogą dziedziczyć kilka ustawień modułów od innych polityk.
- Możesz skonfigurować przypisanie polityki do punktów końcowych tak, że polityka może mieć zastosowanie tylko w pewnych warunkach, w zależności od lokalizacji lub zalogowanego użytkownika. W związku z tym, punkt końcowy może mieć więcej przypisanych polityk.
- Punkty końcowe mogą mieć jedną aktywną politykę w tym samym czasie.
- Możesz przypisać politykę do indywidualnych punktów końcowych lub do grup punktów końcowych. Podczas przypisywania polityki zdefiniujesz również zasady dziedziczenia polityk. Domyślnie każdy punkt końcowy dziedziczy polityki grupy nadrzędnej.
- Polityki są przekazywane do docelowych obiektów sieci natychmiast po utworzeniu lub modyfikacji. Ustawienia powinny być zastosowane na obiektach sieciowych w mniej niż minutę (jeżeli są online). Jeżeli obiekty sieciowe nie są online, ustawienia nie będą stosowane tak długo jak nie pojawią się online.
- Polityka ma zastosowanie tylko do zainstalowanych modułów ochrony.
- Strona **Polityki** wyświetla tylko następujące typy zasad:
  - Polityki własne.

  - Inne polityki (takie jak domyślne polityki lub szablony stworzone przez innych użytkowników) które są przypisywane do punktów końcowych pod twoim kontem.
- Nie możesz edytować polityk stworzonych przez innych użytkowników (chyba że właściciel polityki dopuszcza to w ustawieniach polityki), ale możesz je zmienić przypisując obiektom docelowym inne polityki.

Ostrzeżenie
Tylko wspierane moduły zasad zostaną zastosowane na docelowych punktach końcowych.
Należy pamiętać, że jedynie moduł Antymalware jest wspierana dla systemów operacyjnych serwera.

7.1. Zarządzanie politykami

Możesz przeglądać i zarządzać politykami na stronie **Polityki**



Strona Polityki

Każdy rodzaj punktu końcowego ma określone ustawienia polityk. Zarządzanie politykami, musisz najpierw wybrać rodzaj punktów końcowych (**Komputery i Maszyny wirtualne** lub **Urządzenia Mobilne**) w selektorze widoku.

Istniejące polityki są wyświetlane w tabeli. Dla każdej polityki, możesz zobaczyć:

- Nazwa polityki.
- Użytkownik, który stworzył politykę.
- Data i czas ostatniej modyfikacji polityki.
- Liczba celów, do których została wysłana polityka.*
- Liczba celów, dla których polityka została zastosowana / jest w toku.*

W przypadku polityki włączonego modułu ESX dodatkowe informacje dostępne są:

- Nazwa Polityka NSX, używana do identyfikacji Bitdefender polityki w VMware vSphere.
- Polityka widoczności w zarządzaniu konsolami pozwalająca filtrować politykę dla NSX. Tak więc, gdy **Lokalna** polityka jest widoczna tylko w Bitdefender Control Center, **globalna** polityka jest widoczna także w VMware NSX.

Dane te są domyślnie ukryte.

Aby dostosować szczegóły polityki wyświetlane w tabeli:

1. Kliknij przycisk **Kolumny** z prawej strony Akcja Pasek narzędzi.
2. Wybierz kolumny, które chcesz zobaczyć.
3. Naciśnij przycisk **Reset** aby przywrócić domyślny widok kolumn.

* Klikając liczbę, zostaniesz przekierowany do zakładki **Sieć**, gdzie możesz podejrzeć odpowiednie punkty końcowe. Zostaniesz poproszony o wybranie widok sieci. Ta akcja utworzy filtr korzystając z kryterium polityki.

Możesz sortować dostępne polityki i wyszukać niektórych polityk używając dostępnych kryteriów.

7.1.1. Tworzenie polityk

Możesz utworzyć polityki zarówno dodając nową politykę lub powielając (klonując) istniejącą politykę.

Aby utworzyć politykę bezpieczeństwa:

1. Przejdź do strony **Polityki**.
2. Wybierz pożądany rodzaj punktu końcowego z selektora widoku.
3. Wybierz metodę tworzenia polityki:
   - **Dodaj nową politykę**.
     - Kliknij przycisk **Dodaj** w górnej części tabeli. Ta Komenda tworzy nową politykę używając domyślnego szablony polityki.
   - **Sklonuj istniejącą politykę**.
     a. Zaznacz pole wyboru polityki jaką chcesz powielić.
     b. Kliknij przycisk **Klonuj** z górnej strony tabeli.

4. Konfiguruj ustawienia polityk. Aby uzyskać szczegółowe informacje, odwołaj się do:
   - „Polityki Komputerów i Maszyn Wirtualnych” (p. 233)
   - „Polityki Urządzenia Przenośnego” (p. 390)
5. Naciśnij **Zapisz** aby utworzyć politykę i powrócić do listy polityk.

Przy określaniu polityki, która jest stosowana w VMware NSX, oprócz konfigurowania ustawień ochrony antimalware w GravityZone Control Center, trzeba także stworzyć politykę w NSX, instruującą jak używać GravityZone polityki w profilu usługi. Aby utworzyć politykę bezpieczeństwa NSX:

1. Zaloguj się do sieci klienta vSphere.
2. Idź do **Sieć & Bezpieczeństwo > Service Composer > Polityka bezpieczeństwa** zakładki.
3. Kliknij przycisk **Utwórz Politykę Bezpieczeństwa** na pasku w górnej części tabeli polityka. Wyświetlono okno konfiguracji.
4. Wpisz nazwę polityki, a następnie kliknij przycisk **Dalej**.

   Opcjonalnie można również dodać krótki opis.
5. Kliknij **Dodaj usługę Gości introspekcji** przycisk w górnej części tabeli. Zostanie wyświetlone okno konfiguracji: usługa The Guest Introspection.
6. Wprowadź nazwę i opis usług.
7. Zostaw wybraną domyślną akcję, aby umożliwić Bitdefender usługę profilu, która będzie zastosowana w grupie zabezpieczeń.
8. Z **Nazwa usługi** menu, wybierz **Bitdefender**.
9. Od **Profil usługi** menu, wybierz istniejącą GravityZone politykę bezpieczeństwa.
10. Pozostaw wartości domyślne **Stan** i **Egzekwowanie** opcje.

    Notatka
    Aby uzyskać więcej informacji na temat ustawień polityki zabezpieczeń, należy zapoznać się z dokumentacja VMware NSX.

11. Naciśnij **OK** aby dodać usługę.
12. Kliknij **Następny** do ostatniego kroku, a następnie kliknij przycisk **Zakończ**.

7.1.2. Przypisywanie polityk

Punkty końcowe są początkowo przypisane do polityki domyślnej. Po zdefiniowaniu niezbędnych polityk na stronie **Polityki** możesz przypisać je do punktów końcowych.

Polityka procesu przydziału jest związana z różnymi środowiskami, która integruje się z GravityZone. Dla niektórych integracji, takich jak VMware NSX, polityka jest dostępna poza GravityZone Control Center. Nawiązują również do polityki zewnętrznej.

Przypisywanie Polityk Lokalnych

Możesz przypisać lokalne polityki na dwa sposoby:

- Przypisanie oparte na urządzeniu, oznacza, że ręcznie wybierasz docelowe punkty końcowe, do których przypisujesz polityki. Te polityki są także znane jako polityki urządzenia.
- Przypisanie oparte na regule, oznacza, że polityka jest przypisana do zarządzanego punktu końcowego, jeśli ustawienia sieciowe na punkcie końcowym pasują do podanych warunków istniejącej reguły przypisania.

Notatka

- Możesz przypisać tylko polityki które stworzyłeś. Aby przypisać politykę stworzona przez innego użytkownika, możesz ją najpierw sklonować na stronie **Polityki**.
- Na maszynach wirtualnych chronionych przez HVI samodzielnie, możesz przypisać tylko polityki urządzeń. Kiedy Bitdefender Endpoint Security Tools jest też na nich zainstalowany, możesz przypisać im też oparte na regułach polityki, agent ochrony zarządza aktywacją polityki.

Przypisywanie Polityk Użytkownika

W GravityZone możesz przypisać polityki na kilka sposobów:

- Przypisz politykę bezpośrednio do obiektu docelowego.
- Przypisz politykę grupy nadrzędnej poprzez dziedziczenie.
- Wymuś dziedziczenie polityki na urządzeniu docelowym.

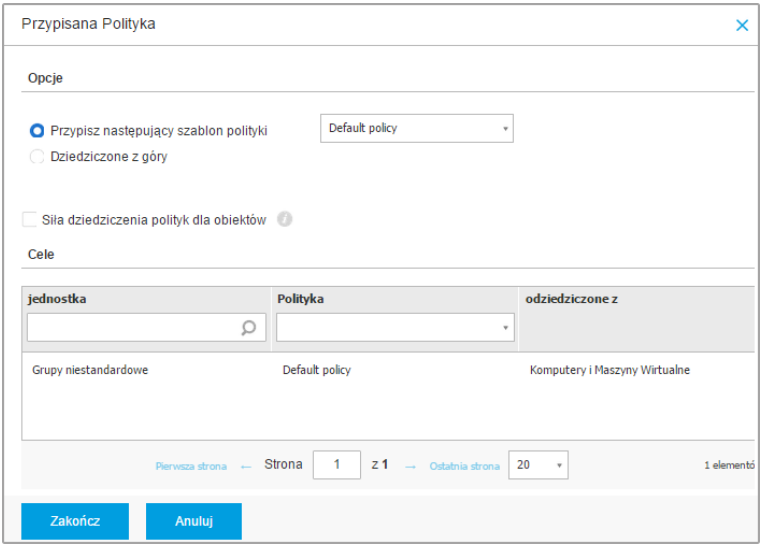
Domyślnie, każdy punkt końcowy bądź grupa punktów końcowych dziedziczy politykę grupy nadrzędnej. Jeśli zmienisz politykę grupy nadrzędnej, wpłynie to na wszystkich członków grupy podrzędnej poza tymi z wymuszoną polityką.

Aby przypisać politykę do urządzenia:

1. Przejdź do strony **Sieć**.
2. Wybierz widok sieci z selektora widoków .
3. Wybierz docelowe punkty końcowe. Możesz wybrać jeden lub kilka punktów końcowych bądź grupy punktów końcowych.

   Dla celów dziedziczenia nie można zmienić polityki grupy głównej na domyślną. Na przykład **Komputer i Maszyny Wirtualne** będą zawsze miały przypisaną **strategię domyślną** .
4. Kliknij **Przypisz politykę** przycisk w górnej części panelu, bądź wybierz opcję **Przypisz politykę** z menu kontekstowego.

   Zostaje wyświetlona strona **Przypisania polityk**:



Ustawienia Przypisania Polityki

5. Sprawdź tabelę z docelowymi punktami końcowymi. Dla każdego punktu końcowego możesz zobaczyć:
   - Przypisana polityka.
   - Grupa nadrzędna z której obiekt dziedziczy politykę (jeśli dotyczy).

Jeśli grupa wymusza politykę, możesz kliknąć jej nazwę aby zobaczyć stronę **Przypisania polityki** z tą grupą jako docelową.

- Status wymuszenia.

  Ten status pokazuje czy element docelowy wymusza dziedziczenie polityki bądź też jest zmuszony do odziedziczenia polityki.

  Zauważ elementy docelowe z wymuszoną polityką (ze statusem **Jest wymuszona** Ich polityki nie mogą zostać zastąpione. W takim przypadku jest wyświetlany komunikat ostrzeżenia.

6. W przypadku ostrzeżenia, kliknij link **Wyklucz te elementy docelowe** aby kontynuować.
7. Wybierz jedną z dostępnych opcji aby przypisać politykę:
   - **Przypisz następujący szablon polityki** - aby wyznaczyć konkretną politykę bezpośrednio do docelowych punktów końcowych.
   - **Odziedzicz z góry** - aby użyć polityki grupy nadrzędnej.
8. Jeśli zdecydujesz się przypisać szablon polityki:
   a. Wybierz politykę z listy rozwijalnej.
   b. Wybierz **Wymuś dziedziczenie polityki dla grup podrzędnych** aby osiągnąć następujący rezultat:
      - Przypisz politykę do wszystkich potomków grup docelowych, bez wyjątku.
      - Zapobiegaj zmienianiu tego z miejsc położonych niżej w hierarchii.

      Nowa tabela wyświetla rekurencyjnie wszystkie dotknięte punkty końcowe i grupy punktów końcowych, razem z politykami, które zostaną zastąpione.
9. Naciśnij **Zakończ** aby zapisać i potwierdzić zmiany. W przeciwnym wypadku kliknij **Wstecz** lub **Przerwij** aby wrócić do poprzedniej strony.

Po zakończeniu polityki są natychmiast wysyłane do docelowych punktów końcowych. Ustawienia powinny być zastosowane na punktach końcowych w mniej niż minutę (jeżeli są online). Jeśli punkt końcowy nie jest online, ustawienia zostaną dla niego zastosowane jak tylko ponownie pojawi się online.

Aby sprawdzić czy polityka została przypisana z sukcesem:

1. Na stronie **Sieć** kliknij nazwę punktu końcowego, który Cię interesuje. Control Center wyświetli okno **Informacji**.

2. Sprawdź sekcję **Polityka** aby zobaczyć stan obecnej polityki. Musi pokazywać **Zastosowana**.

Kolejna metoda sprawdzająca status zadania pochodzi ze szczegółów polityki:

1. Przejdź do strony **Polityki**.
2. Znajdź przypisaną politykę.

   W kolumnie **Aktywne/Zastosowane/Oczekujące** możesz wyświetlić liczbę punktów końcowych dla każdego z trzech statusów.
3. Kliknij dowolną liczbę, aby wyświetlić listę punktów końcowych z odpowiednim stanem na stronie **Sieć**.

Przypisywanie Polityk Opartych na Regule

Strona **Polityki > Reguł Przypisywania** umożliwia zdefiniowanie polityki dotyczącej użytkowników oraz polityki świadomości lokalizacji. Przykładowo, możesz zastosować bardziej restrykcyjne reguły zapory ogniowej, kiedy użytkownicy łączą się z internetem spoza firmy lub możesz włączyć Kontrolę Dostępu do Sieci dla użytkowników, którzy nie są częścią grupy administratorów.

Oto co musisz wiedzieć o regułach przypisywania:

- Punkty końcowe moga tylko mieć aktywena jedną politykę w tym samym czasie.
- Polityka stosowana przez reguły zastąpi politykę urządzenia ustawioną na punkcie końcowym.
- Jeśli żadna z zasad przypisania nie ma zastosowania, to stosowana jest polityka urządzenia.
- Zasady są sortowane i przetwarzane według priorytetu, gdzie `1` to najwyższy priorytet. Możesz mieć kilka reguł dla tego samego celu. W tym przypadku, zostanie zastosowana pierwsza reguła, która odpowiada aktywnym ustawieniom połączenia na docelowym punkcie końcowym.

  Na przykład, jeśli punkt końcowy pasuje do reguły użytkownika z priorytetem 4 i reguły lokalizacji z priorytetem 3, będzie miała zastosowanie reguła lokalizacji.

Ostrzeżenie
Upewnij się, że wziąłeś pod uwagę wrażliwe ustawienia, takie jak wykluczenia, szczegóły komunikacji czy proxy podczas tworzenia reguł.
Aby zachować kluczowe ustawienia z polityki urządzenia w polityce stosowanej przez przypisywanie reguł, zaleca się stosowanie dziedziczenia polityki.

Aby utworzyć nową regułę:

1. Idź do strony strony **Reguły Przypisania**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli.
3. Wybierz typ reguły:
   - Reguła lokalizacji
   - Reguła użytkownika
   - Reguła tagu
4. Skonfiguruj ustawienia reguł według potrzeb.
5. Kliknij **Zapisz**, aby zapisać zmiany i zastosować regułę do docelowych punktów końcowych polityki.

Aby zmienić ustawienia istniejącej reguły:

1. Na stronie **Przypisywanie Reguł**, znajdź regułę, której szukasz i kliknij jej nazwę, aby ją edytować.
2. Skonfiguruj ustawienia reguł według potrzeb.
3. Kliknij **Zapisz**, aby zastosować zmiany i zamknąć okno. Aby opuścić okno bez zapisywania zmian, naciśnij **Anuluj**.

Jeśli nie chcesz już dłużej korzystać z reguły, wybierz regułę i kliknij przycisk ⊖ **Kasuj** z górnej części tabeli. Zostaniesz poproszony o potwierdzenie czynności poprzez kliknięcie **Tak**.

Aby upewnić się, że zostają wyświetlane najnowsze informacje, kliknij przycisk ⟳ **Odśwież** z górnej części tabeli.

Konfigurowanie Reguł Lokalizacji

Lokalizacja jest segmentem sieci zidentyfikowanym przez jedno lub kilka ustawień sieciowych, takich jak określona brama, specyficzny DNS użyty do rozwiązywania adresów URL, lub podzbioru adresów IP. Na przykład, możesz określić lokalizacje, takie jak firmowy LAN, farmy serwerów lub dział.

W oknie konfiguracji reguły, wykonaj następujące kroki:

1. Wpisz sugestywną nazwę i opis reguły, którą chcesz stworzyć.

2. Ustaw priorytet reguły. Reguły są uporządkowane według priorytetu, pierwsza reguła ma najwyższy priorytet. Ten sam priorytet nie może być ustawiony dwa lub więcej razy.
3. Wybierz politykę, dla której tworzysz regułę przypisania.
4. Zdefiniuj lokalizacje, do których stosuje się regułę.
   a. Zaznacz typ ustawień sieci z menu w górnej stronie tabeli Lokalizacje. To są dostępne typy:

Typ	Wartość
Zakres adresów IP/IP	Specyficzne adresy IP w sieci lub podsieciach. Dla podsieci użyj formatu CIDR. Na przykład: `10.10.0.12` lub `10.10.0.0/16`
Adres bramy	Adres IP bramy
Adres serwera WINS	Adres IP serwera WINS **WAŻNE** Opcja ta nie ma zastosowania w systemach Linux i Mac.
Adres serwera DNS	Adres IP serwera DNS
Połączenie DHCP sufiksów DNS	Nazwa DNS bez nazwy hosta dla specyficznego połączenia DHCP Na przykład: `hq.company.biz`
Punkt końcowy może rozwiązać hosta	Nazwa hosta. Na przykład: `fileserv.company.biz`
Punkt końcowy może łączyć się do GravityZone	Tak/Nie
Typ sieci	Wireless/Ethernet Przy wyborze Wireless, możesz również dodać SSID sieci.

Typ	Wartość
	WAŻNE Opcja ta nie ma zastosowania w systemach Linux i Mac.

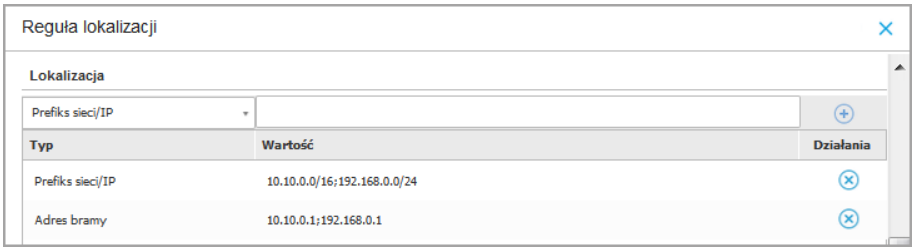
Nazwa hosta	Nazwa hosta
	Na przykład: `cmp.bitdefender.com`
	WAŻNE
	Możesz także używać wildcard. Gwiazdka (*) zastępuje zero lub więcej znaków, a znak zapytania (?) Zastępuje dokładnie jeden znak. Przykłady:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

b. Wprowadź wartość dla wybranego typu. W stosownych przypadkach, możesz wpisać wiele wartości w dedykowane pole, oddzielone średnikiem (;) i bez dodatkowych spacji. Na przykład, gdy wpisujesz `10.10.0.0/16;192.168.0.0/24`, reguła jest zastosowana do docelowego punktu końcowego z IP pasującymi do KAŻDEJ z tych podsieci.

Ostrzeżenie
Możesz użyć tylko jednego typu ustawienia sieci na regułę lokalizacji. Na przykład, jeśli dodasz lokalizację używając **prefiks IP/sieci**, nie możesz zastosować tego ustawienia ponownie w tej samej regule.

c. Kliknij przycisk **Dodaj** po prawej stronie tabeli.

Ustawienia sieciowe na punktach końcowych muszą być zgodne ze WSZYSTKIMI podanymi lokalizacjami, dla reguły, aby zastosować do nich. Na przykład, aby zidentyfikować sieć biurową LAN możesz wejść przez bramę, typ sieci i DNS, a ponadto, jeśli dodasz podsieć, możesz zidentyfikować dział w firmowym LAN.



Reguła lokalizacji

Kliknij pole **Wartość**, aby edytować istniejące kryteria, a następnie naciśnij `Enter`, aby zapisać zmiany.

Aby usunąć lokalizację, zaznacz ją i kliknij przycisk ⊗ **Usuń**.

5. Możesz wyłączyć niektóre lokalizacje z reguły. Aby utworzyć wykluczenia, zdefiniuj lokalizacje, które mają być wykluczone z reguły:
   a. Wybierz pole wyboru **Wykluczenia** z tabeli Lokalizacje.
   b. Wybierz typ ustawień sieci z menu znajdującego się w górnej części tabeli Wykluczenia. Aby uzyskać więcej informacji na temat opcji, odwołaj się do „Konfigurowanie Reguł Lokalizacji” (p. 226).
   c. Wprowadź wartość dla wybranego typu. Możesz wpisać wiele wartości w dedykowane pole, oddzielone średnikiem (;) i bez dodatkowych spacji.
   d. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli.

   Ustawienia sieciowe na punktach końcowych muszą pasować do WSZYSTKICH warunków dostarczonych w tabeli Wykluczenia, aby zastosować wykluczenia.

   Kliknij pole **Wartość**, aby edytować istniejące kryteria, a następnie naciśnij `Enter`, aby zapisać zmiany.

   Aby usunąć wyjątek, kliknij przycisk ⊗ **Usuń** po prawej stronie tabeli.
6. Kliknij **Zapisz**, aby zapisać regułę przypisania i ją zastosować.

   Po utworzeniu, reguła lokalizacji automatycznie stosuje się do wszystkich docelowych punktów końcowych, które są zarządzane.

Konfigurowanie Reguł Użytkownika

WAŻNE

- Możesz tworzyć reguły użytkownika tylko jeśli integracja Active Directory jest dostępna.
- Możesz zdefiniować reguły użytkownika tylko dla użytkowników i grup Active Directory. Reguły oparte na grupach Active Directory nie są wspierane na systemach Linux.

W oknie konfiguracji reguły, wykonaj następujące kroki:

1. Wpisz sugestywną nazwę i opis reguły, którą chcesz stworzyć.
2. Ustaw priorytet. Reguły są uporządkowane według priorytetu, pierwsza reguła ma najwyższy priorytet. Ten sam priorytet nie może być ustawiony dwa lub więcej razy.
3. Wybierz politykę, dla której tworzysz regułę przypisania.
4. W sekcji **Cele**, wybierz użytkowników i grupy bezpieczeństwa, do których chcesz przypisać regułę polityki. Możesz wyświetlić swój wybór w tabeli po prawej stronie.
5. Kliknij **Zapisz**.

   Po utworzeniu, reguła świadomości użytkownika dotyczy docelowych zarządzanych punktów końcowych przy logowaniu użytkownika.

Konfigurowanie Reguł Tagów

WAŻNE

Możesz tworzyć reguły znaczników tylko wtedy, gdy dostępna jest integracja z Amazon EC2 lub Amazon Azure.

Możesz użyć znaczników zdefiniowanych w infrastrukturze chmury, aby przypisać określoną strategię GravityZone do maszyn wirtualnych hostowanych w chmurze. Wszystkie maszyny wirtualne mające znaczniki określone w regule znacznika będą stosowane z zasadami ustawionymi przez regułę.

Notatka

Zgodnie z infrastrukturą chmury można zdefiniować znaczniki maszyny wirtualnej w następujący sposób:

- W przypadku Amazon EC2: na karcie **Tagi** w instancji EC2.
- W przypadku Microsoft Azure: w sekcji **Przegląd** na maszynie wirtualnej.

Reguła znacznika może zawierać jeden lub kilka znaczników. Aby stworzyć regułę znacznika:

1. Wpisz sugestywną nazwę i opis reguły, którą chcesz stworzyć.
2. Ustaw priorytet reguły. Reguły są uporządkowane według priorytetu, pierwsza reguła ma najwyższy priorytet. Ten sam priorytet nie może być ustawiony dwa lub więcej razy.
3. Wybierz politykę, dla której tworzysz regułę znacznika.
4. W tabeli **Tag** dodaj jeden lub kilka tagów.

   Tag składa się z pary klucz-wartość wrażliwej na wielkość liter. Upewnij się, że wprowadzasz tagi zgodnie z definicją w infrastrukturze chmury. Uwzględnione zostaną tylko prawidłowe pary klucz-wartość.

   Aby dodać tag:

   a. W polu **Klucz Tagu** wpisz nazwę klucza.

   b. W polu **Wartość Tagu** wpisz nazwę wartości.

   c. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli.

Przypisywanie Polityk NSX

W NSX polityki bezpieczeństwa są przypisane do grup zabezpieczeń. Grupa zabezpieczeń może zawierać różne obiekty vCenter, takie jak centra danych, klastry i maszyny wirtualne.

Aby przypisać politykę bezpieczeństwa do grupy zabezpieczeń:

1. Zaloguj się do sieci klienta vSphere.
2. Idź do **Sieć & Bezpieczeństwo > Service Composer**; i kliknij **Grupy bezpieczeństwa** zakładkę.
3. Utwórz dowolną liczbę grup bezpieczeństwa zgodnie z potrzebami. Aby uzyskać więcej informacji, należy zapoznać się z dokumentacja VMware.

   Można tworzyć dynamiczne grupy bezpieczeństwa na podstawie tagów bezpieczeństwa. W ten sposób możesz pogrupować wszystkie maszyny wirtualne znalezione jako zainfekowane.

4. Kliknij prawym przyciskiem myszy grupę zabezpieczeń, która cię interesuje i kliknij **Stosuj Politykę**.
5. Wybierz politykę, aby ją zastosować i kliknij **OK**.

7.1.3. Zmiany ustawień polityk.

Ustawienia polityki mogą zostać wstępnie skonfigurowane podczas tworzenia polityki. Później, możesz je zmienić, w zależności od potrzeb, kiedy tylko chcesz.

Notatka
Domyślnie, tylko użytkownik, który stworzył politykę może ją modyfikować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

Aby zmienić ustawienia istniejącej polityki:

1. Przejdź do strony **Polityki**.
2. Wybierz pożądany rodzaj punktu końcowego z selektora widoku.
3. Znajdź politykę poszukiwaną politykę na liście i naciśnij jej nazwę by edytować.
4. Skonfiguruj ustawienia polityki według uznania. Aby uzyskać szczegółowe informacje, odwołaj się do:
   - „Polityki Komputerów i Maszyn Wirtualnych” (p. 233)
   - „Polityki Urządzenia Przenośnego” (p. 390)
5. Kliknij **Zapisz**.

   Polityki są wysyłane do docelowych obiektów sieci zaraz po zmianie polityki przypisanej lub później modyfikując ustawienia polityki. Ustawienia powinny być zastosowane na obiektach sieci w mniej niż minutę (jeżeli są one online). Jeżeli obiekty sieciowe nie są online, ustawienia nie będą stosowane tak długo jak nie pojawią się online.

7.1.4. Zmienianie nazw polityk

Polityki powinny mieć sugestywne nazwy tak by administratorzy mogli szybko je zidentyfikować.

Aby zmienić nazwę polityki:

1. Przejdź do strony **Polityki**.

2. Wybierz pożądany rodzaj punktu końcowego z selektora widoku.
3. Naciśnij nazwę polityki. To otworzy stronę polityki.
4. Wprowadź nazwę nowej polityki.
5. Kliknij **Zapisz**.

Notatka
Nazwa polityki jest unikalna. musisz podać inną nazwę dla każdej nowej polityki.

7.1.5. Usuwanie polityki

Jeżeli dłużej nie potrzebujesz polityki, usuń ją. Kiedy polityka zostanie usunięta, obiekty sieci, do których się ją stosuje zostaną przypisane do polityki grupy dominującej. Jeśli żadna inna polityka nie jest stosowana, ostatecznie będzie egzekwowana polityka domyślna. Podczas usuwania polityki mającej dziedziczone sekcje przez inne polityki, ustawienia odziedziczonych sekcji są przechowywane na politykach podrzędnych.

Notatka
Domyślnie, tylko użytkownik, który stworzył politykę może ją skasować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

Aby móc usunąć politykę NSX z GravityZone Control Center, należy upewnić się, że polityka nie jest w użyciu. W związku z powyższym, należy przypisać docelową grupę zabezpieczeń z innym profilem bezpieczeństwa. Aby uzyskać więcej informacji, odwołaj się do „Przypisywanie Polityk NSX ” (p. 231).

Aby usunąć politykę:

1. Przejdź do strony **Polityki**.
2. Wybierz pożądany rodzaj punktu końcowego z selektora widoku.
3. Zaznacz pole wyboru polityki, którą chcesz skasować.
4. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Czynności należy potwierdzić, klikając **Tak**.

7.2. Polityki Komputerów i Maszyn Wirtualnych

Ustawienia polityki mogą zostać wstępnie skonfigurowane podczas tworzenia polityki. Później, możesz je zmienić, w zależności od potrzeb, kiedy tylko chcesz.

Aby skonfigurować ustawienia polityki:

1. Przejdź do strony **Polityki**.
2. Wybierz **Komputery i Wirtualne Maszyny** z selektora widoku.
3. Naciśnij nazwę polityki. To otworzy stronę ustawień polityki.
4. Skonfiguruj ustawienia polityki według uznania. Ustawienia są zorganizowane w poniższych sekcjach:
   - Ogólne
   - HVI
   - Antymalware
   - Sandbox Analyzer
   - Zapora Sieciowa
   - Ochrona sieci
   - Zarządzanie Aktualizacjami
   - Kontrola Aplikacji
   - Kontrola Urządzenia
   - Relay
   - Ochrona Exchange
   - Szyfrowanie
   - NSX
   - Ochrona pamięci

   Poruszaj się po sekcjach, korzystając z menu po lewej stronie.
5. Naciśnij **Zapisz** aby zapisać zmiany i zastosować je na komputerach docelowych. Aby opuścić stronę polityki bez zapisywania zmian, naciśnij **Anuluj**.

Notatka
Aby nauczyć się jak działają polityki, odwołaj się do „Zarządzanie politykami” (p. 219).

7.2.1. Ogólne

Ogólne ustawienia pomagają w zarządzaniu opcjami wyświetlania interfejsów użytkownika, ochroną haseł, ustawieniami proxy, ustawieniami power user, opcjami komunikacji i preferencjami aktualizacji dla docelowego punktu końcowego.

Ustawienia są zorganizowane w poniższych sekcjach:

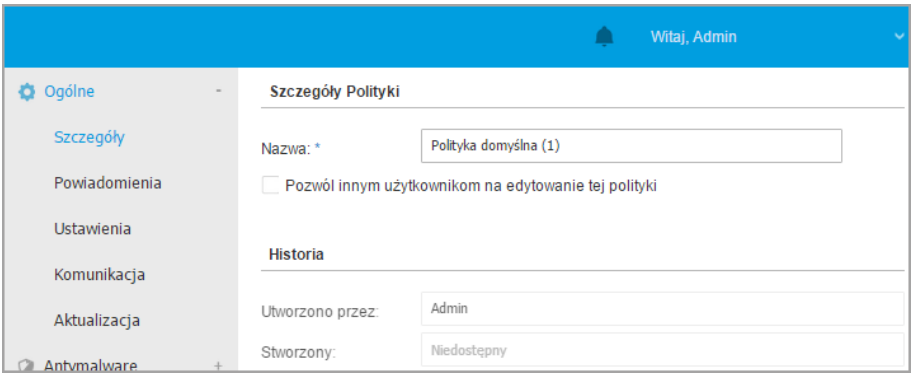
- Szczegóły
- Powiadomienia
- Ustawienia

- Komunikacja
- Aktualizacja

Szczegóły

Strona **Szczegóły** zawiera ogólne informacje o polityce:

- Nazwa polityki
- Użytkownik, który stworzył politykę
- Data i czas utworzenia polityki.
- Data i czas ostatniej modyfikacji polityki



Komputery i Polityki Maszyn Wirtualnych

Możesz zmienić nazwę polityki, wprowadzając nową nazwę w odpowiednim polu i kliknąć przycisk **Zapisz** w dolnej części strony. Polityki powinny mieć sugestywne nazwy tak by administratorzy mogli szybko je zidentyfikować.

Notatka
Domyślnie, tylko użytkownik, który stworzył politykę może ją modyfikować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

Reguły Dziedziczenia

Możesz ustawić sekcje, które mają być dziedziczone od innych polityk. Aby to zrobić:

1. Wybierz moduł i sekcję, które chcesz by aktualna polityka dziedziczyła. Wszystkie sekcje są dziedziczone, z wyjątkiem **Ogólne > Szczegóły**.
2. Określ politykę, z której chcesz dziedziczyć sekcję.
3. Kliknij przycisk **Dodaj** po prawej stronie tabeli.

Jeśli polityka źródłowa zostanie usunięta, dziedziczenie zostanie przerwane, a ustawienia odziedziczonych sekcji są przechowywane na polityce podrzędnej.

Odziedziczone sekcje nie mogą być dalej dziedziczone przez inne polityki. Rozważ następujący przykład:

Polityka A dziedziczy sekcję **Antymalware > Na żądanie** od polityki B. Polityka C nie może dziedziczyć sekcji **Antymalware > Na żądanie** od polityki A.

Informacje o Pomocy Technicznej

Możesz zastosować niestandardowe ustawienia obsługi technicznej i informacji kontaktowych dostępnych w agentach bezpieczeństwa w oknie **O programie** poprzez filtrowanie w odpowiednich polach.

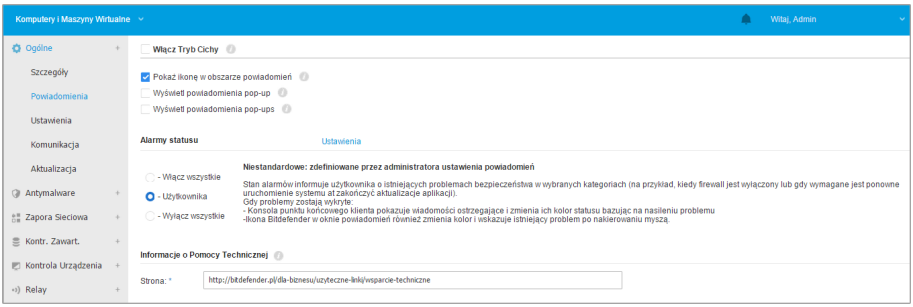
Aby skonfigurować adres e-mail w oknie **O programie**, tak aby otwierał on domyślną aplikację poczty e-mail na punkcie końcowym, musisz go dodać z prefiksem "mailto:" w polu **e-mail**. Na przykład: `mailto: name@domain.com`.

Użytkownicy mają dostęp do tej informacji z poziomu konsoli agenta bezpieczeństwa poprzez kliknięcie prawym klawiszem myszki na ikonie Bitdefender w pasku systemowym poprzez wybranie **O programie**.

Powiadomienia

W tej sekcji możesz skonfigurować opcje wyświetlania ochrony agentów Bitdefender w interfejsie w intuicyjny i wszechstronny sposób.

Przez jedno kliknięcie, możesz włączyć lub wyłączyć typ powiadomienia , zatrzymując tylko to co dla ciebie naprawdę ważne. Oprócz tego, na tej samej stronie, masz możliwość ustawienia kontroli widoczności problemów na punktach końcowych.



Polityki - Opcje wyświetlania

- **Tryb cichy.** Użyj pola wyboru aby włączyć lub wyłączyć Tryb Cichy. Tryb Cichy jest zaprojektowany by pomóc Ci łatwo wyłączyć interakcje z użytkownikiem w agencie bezpieczeństwa. Przełączając w tryb Cichy, poniższe zmiany zostaną wprowadzone do konfiguracji polityki:
  - Opcje **Wyświetl ikonę w obszarze powiadomień**, **Wyświetlaj powiadomienia pop-up** i **Wyświetlaj alerty pop-up** będą wyłączone w tej sekcji.
  - Jeżeli poziom ochrony zapory sieciowej jest ustawiony na **Zestaw reguł i zapytaj** lub **Zestaw reguł, znanych plików i zapytaj** można zmienić na **Zestaw reguł, znanych plików i zezwól**. W przeciwnym razie, ustawienia poziomu bezpieczeństwa nie zmienią się.
- **Pokaż ikonę w obszarze powiadomień.** Wybierz tę opcje aby wyświetlić ikonę Bitdefender B w obszarze powiadomień (znanym również jako zasobnik systemu) Ikona informuje użytkowników o ich statusie ochrony przez zmianę wyglądu i wyświetlenie odpowiedniego powiadomienia pop-up. Dodatkowo, użytkownicy mogą kliknąć prawym klawiszem myszy, w celu szybkiego otwarcia agenta bezpieczeństwa w głównym oknie lub oknie **O produkcie**.
- **Wyświetl powiadomienia pop-ups.** Użytkownicy są poinformowanie poprzez alarmy pop-ups o zdarzeniach w ochronie, które wymagają reakcji. Jeżeli wybierzesz, aby nie wyświetlać alertów pop-up, agent bezpieczeństwa automatycznie wykona zalecane działanie. Alerty pop-up są generowane w poniższych sytuacjach:
  - Jeżeli zapora sieciowa jest ustawiana aby prosić użytkownika o podjęcie działania kiedy nieznane aplikacje żądają dostępu do sieci lub internetu.

- Jeżeli Zaawansowana Kontrola Zagrożeń / System Wykrywania Włamań jest włączone, to zostaną wykryte potencjalnie niebezpieczne aplikacje.
- Jeżeli skanowanie urządzenia jest włączone, gdy zewnętrzne urządzenie magazynujące jest połączone z komputerem. Możesz skonfigurować te ustawienia w sekcji **Antymalware > Na żądanie**

- **Wyświetl powiadomienia pop-up.** W odróżnieniu od alarmów pop-ups, powiadomienia pop-ups informują użytkowników o różnorodnych zdarzeniach w ochronie. Powiadomienia pop-up znikną automatycznie po kilku minutach bez reakcji użytkownika.

  Wybierz **Wyświetl powiadomienia pop-ups**, następnie kliknij link**Pokaż Ustawienia Modułów** aby wybrać zdarzenia z odpowiednich modułów o których chcesz informować klienta. Są trzy typy powiadomień pop-ups, oparte na szkodliwości zdarzenia:

  - **Informacje**. Użytkownicy są informowani o istotnych, ale nieszkodliwych zdarzeniach w ochronie. Na przykład, aplikacja, która połączyła się z Internetem.
  - **Niski**. Użytkownicy są informowani na temat ważności zdarzeń ochrony, które mogą wymagać uwagi. Na przykład, Skanowanie na żądanie wykryło zagrożenie i plik został usunięty lub przeniesiony do kwarantanny.
  - **Krytyczny**. Te powiadomienia pop-ups informują użytkownika o niebezpiecznych sytuacjach, np kiedy skanowanie dostępowe wykryło zagrożenie i domyślna akcja w polityce to **Nic nie rób**, to malware, które są ciągle obecne na punkcie końcowym, lub proces aktualizacji, który nie mógł się ukończyć.

  Zaznacz pole wyboru związane z nazwą typu aby włączyć rodzaj pop-ups'ów dla wszystkich modułów naraz. Zaznacz pola wyboru związane z poszczególnymi modułami do włączania lub wyłączania konkretnych powiadomień.

  Lista modułów może się różnić w zależności od posiadanej licencji.

- **Widoczność Problemów na Punktach Końcowych.** Użytkownicy okreslają, kiedy ich punkt końcowy ma skonfigurować problemy bepzieczeństwa lub inne ryzyko bezpieczeństwa, bazujące na statusie alertów. Na przykład, użytkownucy moga zobaczyć jeżeli jest problem powiązany z ich ochroną antymalware, takie jak: moduł skanowania na żadanie jest wyłączony lub jest zaległe pełne skanownaie systemu. Użytkownicy są informowani o ich statusie ochrony w dwa sposoby:

– Sprawdzając obszar statusu głównego okna, które wyświetla odpowiedni status tekstowy oraz zmienia swój kolor w zależności od powagi zdarzenia bezpieczeństwa. Użytkownicy mają mozliwosc zobaczyć szczegóły problemów, przez kliknięcie dostepnego przycisku.

– Sprawdzanie ikony Bitdefender w zasobniku systemowym, który zmienia swój wygląd po wykryciu problemu.

Agent bezpieczeństwa Bitdefender wykorzystuje następujące schamaty kolorów w obszarze powiadomień:

– Zielone: Żadne problemy nie zostały wykryte.

– Żółty: Punkt końcowy nie posiada żadnych krytycznych zdarzeń mogących wpłynąć na bezpieczeństwo. Użytkownicy nie muszą przerywać swojej pracy aby rozwiązać problemy.

– Czerwony: Punkt końcowy ma krytyczne problemy, które wymagają natychmiastowego działania.

Wybierz **Widoczność Problemów na Punkcie Końcowym** , potem kliknij link **Pokaż Ustawienia Modułów** aby dostosować status alertów wyświetlonych w interfejsie użytkownika w agencie Bitdefendera.

Dla każdego modułu, można wybrać pokazywanie alertu jako ostrzeżenie lub krytyczne zdarzenie, lub nie wyświetlać ich w ogóle. Opcje są opisane tutaj:

– **Ogólne**. Status alertu jest generowany ilekroć wymagane jest ponowne uruchomienie komputera lub po instalacji produktu, jak również gdy agent bezpieczeństwa nie może połączyć się do Usługi Serwisowej Cloud Bitdefender.

– **Antimalware**. Alerty są generowane w poniższych sytuacjach:

  - Skanowanie na żądanie jest dostępne ale wiele lokalizacji plików jest pomijana.
  - Określona liczba dni, która minęła od ostatniego pełnego skanowania systemy wykonanego na maszynie.

    Możesz wybrć jak wyświetlać alerty i zdefiniować liczbę dni od ostatniego pełnego skanowania.
  - Wymagane jest ponownie uruchomienie, aby zakończyć proces dezynfekcji.

- **Zapora sieciowa**. Alarm ten jest generowany, gdy Moduł Firewall jest wyłączony.
- **Kontrola aplikacji**. Status alarmu jest generowany, gdy moduł Kontrola aplikacji jest modyfikowany.
- **Kontrola zawartości**. Alarm ten jest generowany, gdy Moduł Kontrola Treści jest wyłączony.
- **Aktualizacja**. Alarm jest generowany, kiedy system wymaga ponownego uruchomienie aby zakończyć operacje aktualizacji.

- **Powiadomienie o Restarcie Punktu Końcowego.** Ta opcja wyświetla ostrzeżenie o ponownym uruchomieniu na punkcie końcowym za każdym razem, gdy wymagane jest ponowne uruchomienie systemu z powodu zmian dokonanych w punkcie końcowym przez moduły GravityZone wybrane w ramach ustawień modułowych.

  Notatka
  Punkty końcowe wymagające ponownego uruchomienia systemu mają określoną ikonę stanu ( ) w inwentarzu GravityZone

  Możesz dodatkowo dostosować alerty restartu, klikając na **Pokaż ustawienia modułowe**. Dostępne są następujące opcje:

  - **Aktualizacja** - Wybierz tę opcję, aby aktywować powiadomienia o ponownym uruchomieniu aktualizacji agenta.
  - **Zarządzanie Aktualizacjami** - Wybierz tę opcję, aby aktywować powiadomienia o ponownym uruchomieniu instalacji poprawki.

  Notatka
  Możesz także ustawić limit czasu, przez który użytkownik może odłożyć restart. Aby to zrobić, wybierz **Automatycznie uruchom ponownie maszynę po** i wstaw wartość od 1 do 46.

  Alert o ponownym uruchomieniu wymaga, aby użytkownik wybrał jedno z następujących działań:

  - **Zrestartuj teraz**. W takim przypadku system zostanie natychmiast uruchomiony ponownie.
  - **Przełóż ponowne uruchomienie**. W takim przypadku powiadomienie o ponownym uruchomieniu pojawi się okresowo, dopóki użytkownik nie

zrestartuje systemu lub dopóki nie upłynie czas ustawiony przez administratora firmy.

Ustawienia

W tej sekcji możesz konfigurować nastepujące ustawienia:

- **Konfiguracja hasła.** Aby uniemożliwić użytkownikom z prawami administracyjnymi odinstalowanie ochrony, należy ustawić hasło.

  Hasło dezinstalacji może zostać skonfigurowana przed instalacją, dostosowując pakiet instalacyjny. Jeżeli to zrobisz, wybierz **Zatrzymaj ustawienia instalacyjne**, aby zachować obecne hasło.

  Aby ustawić hasło, albo zmienić obecne hasło, wybierz **Włącz hasło** i podaj wybrane hasło. Aby usunąć ochronę hasłem, wybierz **Wyłącz hasło**.

- **Konfiguracja proxy**

  Jeżeli twoja sieć znajduje się za serwerem proxy, musisz zdefiniować ustawienia proxy, które pozwolą punktowi końcowemu komunikować się z komponentami rozwiązania GravityZone. W tym wypadku, musisz włączyć opcję **Konfiguracja Proxy** i wypełnić wymagane parametry:
  - **Serwer** — wprowadź IP serwera proxy
  - **Port** - wpisz port używany do połączenia z serwerem proxy.
  - **Nazwa użytkownika** – wprowadź nazwę użytkownika rozpoznaną przez proxy.
  - **Hasło** - wprowadź poprawne hasło dla określonego użytkownika

- **Power User**

  Moduł Power User umożliwia uprawnienia administratora na poziomie punktu koncowego, umożliwiając użytkownikowi dostęp do punktów końcowych i modyfikację ustawień polityki za pomocą lokalnej konsoli, przez interfejs Bitdefender Endpoint Security Tools.

  Jeżeli chcesz aby konkretny punkt końcowy posiadał prawa Power User, musisz w pierwszej kolejności uwzględnić ten moduł w agencie bezpieczeństwa instalowanym na docelowym punkcie końcowym. Po tym, musisz skonfigurować ustawienia Power User w politykach stosowany dla tych punktów końcowych:

  WAŻNE
  Moduł Power User jest dostępny jedynie dla wspieranych pulpitów Windows i systemów operacyjnych serwerów.

1. Uruchom opcję **Power User**.
2. Zdefiniuj hasło dla Power User w polach poniżej.

   Użytkownicy korzystający z trybu Power User z lokalnego punktu końcowego otrzymają monit o konieczności wprowadzenia zdefiniowanego hasła.

Aby uzyskać dostęp do modułu Power User, musimy kliknąć prawym klawiszem ikonę Bitdefenderz zasobnika systemu i wybrać **Power User** z menu kontekstowego. Po podaniu hasła w oknie logowania, konsola zawierająca aktualnie zaaplikowane polityki ustawień będzie wykazywała, które z opcji użytkownik punktu końcowego może zobaczyć i zmodyfikować w opcjach polityk.

Notatka
Tylko do niektórych opcje bezpieczeństwa możemy mieć dostęp lokalnie za pośrednictwem konsoli Power Usera, zawierającej moduły Antymalware, Zaporę Sieciową, Kontrolę Zawartości i Kontrolę Urządzeń.

Aby przywrócić zmiany dokonane w module Power User:

– W Control Center, otwórz szablony polityk przypisane do punktu końcowego, który posiada uprawnienia Power User i kliknij **Zapisz**. W ten sposób, oryginalne ustawienia zostaną zastąpione w docelowym punkcie końcowym.
– Przypisz nową politykę do punktu końcowego posiadając uprawnienia Power User.
– Zaloguj się na lokalnym punkcie końcowym, otwórz konsolę Power user i kliknij **Resync**.

Aby z łatwością odnaleźć punkt końcowy z politykami zmodyfikowanymi w trybie Power User:

– Na stronie **Sieć**, kliknij menu **Filtry** i wybierz opcję **Edytowanie przez Power User** z zakładki **Polityki**.
– Na stronie **Sieć**, kliknij pożądany punkt końcowy w wyświetlanym oknie **Informacje**. Jeżeli polityki były modyfikowane w trybie Power User, zostanie wyświetlone powiadomienie w zakładce **Ogólne** w sekcji > **Polityki**.

WAŻNE
Moduł Power User został swoiście zaprojektowany w celach rozwiązywania problemów, pozwala administratorowi sieci na łatwy wgląd i zmianę ustawień polityk lokalnego komputera. Przypisywanie praw Power User innym

użytkownikom w firmie musi być ograniczone do autoryzowanego personelu, dla zapewnienia bezpieczeństwa stosowanych polityk na wszystkich punktach roboczych w firmowej sieci.

- **Opcje**

  W tej sekcji możesz zdefiniować nastepujące ustawienia:

  – **Usuń zdarzenia starsze niż (dni).** Agent bezpieczeństwa Bitdefender przechowuje szczegółowe logi zdarzeń dotyczących ich aktywności na komputerze (również zawiera aktywności na komputerze ustawiane w Kontroli Zawartości). Domyślnie, zdarzenia są usuwane z dziennika po 30 dniach. Jeżeli chcesz zmienić przedział, wybierz inne opcje z menu.

  – **Złóż raport o awariach do Bitdefender.** Wybierz tę opcję, żeby raport został przesłany do Laboratorium analizy Bitdefender jeżeli agent bezpieczeństwa ulegnie awarii. aporty pomogą naszym inżynierom znaleźć co jest powodem problemu i zapobiec jego wystąpienia następnym razem. Żadne prywatne informacje nie zostaną wysłane.

  – **Wyślij podejrzane pliki wykonywalne do analizy.** Wybierz tę opcję, aby pliki, które wydają się niegodne zaufania lub podejrzanie się zachowują będą wysyłane do Laboratoriów Bitdefender do analizy.

  – **Przekazuj naruszenia pamięci HVI do Bitdefender.** Domyślnie HVI wysyła anonimowe informacje dotyczące wykrytych naruszeń do Serwerów Cloud Bitdefender. Informacje te są wykorzystywane w statystykach oraz w celu poprawiania wskaźników wykrywania produktów. Jeśli nie chcesz przesyłać takich informacji ze swojej sieci, możesz wyczyścić to pole wyboru.

Komunikacja

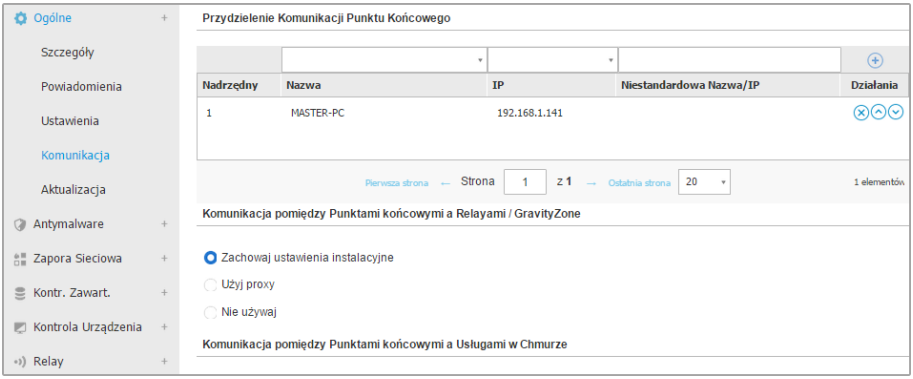
W tej sekcji, możesz przypisać jedną lub więcej maszyn relay docelowemu punktowi końcowemu, po czym skonfigurować preferencje proxy w celu ustawienia komunikacji docelowego punktu końcowego i GravityZone.

Przydzielenie Komunikacji Punktu Końcowego

Gdy serwery komunikacyjne instalowane są na urządzeniu GravityZone, możesz przypisać im docelowe komputery zawierające jeden lub więcej serwerów komunikacyjnych poprzez politykę. Dostępne punkty końcowe relay, które służą jako serwery komunikacyjne, są również brane pod uwagę.

Aby przypisać serwery komunikacji do docelowych komputerów:

1. W tabeli **Przypisanie Komunikacji Punktu końcowego** naciśnij pole **Nazwa**. Wyświetlono listę wykrytych serwerów komunikacji.
2. Wybierz jednostkę.



Polityki Komputerów i Maszyn Wirtualnych - Ustawienia Komunikacji

3. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli.

   Serwer komunikacji został dodany do listy. Wszystkie komputery docelowe będą komunikować się z Control Center tylko przez określony serwer komunikacji.
4. Zrób te same kroki, aby dodać kilka serwerów komunikacyjnych, jeżeli jest to możliwe.
5. Możesz skonfigurować priorytet serwerów komunikacji używając strzałek góra i dół dostępnych po prawej stronie każdego wpisu. Komunikacja z docelowymi komputerami będzie przeprowadzona przez jednostkę na górze listy. Gdy nie można skomunikować się z tym wpisem, następny zostanie wzięty do konta.
6. Aby usunąć wpis z listy, naciśnij przycisk ⊗ **Usuń** po prawej stronie tabeli.

Komunikacja między Punktami Końcowymi a Relayami / GravityZone

W tej sekcji, możesz konfigurować preferencje proxy dla komunikacji pomiędzy docelowymi punktami końcowymi i przypisanymi maszynami relay, lub pomiędzy docelowymi punktami końcowymi, a urządzeniami GravityZone (gdy żaden relay nie został przypisany):

- **Zachowaj ustawienia instalacyjne**, w celu zachowania tych samych ustawień proxy zdefiniowanych wraz z paczką instalacyjną.
- **Użyj zdefiniowanego w Głównej sekcji proxy**, aby użyć ustawień zdefiniowanych dla aktualnej polityki, pod sekcją **Ogólne > Ustawienia**.
- **Nie stosuj**, gdy docelowy punkt końcowy nie komunikuje z określonym komponentem GravityZone za pośrednictwem proxy.

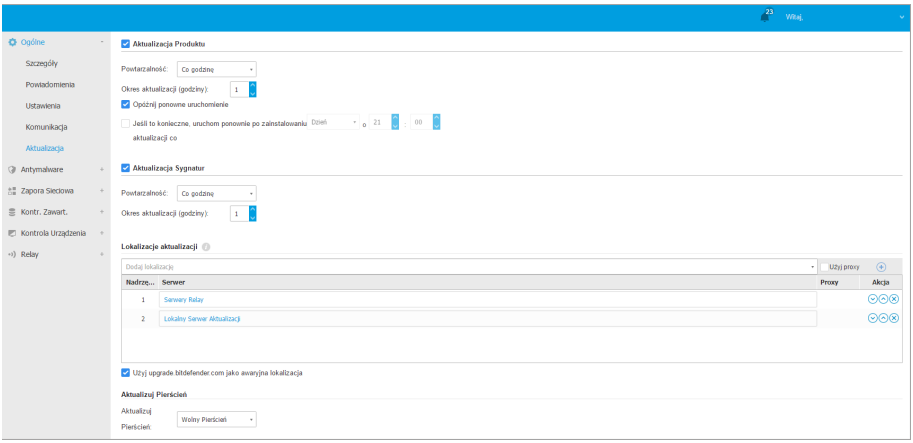
Komunikacja pomiędzy Punktami końcowymi a Usługami w Chmurze

W tej sekcji, możesz skonfigurować ustawienia proxy dla komunikacji między docelowym punktem końcowym, a Usługami Cloud Bitdefender (wymaga połączenia internetowego):

- **Zachowaj ustawienia instalacyjne**, w celu zachowania tych samych ustawień proxy zdefiniowanych wraz z paczką instalacyjną.
- **Użyj zdefiniowanego w Głównej sekcji proxy**, aby użyć ustawień zdefiniowanych dla aktualnej polityki, pod sekcją **Ogólne > Ustawienia**.
- **Nie stosuj**, gdy docelowy punkt końcowy nie komunikuje z określonym komponentem GravityZone za pośrednictwem proxy.

Aktualizacja

Aktualizacje są bardzo ważne ponieważ umożliwiają zwalczanie najnowszych zagrożeń. Bitdefender publikuje wszystkie aktualizacje produktów i treści zabezpieczeń za pośrednictwem serwerów Bitdefender w Internecie. Wszystkie aktualizacje są zaszyfrowane i podpisane cyfrowo, żeby nie można nimi było manipulować. Kiedy nowa aktualizacja jest dostępna, agent ochrony Bitdefendera sprawdza cyfrowe sygnatury aktualizacji pod kątem autentyczności i integralności zawartości pakietu. Następnie, każdy plik aktualizacji jest parsowany a jego wersja sprawdzona w porównaniu z zainstalowanym. Nowsze pliki są pobierane lokalnie i sprawdzane pod kątem ich MD5 hash, aby się upewnić, że nie są zmienione. W tej sekcji możesz skonfigurować agenta zabezpieczeń Bitdefender i ustawienia aktualizacji zawartości zabezpieczeń.



Polityki Komputerów i Maszyn Wirtualnych - Opcje Aktualizacji

- **Aktualizacja Produktu.** Agent bezpieczeństwa Bitdefender automatycznie sprawdza co godzinę w poszukiwaniu dostępnych nowych aktualizacji, pobiera je i instaluje. Automatyczne aktualizacje są wykonywane w tle.
  - **Powtarzalność**. Aby zmienić częstotliwość automatycznej aktualizacji, wybierz inną opcję z menu i skonfiguruj ją według własnych potrzeb w kolejnych polach.
  - **Przełóż ponowne uruchomienie**. Niektóre aktualizacje wymagają restartu systemu aby mogły zostać zainstalowane i działać poprawnie. Domyślnie, produkt będzie pracował ze starymi plikami aż do restartu komputera, po którym zastosowane zostaną najnowsze aktualizacje. Powiadomienie w interfejsie użytkownika poinformuje go, za każdym razem kiedy aktualizacja wymaga restartu systemu. Jest zalecany aby zostawić tą opcję włączoną. W innym przypadku, system automatycznie zrestartuje system po zainstalowaniu aktualizacji, jeśli ona tego wymaga. Użytkownicy będą powiadomieni aby zapisać swoją pracę, ale restart nie może być anulowany.
  - Jeżeli zdecydujesz się uruchomić ponownie później, możesz ustawić dogodny czas, w którym komputer automatycznie uruchomi się ponownie, jeżeli nadal będzie potrzebował. Może to być bardzo przydatne dla serwerów. Wybierz **Jeżeli potrzeba, uruchom ponownie po instalacji aktualizacji** i określ, kiedy jest to wygodne aby ponownie uruchomić komputer (codziennie lub co tydzień w określonym dniu, o określonej porze dnia).

- **Aktualizacja Zawartości Zabezpieczeń.** Treść dotycząca bezpieczeństwa odnosi się do statycznych i dynamicznych środków wykrywania zagrożeń, takich jak między innymi silniki skanowania, modele uczenia maszynowego, heurystyki, reguły, podpisy i czarne listy. Agent zabezpieczeń Bitdefender automatycznie sprawdza aktualizację zawartości zabezpieczeń co godzinę (ustawienie domyślne). Automatyczne aktualizacje są wykonywane w tle. Aby zmienić częstotliwość automatycznej aktualizacji, wybierz inną opcję z menu i skonfiguruj ją według własnych potrzeb w kolejnych polach.
- **Lokalizacje aktualizacji**. Domyślną lokalizacją aktualizacji agentów bezpieczeństwa Bitdefender jest lokalny serwer aktualizacji GravityZone. Dodaj lokalizacje aktualizacji albo wybierając predefiniowaną lokację z listy rozwijalnej albo podając IP lub nazwę hosta jednego lub więcej serwerów aktualizacji z twojej sieci. Skonfiguruj ich priorytet korzystając z przycisków góra i dół lub przewiń myszką. Jeżeli pierwsza lokalizacja aktualizacji jest niedostępna, następna zostanie sprawdzona i tak dalej.

  Aby ustawić adres lokalnych aktualizacji:

  1. Wprowadź adres serwera aktualizacji w polu **Dodaj lokalizację**. Możesz:
     - Wybierz predefiniowaną lokalizację:
       - **Serwery Relay**. Punkt końcowy będzie automatycznie łączyć się z jej przypisanym Relay Server.

         Ostrzeżenie
         Serwery Relay nie są obsługiwane w starszych systemach operacyjnych. Aby uzyskać więcej informacji, zapoznaj się z Instrukcją instalacji.

         Notatka
         Można sprawdzić przypisany Server Relay w **Informacje** oknie. Bardziej szczegółowe informacje znajdują się Viewing Computer Details.

       - **Lokalny serwer aktualizacji**
     - Wprowadź adres IP lub nazwę hosta jednego lub kilku serwerów aktualizacji w Twojej sieci. Użyj jednej z tych składni:
       - `aktualizacja_serwer_ip:port`
       - `aktualizacja_serwer_nazwa:port`

Domyślny port 7074.

Pole wyboru **Użyj serwera Bitdefender jako awaryjnego** jest zaznaczone domyślnie. Jeśli aktualizacja lokalizacji jest niedostępna, lokalizacja awaryjna zostanie wykorzystana.

Ostrzeżenie
Wyłączanie lokalizacji awaryjnej zatrzyma automatyczne aktualizacje, pozostawiając Twoją sieć podatną, gdy przewidziane miejsca są niedostępne.

2. Jeżeli klient komputerów łączy się do lokalnego serwera aktualizacji przez serwer proxy, wybierz **Użyj Proxy**.
3. Kliknij przycisk **Dodaj** po prawej stronie tabeli.
4. Użyj strzałek Góra / Dół w kolumnie **Akcja** aby ustawić priorytety zdefiniowanych lokalizacji aktualizacji. Jeżeli pierwsza lokalizacja aktualizacji nie jest dostępna, następna jest brana pod uwagę i tak dalej.

Aby usunąć lokalizację z listy, kliknij odpowiedni przycisk **Usuń**. Można usunąć domyślną lokalizacje, jednak nie jest to zalecane.

- **Pierścień Aktualizacji.** Można rozwijać aktualizację produktów w etapach, przy użyciu aktualizacji pierścieni:
  - **Wolny Alert**. Maszyny z slow ring policy otrzymają aktualizację w późniejszym terminie, w zależności od odpowiedzi otrzymanej od fast ring endpoints. Jest to środek zapobiegawczy w procesie aktualizacji. To jest ustawienie domyślne.
  - **Szybki Alert**. Maszyny z polityką szybkich alertów otrzyma najnowsze dostępne aktualizacje. To ustawienie jest rekomendowane dla niekrytycznych maszyn w produkcji.

WAŻNE
- W mało prawdopodobnym przypadku, kiedy problem występuje on the fast ring na maszynach z konkretnej konfiguracji, zostanie ustalona przed the slow ring update.
- BEST for Windows Legacy nie obsługuje stagingu. Starsze punkty końcowe w lokalizacji stagingu muszą zostać przeniesione do miejsca produkcji.

Notatka
Aby uzyskać szczegóły jak alerty aktualizacji wpływają na staging, patrz rozdział **Aktualizuj GravityZone > Staging** z Przewodnik Instalacji GravityZone.

7.2.2. HVI

Notatka
HVI dostarcza ochronę tylko dla maszyn wirtualnych na hypervisor'ach Citrix Xen .

Hypervisor Memory Introspection chroni maszyny wirtualne przed zaawansowanymi zagrożeniami, których silniki oparte na sygnaturach nie mogą pokonać. To zapewnia ochronę w czasie rzeczywistym przed atakami, poprzez monitorowanie procesów z zewnętrzych systemów operacyjnych gościa. Mechanizm ochrony zawiera kilka opcji do blokowania ataków, które się zdarzą i natychmiast usuwane jest zagrożenie.

Zgodnie z zasadą rozdziału pamięci systemów operacyjnych, HVI zawiera również dwa moduły ochrony zorganizowane w powiązanych kategoriach:

- Przestrzeń Użytkownika, adresowanie normalnych procesów aplikacji użytkownika.
- Przestrzeń Kernel, adresowanie zastrzeżonych procesów do rdzenia systemu operacyjnego.

Dodatkowo polityka HVI obejmuje dwie funkcje ułatwiające zarządzanie bezpieczeństwem i utrzymanie chronionych maszyn wirtualnych:

- Wykluczenia, do przeglądania i zarządzania procesami, z wyjątkiem skanowania.
- Narzędzia Niestandardowe, do wstrzykiwania narzędzi, które są konieczne podczas czynności operacyjnych i kryminalistycznych, wewnątrz systemów operacyjnych gościa.

Przestrzeń Użytkownika

W tej sekcji możesz konfigurować ustawienia ochrony dla procesów uruchomionych w pamięci użytkownika.

Użyj pole wyboru **Introspekcja Pamięci Przestrzeni Użytkownika**, aby włączyć lub wyłączyć ochronę.

Funkcjonalność tego modułu opiera się na regułach, dzięki czemu można skonfigurować ochronę oddzielnie dla różnych grup procesów. Dodatkowo, możesz wybrać opcje zbierania bardziej szczegółowych informacji.

- Reguły przestrzeni użytkownika
- Informacje Śledcze

Reguły przestrzeni użytkownika

Moduł jest wyposażony w zestaw predefiniowanych reguł, które dotyczą najbardziej wrażliwych aplikacji. Tabela w tej sekcji zawiera listę obowiązujących reguł, zapewniając ważne informacje na temat każdego z nich:

- Nazwa reguły
- Procesowanie reguły stosuje się do
- Tryb monitorowania
- Akcja, która blokuje wykryty atak
- Działania, aby usunąć zagrożenie

Możesz także dostarczyć listę niestandardowych reguł dla procesów, które chcesz monitorować. Aby utworzyć nową regułę:

1. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Ta akcja otwiera okno konfiguracyjne reguły.
2. Konfiguruj moduł używając następujących ustawień reguł:
   - **Nazwa Reguły.** Podaj nazwę pod którą reguła będzie przypisana w tabeli reguł. Na przykład, dla procesów takich jak `firefox.exe` lub `chrome.exe`, możesz nazwać regułę `Przeglądarki`.
   - **Procesy.** Wprowadź nazwy procesów, które chcesz monitorować, oddzielone średnikiem (;).
   - **Tryb monitoringu.** Dla szybkiej konfiguracji, kliknij poziom bezpieczeństwa, który najlepiej pasuje Twoim potrzebom (**Agresywny**, **Normalny** lub **Tolerancyjny**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

     Możesz szczegółowo konfigurować ustawienia modułu wybierając poziom ochrony **Użytkownika** i wybierając jedną lub więcej z następujących opcji:

     – **Hooks są ustawione na krytyczne DLL w trybie użytkownika.** Wykrywają iniekcje DLL, które ładują złośliwy kod do procesu wywołującego.

- **Rozpakowywanie/odszyfrowywanie prób w głównym pliku wykonywalnym.** Wykrywa próby rozszyfrowania kodu w głównym procesie wykonywalnym i chroni proces przed zmianą złośliwym oprogramowaniem.
- **Obcy wewnątrz procesu docelowego.** Chroni przed wstrzyknięciem kodu w procesie chronionym.
- **Exploity.** Wykrywają niezamierzone zachowanie procesów spowodowanych przez eksploatację błędu lub wcześniej nieujawnionych podatności. Użyj tej opcji, jeśli chcesz monitorować kod wykonywany ze sterty i stosu chronionych aplikacji.
- **Hookowanie WinSock.** Zablokuj przypadki wykrycia sieci bibliotek (DLL) używane przez system operacyjny, zapewniając komunikację TCP/IP.

- **Akcje.** Istnieje wiele działań, które można podjąć na wykrytych zagrożeniach. Każde działanie ma z kolei kilka możliwych rozwiązań lub działań dodatkowych. Znajdź je opisane tutaj:
  - **Pierwotne działanie.** To jest podjęcie natychmiastowych działań, które można podjąć, gdy atak zostanie wykryty na komputerze gościa, co pozwala go zablokować. To są dostępne opcje:
    - **Log.** Rejestruje tylko zdarzenia w bazie danych. W tym przypadku będziesz otrzymywać tylko powiadomienia (jeśli jest skonfigurowane) i będziesz w stanie wyświetlić zdarzenie w raporcie **Aktywność HVI**.
    - **Odmów.** Odrzuć wszelkie próby zagrożenia do alertu procesu docelowego.
    - **Zamknij Maszynę.** Wyłącz maszynę wirtualną, na której przebiega proces docelowy.

      WAŻNE
      Jest zalecane ustawić główną akcje pierw w **Dziennik**. Wtedy używaj polityki przez odpowiednią ilość czasu aby upewnić się, że wszystko działa zgodnie z oczekiwaniami. Następnie można wybrać jakiekolwiek działanie, jakie należy podjąć w przypadku wykrycia naruszenia pamięci.

  - **Działanie naprawcze.** W zależności od wybranej opcji, Security Server wstrzykuje narzędzie naprawcze w systemie operacyjnym gościa. Narzędzie automatycznie rozpocznie skanowanie w poszukiwaniu

złośliwego oprogramowania, a po wykryciu zagrożenia, postępuje z wybraną akcją. To są dostępne opcje:

- **Dezynfekuj.** Usuń złośliwy kod z zainfekowanych plików. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach.
- **Usuń.** Usuwa wykryte pliki z dysku, bez żadnego ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Ignoruj.** Narzędzie naprawcze wykrywa i tylko raportuje wykryte pliki.
- **Żaden.** Narzędzie naprawcze nie zostanie wprowadzone do systemu operacyjnego gościa.

Notatka
Zamknięcie narzędzia usunie je z systemu, a także nie pozostawi żadnych śladów w systemie operacyjnym gościa.

– **Akcja naprawy backupu.** Gdy akcja naprawy nie powiodła się, możesz wybrać inne działania naprawcze z dostępnych opcji.

3. Kliknij **Zapisz**.

Po utworzeniu, możesz edytować regułę w dowolnym momencie. Klikając nazwę reguły otworzy się okno konfiguracyjne.

GravityZone pozwala również na szybką konfigurację Introspekcji Pamięci zachowania w momencie wykrycia, zmieniając kilka reguł na raz. Aby ustawić wiele reguł z tymi samymi akcjami:

1. Wybierz reguły, które chcesz zmienić.
2. Kliknij przycisk **Akcja lub Naprawa** w górnej części tabeli.
3. Wybierz opcję dla każdego działania.
4. Kliknij **Zapisz**. Nowe akcje wejdą w życie po zapisaniu polityki, pod warunkiem że maszyny docelowe są online.

Aby usunąć jedną lub kilka reguł z listy, wybierz je i kliknij przycisk ⊗ **Usuń** z górnej strony tabeli.

Informacje Śledcze

Wybierz pole wyboru **Zdarzenia awarii aplikacji** pod tabelą reguł przestrzeni użytkownika aby zezwolić na zebranie szczegółowych informacji w trakcie usuwania aplikacji.

Można zobaczyć tę informację w HVI sprawozdaniu z działalności i znaleźć powód, który spowodował zamknięcie aplikacji. Jeżeli zdarzenie jest związane z atakiem, jego detale pojawią się pogrupowane z innymi zdarzeniami, pod odpowiednim incydentem, który prowadzi do zdarzenia.

Przestrzeń Jądra

HVI chroni kluczowe elementy systemu operacyjnego, takie jak:

- Krytyczne sterowniki jądra i związane z nimi obiekty napędu, obejmujące szybkie I/O tabele wysyłkowe związane ze sterownikami rdzenia.
- Sterowniki sieciowe, których zmiana pozwoliłaby na przechwytywanie ruchu przez złośliwe oprogramowanie i na wstrzyknięcie szkodliwych składników w strumień ruchu.
- Obraz jądra systemu operacyjnego obejmujący następujące: sekcję kodu, sekcję danych i sekcję tylko do odczytu, w tym Import Tabeli Adresów (IAT), Eksport Tabeli Adresów (EAT) i zasoby.

W tej sekcji możesz konfigurować ustawienia ochrony dla procesów uruchomionych w pamięci jądra.

Użyj pole wyboru **Introspekcja Pamięci Przestrzeni Jądra**, aby włączyć lub wyłączyć ochronę.

Dla szybkiej konfiguracji, wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (**Agresywny**, **Normalny** lub **Tolerancyjny**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

Możesz szczegółowo konfigurować ustawienia modułu wybierając poziom ochrony **Użytkownika** i wybierając jedną lub więcej z następujących opcji:

- **Rejestry kontrolne**. Rejestry Kontroli (CR), to rejestry procesora sterujące ogólnym zachowaniem procesora lub innego cyfrowego urządzenia. Wybierz tę opcję, aby wykrywać próby ładowania nieprawidłowych wartości do określonych Rejestrów Kontroli.
- **Model określonych rejestrów**. Rejestry te odnoszą się do każdego z poszczególnych rejestrów kontrolnych w zestawie instrukcji x86 używanych

do debugowania, śledzenia wykonania programu, monitorowania wydajności komputera i przełączania niektórych funkcji CPU. Wybierz tę opcję, aby wykryć próby zmiany tych rejestrów.

- **Integralność IDT/GDT**. Tabele Opisów Globalnych i Przerwań (ITD/GDT) są wykorzystywane przez procesor w celu określenia właściwej odpowiedzi na przerwania i wyjątki. Wybierz tę opcję, aby wykryć jakiekolwiek próby zmiany tych tabel.
- **Ochrona antymalware sterowników.** Wybierz tę opcję, aby wykryć próby ostrzegania sterowników wykorzystywanych przez oprogramowanie antymalware.
- **Ochrona sterowników Xen.** Wybierz tę opcję, aby wykryć próby ostrzegania sterowników hypervisora Citrix XenServer.

Istnieje wiele działań, które można podjąć na wykrytych zagrożeniach. Każde działanie ma z kolei kilka możliwych rozwiązań lub działań dodatkowych. Znajdź je opisane tutaj:

- **Pierwotne działanie.**
  - **Log.** Rejestruje tylko zdarzenia w bazie danych. W tym przypadku będziesz otrzymywać tylko powiadomienia (jeśli jest skonfigurowane) i będziesz w stanie wyświetlić zdarzenie w raporcie **Aktywność Introspekcji Pamięci**.
  - **Odmów.** Odrzuć wszelkie próby zagrożenia do alertu procesu docelowego.
  - **Zamknij Maszynę.** Wyłącz maszynę wirtualną, na której przebiega proces docelowy.

  WAŻNE
  Jest zalecane ustawić główną akcje pierw w **Dziennik**. Wtedy używaj polityki przez odpowiednią ilość czasu aby upewnić się, że wszystko działa zgodnie z oczekiwaniami. Następnie można wybrać jakiekolwiek działanie, jakie należy podjąć w przypadku wykrycia naruszenia pamięci.

- **Działanie naprawcze.**
  - **Dezynfekuj.** Usuń złośliwy kod z zainfekowanych plików. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach.
  - **Usuń.** Usuwa wykryte pliki z dysku, bez żadnego ostrzeżenia. Wskazane jest, aby unikać tego działania.

- **Ignoruj.** Narzędzie naprawcze wykrywa i tylko raportuje wykryte pliki.
- **Żaden.** Narzędzie naprawcze nie zostanie wprowadzone do systemu operacyjnego gościa.

- **Akcja naprawy backupu.** Gdy akcja naprawy nie powiodła się, możesz wybrać inne działania naprawcze z dostępnych opcji.

Dodatkowo, możesz wybrać zbieranie informacji, które wzbogacą dane dostarczone do grup śledczych. Zaznacz pola wyboru **Zdarzenie awarii w Systemie Operacyjnym** i **Zdarzenia sterownika** aby zezwolić na zbieranie informacji związanych z błędami systemów operacyjnych lub zdarzeń wygenerowanych przez dodatkowe moduły załadowane przez system operacyjny. Te zdarzenia, poprzedzające incydent pomogą w szybszym wykryciu ataku zero in on the root-cause.

Te zdarzenia są związane z raportem Aktywnością HVI pod incydentem, które prowadzą do nich.

Wykluczenia

GravityZone umożliwia wykluczanie procesów ze skanowania HVI za pomocą raportów **Zablokowane Aplikacje** i **Aktywność HVI**. Sekcja **wykluczenia** gromadzi wszystkie te procesy z wymienionych raportów i wyświetla je w formie tabeli.

Dla każdego wykluczonego procesu można wyświetlić komentarz zawierający przyczynę wykluczenia.

Jeśli zmienisz zdanie na temat wykluczonego procesu, kliknij przycisk **Usuń** w górnej części tabeli, a zostanie on uwzględniony w przyszłych skanach.

Narzędzia Niestandardowe

W tej sekcji można skonfigurować wstrzykiwanie narzędzi wewnątrz docelowych systemów operacyjnych gościa. Narzędzia te muszą być przesłane do GravityZone przed ich użyciem. Aby uzyskać więcej informacji, odwołaj się do „Iniekcja Narzędzi Niestandardowych z HVI” (p. 483).

Aby skonfigurować wstrzyknięcia:

1. Użyj pola wyboru **Aktywuj wstrzyknięcia**, aby włączyć lub wyłączyć tę funkcję.
2. Kliknij przycisk ⊕ **Doda** z górnej części tabeli, aby dodać nowe narzędzie. Wyświetlono okno konfiguracji.
3. Wybierz narzędzie, którego chcesz użyć z listy rozwijanej **Wybierz narzędzie**.

Narzędzia te zostały wcześniej przesłane do GravityZone. Jeśli nie znajdziesz odpowiedniego narzędzia na liście, przejdź do **Centrum Zarządzania Narzędziami** i dodaj go z tego poziomu. Aby uzyskać więcej informacji, zapoznaj się z „Iniekcja Narzędzi Niestandardowych z HVI" (p. 483).

4. W części **Opis narzędzia** wprowadź zamierzone wykorzystanie narzędzia lub inne przydatne informacje.
5. Wpisz wiersz polecenia narzędzia, wraz z wszystkimi potrzebnymi parametrami wejściowymi, podobnie jak w Wierszu Polecenia lub w Terminalu. Na przykład:

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

   .

   W przypadku Narzędzi Naprawczych BD można wybrać tylko działanie naprawcze i działanie zaradcze kopii zapasowych z obu rozwijanych menu.
6. Wskaż lokalizację, z której serwer Security Server powinien zbierać dzienniki:
   - **stdout**. Zaznacz to pole wyboru, aby przechwycić dzienniki ze standardowego kanału komunikacyjnego.
   - **Plik wyjściowy**. Zaznacz to pole wyboru, aby zebrać plik dziennika zapisany w punkcie końcowym. W tym przypadku należy wprowadzić ścieżkę, na której Security Server może odnaleźć plik. Możesz używać ścieżek bezwzględnych lub zmiennych systemowych.

     Tutaj znajdziesz dwie dodatkowe opcje:

     a. **Usuń pliki dziennika z Gościa po ich przeniesieniu**. Zaznacz pliki, których już nie potrzebujesz w punkcie końcowym.

     b. **Przenieś dzienniki do**. Wybierz tę opcję, aby przenieść plik dzienników z folderu Security Server do innej lokalizacji. W takiej sytuacji należy podać ścieżkę do lokalizacji docelowej i poświadczenia uwierzytelniania.
7. Wybierz sposób, w jaki zostanie uruchomione wstrzyknięcie. Możesz wybrać spośród dostępnych opcji:
   - **Po wykryciu naruszenia w maszynie wirtualnej gościa.** Narzędzie jest wtryskiwane natychmiast po wykryciu zagrożenia na maszynie wirtualnej.
   - **Według określonego harmonogramu.** Użyj opcji planowania, aby skonfigurować harmonogram iniekcji. Możesz ustawić narzędzie tak, aby

uruchamiało się co kilka godzin, dni lub tygodni, rozpoczynając się określonego dnia o ustalonej porze.

Proszę wziąć pod uwagę, że maszyna wirtualna musi być włączona, w trakcie wykonywaniu zaplanowanych zadań. Planowana iniekcja nie będzie działać jak zaplanowano, jeśli maszyna zostanie wyłączona lub wstrzymana. W takich sytuacjach zaleca się włączenie pola wyboru **Jeśli planowany czas iniekcji nie zostanie zachowany, uruchom zadanie tak szybko, jak to możliwe**.

- Czasami narzędzie może wymagać dłuższego czasu niż oczekiwano, aby zakończyć pracę lub może przestać reagować. Aby uniknąć awarii w takich sytuacjach, w sekcji **Konfiguracja Bezpieczeństwa** wybierz, po upływie jakiego czasu Security Server powinien automatycznie zakończyć proces.
- Kliknij **Zapisz**. Narzędzie zostanie dodane do tabeli.

Możesz dodać dowolną liczbę narzędzi, postępując zgodnie z wcześniej wspomnianą instrukcją.

7.2.3. Antymalware

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów
- Linux
- macOS

Moduł antymalware chroni system przed wszelkimi rodzajami złośliwego oprogramowania (wirusami, trojanami, oprogramowaniem typu spyware/adware, rootkitami i nie tylko). Ochrona jest podzielona na trzy kategorie:

- Skanowanie dostępowe: - nie dopuszcza, aby nowe szkodliwe oprogramowanie dostało się do systemu.
- Skanowanie podczas wykonania: proaktywnie chroni przed zagrożeniami.
- Skanowanie na żądanie - funkcja ta służy do wykrywania i usuwania złośliwego oprogramowania zainstalowanego w systemie.

Jeżeli zostanie wykryty wirus lub inne złośliwe oprogramowanie, agent bezpieczeństwa Bitdefender automatycznie spróbuje usunąć złośliwy kod z zainfekowanego pliku i odtworzyć jego oryginalną strukturę. Ta operacja określana

jest mianem oczyszczania. Plików, których nie można zdezynfekować, są poddawane kwarantannie, aby izolować infekcję. Kiedy wirus znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być uruchomiony lub otwierany.

Zaawansowani użytkownicy mogą skonfigurować wyjątki, aby pominąć określone pliki lub typy plików podczas skanowania.

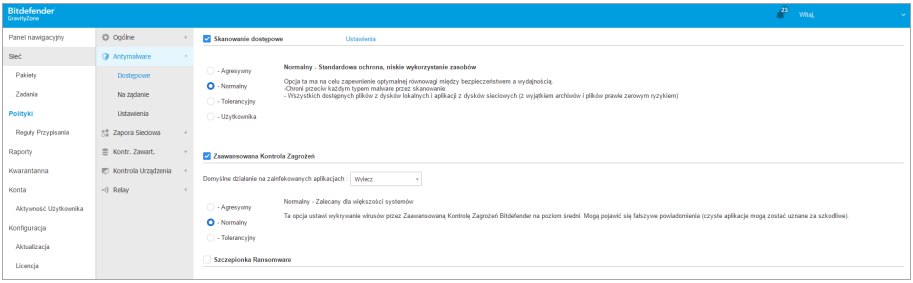
Ustawienia są zorganizowane w poniższych sekcjach:

- Dostępowe
- Przy-Wykonywaniu
- Na żądanie
- HyperDetect
- Zaawansowany Anty-Exploit
- Ustawienia
- Serwery Bezpieczeństwa

Dostępowe

W tej sekcji możesz skonfigurować komponenty zapewniające ochronę, gdy jest dostęp do pliku lub aplikacji:

- Skanowanie dostępowe
- Szczepionka ransomware



Polityki - Ustawienia Dostępowe

Skanowanie dostępowe

Skanowanie na żądanie zapobiega przed dostaniem się nowego malware do systemy przez skanowanie lokalne i plików sieciowych podczas dostępu do nich

(otwieranie, przenoszenie, kopiowanie, uruchamianie), sektory rozruchu i potencjalnie niechciane aplikacje(PUA).

Notatka
Ta funkcja ma pewne ograniczenia w systemach opartych na Linux. Szczegółowe informacje znajdują się w rozdziale Wymagania w Instrukcji instalacji GravityZone.

Aby skonfigurować skanowanie zależne od dostępu:

1. Użyj pola wyboru, żeby włączyć lub wyłączyć skanowanie zależne od dostępu.

   Ostrzeżenie
   Jeżeli wyłączysz skanowanie dostępowe, punkt końcowy będzie podatny na złośliwe oprogramowanie.

2. Dla szybkiej konfiguracji, wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.
3. Możesz skonfigurować szczegóły ustawień skanowania poprzez **niestandardowy** poziom ochrony i naciśnięcie odnośnika **Ustawienia**. Pojawiające się okno **Ustawienia Skanowania Dostępowego** zawiera kilka opcji zorganizowanych w dwóch zakładkach, **Ogólne** i **Zaawansowane**.

   Opcję w zakładce **Ogólne** są opisane tutaj i później:

   - **Lokalizacja pliku**. Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Preferencje skanowania mogą zostać skonfigurowane osobno dla plików lokalnych (przechowywanych na lokalnym punkcie końcowym) lub plików sieciowych (przechowywanych w zasobach sieciowych). Jeżeli ochrona antymalware jest zainstalowana na wszystkich komputerach w sieci, możesz wyłączyć skanowanie plików sieciowych aby pozwolić na szybsze działanie sieci.

     Możesz ustawić agenta bezpieczeństwa w celu skanowania wszystkich plików (niezależnie od rozszerzenia pliku), wyłącznie plików aplikacji lub określonych rozszerzeń plików, które rozważasz jako niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich użytych plików, natomiast lepszą wydajność zapewnia skanowanie tylko aplikacji.

     Notatka
     Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji” (p. 516).

Jeżeli chcesz aby tylko określone rozszerzenia zostały przeskanowane, wybierz **Zdefiniowane przez użytkownika rozszerzenia** z menu wtedy podaj rozszerzenia w polu edycji, naciskając `Enter` po każdym rozszerzeniu.

> **Notatka**
> W systemach opartych na Linux, w rozszerzeniach plików rozróżniana jest wielkość liter, a pliki o tej samej nazwie, ale z innym rozszerzeniem są uważane za odrębne obiekty. Na przykład, `file.txt` różni się od `file.TXT`.

Dla lepszej wydajności systemu, możesz również wykluczyć duże pliki ze skanowania. Zaznacz pole wybory **Maksymalny rozmiar (MB)** i określ limit wielkości plików, które będą skanowane. Używaj tej opcji mądrze, ponieważ złośliwe oprogramowanie może mieć wpływ na większe pliki.

- **Skanowanie.** Zaznacz odpowiednie pola, aby włączyć żądane opcje skanowania.
  - **Tylko nowe lub zmienione pliki.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
  - **Boot sektory.** Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera niezbędny kod potrzebny do uruchomienia procesu rozruchu. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
  - **Dla keyloggerów.** Keyloggery zapisują to, co wpiszesz na klawiaturze i wysyłają raporty przez internet do hakera. Haker może poznać ważne informacje z ukradzionych danych, takie jak numer i hasło do konta bankowego i użyć ich na własną korzyść.
  - **Dla potencjalnie niechcianych aplikacji (PUA).** Potencjalnie nie chciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-suppored). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.
  - **Archiwa**. Wybierz tę opcję, jeżeli chcesz włączyć skanowanie na wejściu zarchiwizowanych plików. Skanowanie wewnątrz archiwów to powolny i zasobożerny proces, który z tego powodu nie jest zalecany do użycia

w ochronie w czasie rzeczywistym. Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony na żądanie.

Jeżeli zdecydowałeś aby używać tej opcji, możesz skonfigurować poniższe opcje optymalizacji:

- **Maksymalny rozmiar archiwum (MB) .** Możesz ustawić maksymalną akceptowalną wielkość archiwum do skanowania zależnego od dostępu. Zaznacz odpowiadające pole wyboru i wpisz maksymalny rozmiar archiwum (w MB).
- **Maksymalna głębokość archiwum (poziomy).** Zaznacz odpowiednie pole i wybierz maksymalną głębokość archiwum z menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.

– **Odroczone Skanowanie.** Odroczone skanowanie poprawia wydajność systemu podczas wykonywania operacji dostępu do plików. Na przykład, zasoby systemowe nie są naruszone, gdy duże pliki są kopiowane. Ta opcja jest domyślnie włączona.

- **Czynności Skanowania**. W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:
  – **Domyślne działanie dla zainfekowanych plików.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI). Agent bezpieczeństwa Bitdefender może normalnie usunąć złośliwy kod z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

    Domyślnie, jeśli zainfekowany plik jest wykryty, agent ochrony Bitdefendera automatycznie spróbuje go wyleczyć. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję. Możesz zmienić zalecane ustawienia odnośnie swoich potrzeb.

    WAŻNE
    W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

– **Domyślne działanie dla podejrzanych plików.** Pliki są wykryte jako podejrzane przez analizę heurystyczną i inne technologie Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

  Jeżeli podejrzany plik zostanie wykryty, użytkownicy dostaną odmowę dostępu do pliku, żeby zapobiec potencjalnej infekcji.

Choć nie jest to polecane, możesz zmienić domyślne działania. Możesz zdefiniować dwie akcje dla każdego typu pliku. Dostępne są następujące działania:

Blokuj dostęp
Odmowa dostępu do wykrytych plików.

> **WAŻNE**
> W przypadku punktów końcowych MAC, akcja **Przenieś do kwarantanny** jest podejmowana zamiast **Blokowanie dostępu**

Dezynfekuj
Usuń złośliwy kod z zainfekowanych plików. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach.

Usuń
Usuwa wykryte pliki z dysku, bez żadnego ostrzeżenia. Wskazane jest, aby unikać tego działania.

Przenieś pliki do kwarantanny
Przenieś wykrytych plików z ich obecnego miejsca położenia do folderu kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami kwarantanny ze strony Kwarantanna w konsoli.

Nie podejmuj żadnych działań
Raportuj tylko zainfekowane pliki wykryte przez Bitdefender.

Zakładka **Zaawansowane** odnosi się do skanowania dostępowego dla maszyn z Linuxem. Użyj pola wyboru aby go włączyć lub wyłączyć.

W tabeli poniżej, możesz skonfigurować ścieżki w Linuxie, które chcesz skanować. Domyślnie, jest 5 wpisów, każdy odnoszący się do specyficznej lokacji na punkcie końcowym:`/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

Aby dodać więcej wpisów:

- Zapisz dowolną niestandardową nazwę lokalizacji w polu wyszukiwania w górnej części tabeli.
- Wybierz predefiniowane katalogi z listy wyświetlane po kliknięciu na strzałkę po prawej stronie pola wyszukiwania.

Kliknij przycisk ⊕ **Dodaj** aby zapisać katalog do tabeli lub wybierz przycisk ⊗ **Usuń** aby usunąć.

Szczepionka ransomware

Ransomware vaccine uodparnia twoje maszyny przed **znanym** ransomware blokującym proces szyfrowania, nawet jeśli komputer jest zainfekowany. Użyj pola wyboru, aby włączyć lub wyłączyć szczepionkę Ransomware.

Funkcja szczepionki Ransomware jest domyślnie deaktywowana. Bitdefender Labs analizuje zachowanie powszechnego oprogramowania ransomware, a nowe aktualizacje sygnatur są dostarczane wraz z każdą aktualizacją zawartości zabezpieczeń, aby rozwiązać najnowsze zagrożenia.

Ostrzeżenie
Aby jeszcze bardziej zwiększyć ochronę przed infekcjami ransomware, należy zachować ostrożność w przypadku niezamówionych lub podejrzanych załączników i upewnić się, że treść zabezpieczeń jest aktualizowana.

Notatka
Szczepionka ransomware jest dostępna tylko dla Bitdefender Endpoint Security Tools dla Windows.

Przy-Wykonywaniu

W tej sekcji możesz skonfigurować ochronę przed złośliwymi procesami podczas ich wykonywania. Obejmuje następujące warstwy ochronne:

Zaawansowana Kontrola Zagrożeń

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów
- macOS

Bitdefender Zaawansowana Kontrola Zagrożeń jest proaktywną technologią wykrywania, która wykorzystuje zaawansowane metody heurystyczne do wykrywania nowych potencjalnych zagrożeń w czasie rzeczywistym.

Zaawansowana Kontrola Zagrożeń nieustannie monitoruje aplikacje uruchomione na punkcie końcowym, w poszukiwaniu aktywności charakterystycznej dla złośliwego oprogramowania. Każde z tych działań jest oceniane, a dla każdego procesu obliczana jest ocena ogólna. Gdy wynik ogólny dla danego procesu osiąga podany próg, proces ten zostaje uznany za szkodliwy.

Zaawansowana Kontrola Zagrożeń automatycznie spróbuje wyleczyć wykryty plik. Jeśli rutynowe leczenie się nie powiedzie, Zaawansowana Kontrola Zagrożeń usunie plik.

Notatka
Przed zastosowaniem działań dezynfekcji, kopia pliku jest wysyłana do kwarantanny, dzięki czemu masz możliwość przywrócenia jej później, w przypadku błędnego zaklasyfikowania. To działanie można skonfigurować używając opcji **Kopiuj pliki do kwarantanny przed użyciem zadania dezynfekcji** opcja dostępna w zakładce **Antymalware > Ustawienia** ustawień polityki. Ta opcja jest włączona domyślnie w szablonie polityki.

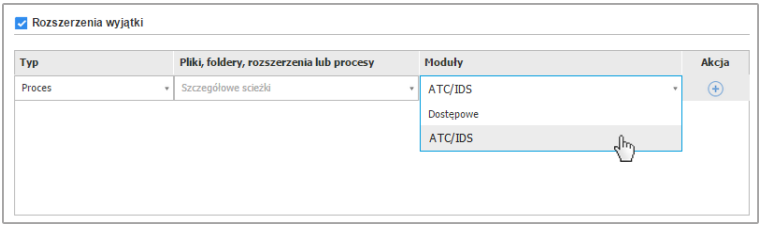
Aby skonfigurować Zaawansowaną Kontrolę Zagrożeń:

1. Użyj pola wyboru, aby włączyć lub wyłączyć Zaawansowaną Kontrolę Zagrożeń.

   Ostrzeżenie
   Jeżeli wyłączysz Zaawansowaną Kontrolę Zagrożeń, komputery będą podatne na nieznane złośliwe oprogramowanie.

2. Zaawansowana Kontrola Zagrożeń domyślnie będzie próbowała wyleczyć zainfekowane aplikacje. Możesz ustawić inne domyślne działanie, używając dostępnego menu:
   - **Zablokuj**, aby odmówić dostępu do zainfekowanej aplikacji.
   - **Nie podejmuj żadnych akcji**, aby raportować tylko zainfekowane aplikacje wykryte przez Bitdefender.
3. Kliknij na poziom bezpieczeństwa, który najlepiej odpowiada Twoim potrzebom (**Agresywny, Normalny, Tolerancyjny**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

Notatka
Jeśli podniesiesz poziomy ochrony, Zaawansowana Kontrola Zagrożeń będzie wymagać mniejszej liczby oznak złośliwego zachowania, by zgłosić dany proces. To sprawi, że raportowana będzie większa liczba aplikacji, a jednocześnie wzrośnie prawdopodobieństwo wystąpienia fałszywych alarmów (nieszkodliwych aplikacji rozpoznanych jako złośliwe).
Wysoce zalecane jest by stworzyć wykluczenia zasad dla powszechnie użytkowanych lub znanych aplikacji w celu zapobiegania fałszywym alarmom (niepoprawne wykrycie poprawnie działających aplikacji). Przejdź do zakładki Antymalware > Ustawienia i skonfiguruj zasady wykluczeń ATC/IDS dla zaufanych aplikacji.



Polityki Komputerów i Maszyn Wirtualnych - proces wykluczenia ATC/IDS

Łagodzenie Skutków Ransomware

Łagodzenie Skutków Ransomware używa technologii wykrywania i zapobiegania, aby zabezpieczyć twoje dane przed atakami ransomware. Niezależnie od tego czy ransomware jest nowe czy znane GravityZone wykryje nieautoryzowane próby szyfrowania i zablokuje proces. Następnie, odzyska pliki z kopii zapasowych do oryginalnych lokalizacji.

WAŻNE
Łagodzenie Skutków Ransomware wymaga Aktywnej Kontroli Zagrożeń.

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów

Aby skonfigurować Łagodzenie Skutków Ransomware:

1. Wybierz **Łagodzenie Skutków Ransomware** w sekcji polityki **Antymalware > Przy-Wykonaniu**, aby włączyć tę funkcję.
2. Wybierz jakiego trybu monitorowania chcesz używać:
   - Lokalnie. GravityZone monitoruje procesy i wykrywa ataki ransomware zainicjowane lokalnie na punktach końcowych. Jest to zalecane dla stacji roboczych. Należy zachować ostrożność na serwerach ze względu na wpływ na wydajność.
   - Zdalny. GravityZone monitoruje dostęp do ścieżek udziałów sieciowych i wykrywa ataki ransomware, które są inicjowane z innej maszyny. Użyj tej opcji, jeśli punktem końcowym jest serwer plików lub włączono udziały sieciowe.
3. Wybierz metodę odzyskiwania:
   - Na żądanie. Ręcznie wybierasz ataki z których chcesz odzyskać pliki. Możesz to zrobić na stronie **Raporty > Aktywność Ransomware** kiedy tylko zechcesz, ale nie później niż 30 dni po ataku. Po tym czasie odzyskanie nie będzie już możliwe.
   - Automatyczne. GravityZone automatycznie odzyska pliki zaraz po wykryciu ransomware.

   Aby odzyskiwanie powiodło się, punkty końcowe muszą być dostępne.

Po uruchomieniu masz wiele możliwości sprawdzenia czy twoja sieć jest atakowana przez ransomware:

- Sprawdź powiadomienia i szukaj **Detekcja Ransomware**.

  Aby uzyskać więcej informacji na temat tego powiadomienia, odwołaj się do „Rodzaje powiadomień” (p. 485).
- Sprawdź raport **Audyt Bezpieczeństwa**.
- Sprawdź stronę **Aktywność Ransomware**.

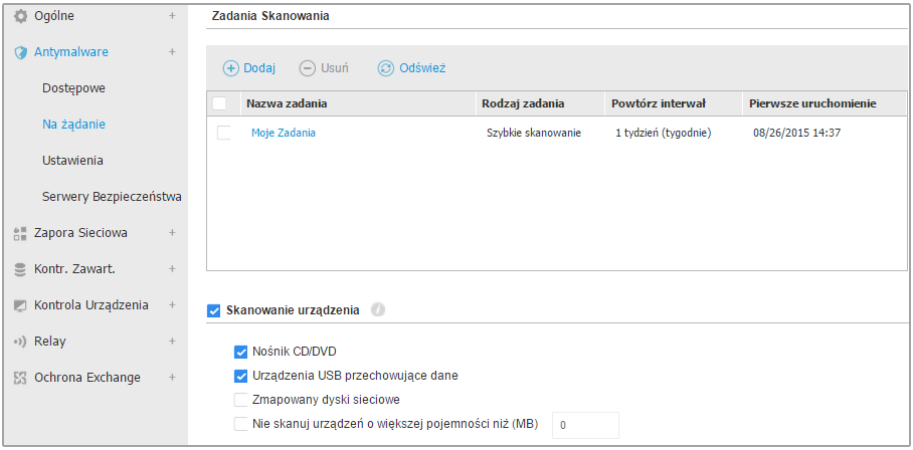
  Co więcej, z tej strony możesz uruchomić zadanie przywracania, jeśli jest taka potrzeba, Aby uzyskać więcej informacji, odwołaj się do ???.

Jeżeli zauważysz detekcję, która jest autoryzowanym procesem szyfrowania, ustaw ścieżki w których zezwalasz na szyfrowanie plików lub zezwól na zdalny dostęp z niektórych urządzeń, dodaj wyjątki w sekcji polityki **Antymalware > Ustawienia > Niestandardowe Wykluczenia**. Łagodzenie Skutków Ransomware dopuszcza

wykluczenia dla folderów, procesu i IP/maski. Aby uzyskać więcej informacji, zapoznaj się z „Wykluczenia” (p. 287).

Na żądanie

W tej sekcji możesz dodać i konfigurować skanowanie antymalware, które będą uruchamiać się regularnie na docelowych komputerach, według zdefiniowanego harmonogramu.



Polityki Komputerów i Maszyn Wirtualnych - Zadanie Skanowania Na Żądanie

Skanowanie odbywa się w tle, bez względu na to czy użytkownik jest zalogowany w systemie, czy nie.

Choć nie jest to obowiązkowe, zalecane jest zaplanowanie wszechstronnego systemu skanowania uruchamianego cotygodniowo na wszystkich punktach końcowych. Regularne skanowanie punktów końcowych jest pro aktywnym zabezpieczeniem, które może pomóc wykrywać i blokować złośliwie oprogramowanie, które może uchronić się przed ochroną w czasie rzeczywistym.

Oprócz regularnego skanowania, możesz również skonfigurować automatyczne wykrywanie i skanowanie zewnętrznych nośników pamięci.

Zarządzanie Zadaniami skanowania

Tabela Zadań skanowania informuje o istniejących zadań skanowania, dostarcza ważnych informacji na temat każdego z nich:

- Nazwa i rodzaj zadania.
- Harmonogram bazujący na zadaniach, które działają regularnie (rekurencyjnie).
- Czas kiedy zadanie zostanie po raz pierwszy uruchomione.

Możesz dodać i skonfigurować następujące typy zadań skanowania:

- **Szybkie skanowanie** Do wykrywania w systemie złośliwego oprogramowania Szybkie Skanowanie wykorzystuje skanowanie w chmurze. Wykonanie szybkiego skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.

  Kiedy zostaje wykryte złośliwe oprogramowanie lub rootkity, Bitdefender automatycznie przeprowadza dezynfekcję. Jeśli z jakiegokolwiek powodu plik nie może zostać zdezynfekowany, zostaje przeniesiony do kwarantanny. Ten typ skanowania ignoruje podejrzane pliki.

  Szybkie Skanowanie jest domyślnym zadaniem skanowania z wstępnie skonfigurowanymi opcjami, które nie mogą zostać zmienione. Możesz dodać jedynie jedno zadanie szybkiego skanowania dla tej samej polityki.

- **Pełne Skanowanie** sprawdza cały punkt końcowy w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu, takich jak wirusy, oprogramowanie szpiegowskie, adware, rootkity i inne.

  Bitdefender automatycznie próbuje zdezynfekować wykryte pliki zawierające złośliwe oprogramowanie. W przypadku, gdy nie można usunąć złośliwego oprogramowania, znajduje się ono w kwarantannie, gdzie nie może wyrządzić żadnej szkody. Podejrzane pliki są ignorowane. Jeśli chcesz podjąć działania dotyczące podejrzanych plików lub inne domyślne akcje zainfekowanych plików, wybierz opcję uruchomienia skanowania niestandardowego.

  Pełne skanowanie jest domyślnym zadaniem z wstępnie skonfigurowanymi opcjami, które nie mogą być zmieniane. Możesz dodać tylko jedno zadanie pełnego skanowania dla tej samej polityki.

- **Niestandardowe Skanowanie** pozwala na wybranie konkretnej lokalizacji, które mają zostać przeskanowane i na skonfigurowanie opcji skanowania.

- **Skanowanie Sieci** jest typem niestandardowego skanowania, które pozwala na przypisywanie jednego zarządzanego punktu końcowego w celu skanowania dysków sieciowych, następnie konfigurowania opcji skanowania i skanowania odpowiednich lokalizacji. W celu wykonania zadania skanowania sieciowego, musisz wprowadzić listy uwierzytelniające dla kont użytkowników posiadających

prawo odczytu/zapisu na docelowych dyskach sieciowych, dla umożliwienia agentowi bezpieczeństwa dostęp i podejmowanie czynności na dyskach sieciowych.

Zadanie skanowania rekurencyjnej sieci zostanie wysłane tylko do wybranych skanujących punktów końcowych. Jeżeli wybrany punkt końcowy jest niedostępny, zostaną zastosowane lokalne ustawienia skanowania.

Notatka
Możesz stworzyć sieć skanowania zadań tylko przy użyciu polityk które są już zastosowane do punktów końcowych które mogą być użyte jako skanery.

Oprócz domyślnych zadań (których nie można usunąć lub zduplikować) możesz utworzyć tak wiele niestandardowych zadań skanowania ile chcesz.

aby utworzyć i skonfigurować nowe niestandardowe zadanie skanowania lub zadanie skanowania sieci, naciśnij przycisk ⊕ **Dodaj** po prawej stronie tabeli. Aby zmienić ustawienia istniejących zadań skanowania, naciśnij nazwę tego zadania. Zobacz poniższy temat aby dowiedzieć się jak skonfigurować zadanie.

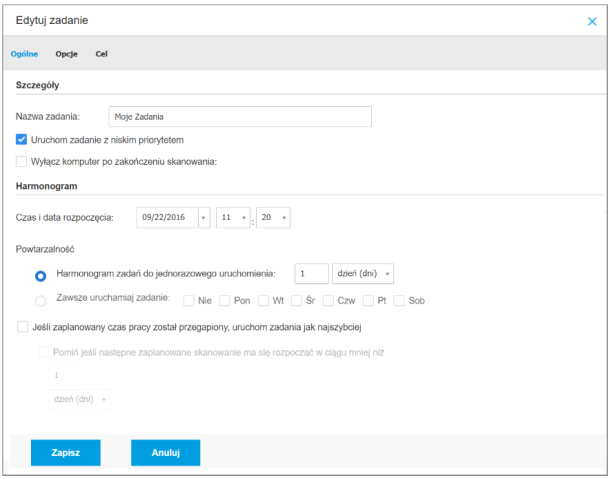
Aby usunąć zadanie z listy, wybierz zadanie i naciśnij przycisk ⊖ **Usuń** po prawej stronie tabeli.

Konfiguracja Zadania Skanowania

Ustawienia zadania skanowania można organizować w trzech zakładkach:

- **Ogólne**: ustaw nazwę zadania i harmonogram realizacji.
- **Opcje**: wybierz profil skanowania dla szybkiej konfiguracji ustawień skanowania i zdefiniuj ustawienia skanowania dla niestandardowego skanowania.
- **Cel**: wybierz pliki i foldery do przeskanowania i zdefiniuj wyjątki skanowania.

Opcje są opisane poniżej od pierwszej do ostatniej zakładki:



Polityki Komputerów i Maszyn Wirtualnych - Konfiguracja Ustawień Ogólnych Zadań Skanowania Na Żądanie.

- **Szczegóły.** Wybierz sugestywna nazwę dla raportu, aby w łatwy sposób móc zidentyfikować co zawiera. Kiedy wybierasz nazwę, weź pod uwagę cel zadania skanowania i ewentualne ustawienia skanowania.

  Domyślnie zadania skanowania działają ze zmniejszonym priorytetem. W ten sposób Bitdefender pozwala innym programom działać szybciej, ale wydłużając czas potrzebny na zakończenie skanowania. Użyj **Uruchom zadanie o niskim priorytecie** pole wyboru, aby wyłączyć lub ponownie włączyć tę funkcję sprawdzenia.

  Notatka
  Ta opcja dotyczy tylko Bitdefender Endpoint Security Tools i Endpoint Security (agent legacy).

  Zaznacz pole wyboru **Wyłącz komputer kiedy skanowanie się zakończy** aby wyłączyć twoją maszynę, jeśli nie zamierzasz z niej korzystać przez jakiś czas.

  Notatka
  Ta opcja dotyczy Bitdefender Endpoint Security Tools, Endpoint Security (agent legacy) i Endpoint Security for Mac.

- **Harmonogram.** Użyj opcji planowania aby skonfigurować harmonogram skanowania. Możesz ustawić skanowanie aby uruchamiało się co kilka godzin, dni lub tygodni, rozpoczynając się określonego dnia o ustalonej porze.

  Punkty końcowe muszą być włączone, gdy zaplanowane jest skanowanie. Zaplanowane skanowanie nie zostanie uruchomione jeżeli maszyna jest wyłączona, za hibernowana, uśpiona. W takich sytuacjach, skanowanie zostanie odłożone do następnego razu.

  > **Notatka**
  > Zaplanowane skanowanie uruchomi się na docelowych punktach końcowych według czasu lokalnego. Na przykład, jeżeli zaplanowane skanowanie jest ustawione o 18:00 i punkt końcowy posiada inną strefę czasową niż Control Center, skanowanie odbędzie się o 18:00 według czasu punktu końcowego.

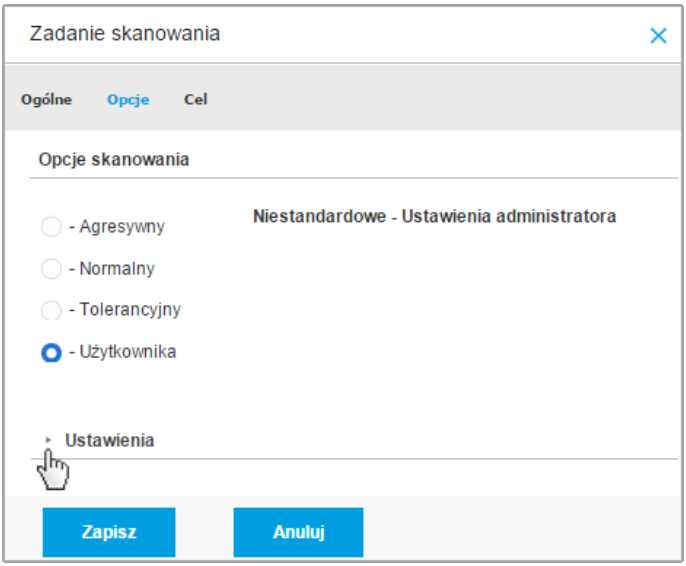
  Opcjonalnie możesz określić, co się stanie, gdy zadanie skanowania nie może się uruchomić w zaplanowanym czasie (punkt końcowy był offline lub wyłączony). Skorzystaj z opcji **Jeśli zaplanowany czas pracy zostanie pominięty, uruchom zadanie tak szybko, jak to możliwe** zgodnie z Twoimi potrzebami:

  – Jeśli nie oznaczysz opcji, zadanie skanowania zostanie uruchomione ponownie w następnym zaplanowanym czasie.

  – Po wybraniu opcji skanowanie wymuszane jest, tak szybko, jak to możliwe. Aby dostroić najlepszy czas dla środowiska wykonawczego skanowania i uniknąć przeszkadzania użytkownikowi podczas godzin pracy, wybierz opcję **Pomiń, jeśli następne zaplanowane skanowanie ma się rozpocząć za mniej niż**, a następnie określić żądany interwał.

- **Opcje skanowania.** Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

  Bazując na wybranym profilu, opcje skanowania w sekcji **Ustawienia** zostaną automatycznie skonfigurowane. Jednak, jeżeli chcesz, możesz skonfigurować je szczegółowo. Aby to zrobić, zaznacz pole wyboru **Niestandardowe** i przejdź do sekcji **ustawienia**.



Zadanie Skanowania Komputerów - Konfiguracja Niestandardowego Skanowania

- **Typy plików.** Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Możesz ustawić agenta bezpieczeństwa tak by skanował wszystkie pliki (niezależnie od rozszerzenia pliku), tylko pliki aplikacji lub określone rozszerzenia plików, które uważasz za potencjalnie niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.

  > **Notatka**
  > Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji" (p. 516).

  Jeżeli chcesz aby tylko określone rozszerzenia zostały przeskanowane, wybierz **Zdefiniowane przez użytkownika rozszerzenia** z menu wtedy podaj rozszerzenia w polu edycji, naciskając `Enter` po każdym rozszerzeniu.

- **Archiwa.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany

i uruchomiony bez włączonej ochrony w czasie rzeczywistym. Zaleca się użycie tej opcji, w celu wykrycia i usunięcia wszelkich potencjalnych zagrożeń, nawet jeśli nie jest to zagrożenie bezpośrednie.

Notatka
Skanowanie zarchiwizowanych plików wydłuża ogólny czas skanowania i wymaga więcej zasobów systemowych.

– **Skanowanie wewnątrz archiwów.** Wybierz tę opcję tylko jeżeli chcesz sprawdzać pliki archiwów w poszukiwaniu malware. Jeżeli zdecydowałeś aby używać tej opcji, możesz skonfigurować poniższe opcje optymalizacji:
  - **Ogranicz rozmiar archiwum do (MB).** Możesz ustawić maksymalną akceptowalną wielkość archiwum do skanowania. Zaznacz odpowiadające pole wyboru i wpisz maksymalny rozmiar archiwum (w MB).
  - **Maksymalna głębokość archiwum (poziomy).** Zaznacz odpowiednie pole i wybierz maksymalną głębokość archiwum z menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.
– **Skanowanie archiwum e-mail.** Zaznacz tę opcję jeżeli chcesz włączyć skanowanie plików wiadomości e-mail i bazy e-mail, włączając formaty takie jak .eml, .msg, .pst, .dbx, .mbx, .tbb i inne.

Notatka
Skanowanie archiwum e-mail zużywa wiele zasobów i może mieć wpływ na wydajność systemu.

- **Inne.** Zaznacz odpowiednie pola, aby włączyć żądane opcje skanowania.
  – **Skanowanie sektorów startowych.** Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera niezbędny kod potrzebny do uruchomienia procesu rozruchu. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
  – **Skanowanie rejestru.** Włącz tę opcję, aby skanować klucze rejestru. Rejestr systemu Windows jest bazą danych przechowującą ustawienia konfiguracji i opcje dla komponentów systemu operacyjnego Windows oraz dla zainstalowanych aplikacji.

- **Skanowanie w poszukiwaniu rootkitów.** Zaznacz tę opcję, aby skanować w poszukiwaniu rootkitów i ukrytych obiektów, które korzystają z tego rodzaju oprogramowania.
- **Skanuj w poszukiwaniu keyloggerów.** Zaznacz opcje skanowania dla oprogramowania keylogger.
- **Skanuj zasoby sieciowe.** Ta opcja skanuje zamontowane dyski sieciowe.

  Dla szybkiego skanowania, ta opcja jest domyślnie dezaktywowana. Dla pełnego skanowania, to jest domyślnie aktywowane. Dla skanowania niestandardowego, jeśli ustawisz poziom ochrony na **Agresywny/Normalny** opcja **Skanuj zasoby sieciowe** będzie automatycznie dostępna. Jeśli ustawisz poziom ochrony na **Tolerancyjny**, opcja **Skanuj zasoby sieciowe** będzie automatycznie wyłączona.
- **Skanowanie pamięci.** Wybierz tę opcję, aby przeskanować programy działające w pamięci systemu.
- **Skanowanie ciasteczek.** Wybierz tę opcję, aby przeskanować ciasteczka zapisane przez przeglądarkę na punkcie końcowym.
- **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Potencjalnie nie chciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-suppored). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.

- **Akcje.** W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:
  - **Domyślne działanie dla zainfekowanych plików.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI). Agent bezpieczeństwa może normalnie

usunąć złośliwy kod z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

Jeżeli zainfekowany plik został wykryty, agent bezpieczeństwa podejmie automatyczną próbę jego dezynfekcji. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.

WAŻNE
W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Domyślne działanie dla podejrzanych plików.** Pliki są wykryte jako podejrzane przez analizę heurystyczną i inne technologie Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

  Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny. Pliki kwarantanny są wysyłane do analizy do Laboratorium Bitdefender w regularnych odstępach czasu. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

- **Domyślne działanie dla rootkitów.** Rootkity stanowią specjalistyczne oprogramowanie wykorzystywane do ukrywania plików systemowych. Rootkity choć są nieszkodliwe, często są używane do ukrywania złośliwego oprogramowania lub intruza w systemie.

  Wykrywanie rootkitów i ukrywanie plików jest domyślnie ignorowane.

Choć nie jest to polecane, możesz zmienić domyślne działania. Można tu wybrać osobną czynność dla każdej kategorii, a także określić drugą czynność, jaka ma zostać podjęta, jeśli pierwsza nie przyniesie skutku. Wybierz z odpowiedniego menu pierwszą i drugą czynność, jaka ma zostać zastosowana do każdego z wykrytych plików. Dostępne są następujące działania:

Nie podejmuj żadnych działań
Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania.

Dezynfekuj
Usuń złośliwy kod z zainfekowanych plików. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach.

Usuń
Usuwa wykryte pliki z dysku, bez żadnego ostrzeżenia. Wskazane jest, aby unikać tego działania.

Przenieś pliki do kwarantanny
Przenieś wykrytych plików z ich obecnego miejsca położenia do folderu kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami kwarantanny ze strony Kwarantanna w konsoli.

- **Cel Skanowania.** Dodaj listę wszystkich lokacji które chciałbyś przeskanować na docelowych komputerach.

  Aby dodać nowy plik lub folder do skanowania:

  1. Wybierz wcześniej zdefiniowaną lokalizacje z rozwijanego menu lub wprowadź **Określoną ścieżkę**, którą chciałbyś przeskanować.
  2. W polu edycji określ ścieżkę do obiektów, które mają zostać przeskanowane.
     - Jeżeli wybrałeś wcześniej zdefiniowana lokalizację, wypełnij ścieżkę jeśli potrzebujesz. Na przykład, aby przeskanować folder `Program Files` wystarczy wybrać odpowiednią ścieżkę z rozwijanego menu. Aby przeskanować konkretny folder z `Program Files`, musisz uzupełnić ścieżkę dodając backslash (\) i nazwę folderu.
     - Jeżeli wybrałeś **Określona ścieżka**, podaj pełną ścieżkę do obiektu, który chcesz przeskanować. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.
  3. Naciśnij przycisk ⊕ **Dodaj**.

  Aby edytować istniejącą lokalizację, kliknij ją. Aby usunąć lokalizację z listy, przesuń kursor nad nią, a następnie kliknij odpowiedni przycisk ⊖ **Usuń**.

- W celu wykonania zadania skanowania sieciowego, musisz wprowadzić listy uwierzytelniające dla kont użytkowników posiadających prawo odczytu/zapisu na docelowych dyskach sieciowych, dla umożliwienia agentowi bezpieczeństwa dostęp i podejmowanie czynności na dyskach sieciowych.

- **Wykluczenia.** Możesz korzystać z wyjątków z sekcji **Antymalware > Wyjątki** obecnej polityki, lub zdefiniować niestandardowe wyjątki dla bieżącego zadania skanowania. Aby uzyskać więcej informacji dotyczących wykluczeń, odwołaj się do „Wykluczenia” (p. 287).

Skanowanie urządzeń

Możesz skonfigurować agenta bezpieczeństwa, aby automatycznie wykrywał i skanował zewnętrzne urządzenia pamięci masowej, kiedy są podłączone do punktu końcowego. Wykryte urządzenia są przyporządkowywane do jednej z tych kategorii:

- CD/DVD
- Urządzenia pamięci masowej USB, takie jak flash i zewnętrzne dyski twarde
- Urządzenia z większą ilością przechowywanych danych niż określona.

Skanowanie urządzenie automatycznie podejmuję próbę wyleczenia plików wykrytych jako zainfekowane lub przenosi je do kwarantanny jeżeli wyleczenie nie jest możliwe. Zauważ, że niektóre urządzenia takie jak CD/DVD są tylko do odczytu. Nie można podjąć żadnych akcji na zainfekowanych plikach przechowywanych w takim magazynie.

Notatka
Podczas skanowania urządzenia, użytkownik może mieć dostęp do danych z urządzenia.

Jeżeli powiadomienia pop-up są włączone w sekcji **Ogólne > Wyświetl** użytkownik jest monitowany o rozpoczęcie skanowania, gdy zostanie wykryte urządzenie, zamiast automatycznego rozpoczęcia skanowania.

Gdy rozpocznie się skanowanie urządzenia:

- Wyskakujące okienko informuje użytkownika o skanowaniu urządzenia, pod warunkiem, że wyskakujące okienka powiadomień są włączone w sekcji **Ogólne>Powiadomienia**.

Po zakończeniu skanowania, użytkownik powinien sprawdzić wykryte zagrożenia, jeżeli zostaną znalezione.

Aby włączyć automatyczne wykrywanie i skanowanie urządzeń, zaznacz **Skanowanie Urządzenia**. Aby skonfigurować skanowanie urządzenia indywidualnie dla każdego rodzaju urządzenia, można użyć następujących opcji:

- **Nośnik CD/DVD**

- **Urządzenia USB przechowujące dane**
- **Nie skanuj urządzeń o większej pojemności niż (MB)**. Użyj tej opcji aby automatycznie pominąć skanowanie wykrytych urządzeń, jeżeli ilość przechowywanych danych przekroczy określoną wielkość. W odpowiednim polu podaj limit (w megabajtach). Zero oznacza brak limitu.

HyperDetect

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów
- Linux

HyperDetect dodaje kolejną warstwę ochrony do istniejących technologii skanowania (Dostępowego, Na żądanie i Skanowania Ruchu), aby walczyć z nową generacją cyber-ataków, w tym z zaawansowanymi długotrwałymi zagrożeniami. HyperDetect, swoją silną heurystyką opartą na sztucznej inteligencji i uczeniu maszyn, wzmacnia moduły ochrony Antymalware i Kontroli Zawartości.

Dzięki możliwości przewidywania ataków celowych i wykrywania najbardziej zaawansowanych złośliwych programów jeszcze zanim one zaatakują, HyperDetect wykrywa zagrożenia znacznie szybciej niż technologie skanowania opartego na sygnaturach lub skanowaniu behawioralnym.

Aby skonfigurować HyperDetect;

1. Użyj pola wyboru **HyperDetect** aby włączyć lub wyłączyć moduł.
2. Wybierz przed jakimi zagrożeniami chcesz chronić swoją sieć. Dla wszystkich typów zagrożeń włączona jest domyślna ochrona : ataków typu target, podejrzanych plików i ruchu sieciowego, exploitów, ransomware lub grayware.

   Notatka
   Heurystyka ruchu sieciowego wymaga włączenia **Kontroli Zawartości > Skanowania Ruchu**.

3. Dostosuj poziom ochrony przed wybranymi zagrożeniami.

Użyj przełącznika głównego, znajdującego się na górze listy zagrożeń, aby wybrać unikalny poziom ochrony przed wszystkimi zagrożeniami lub wybierz poszczególne poziomy, aby dokładnie doprecyzować ochronę.

Ustawienie modułu nadanym poziomie spowoduje podejmowanie działań na tym poziomie. Na przykład, jeśli jest ustawiony na **Normalny**, moduł wykrywa i zabezpiecza zagrożenia, które włączają **Tolerancyjny** tryb i progi **Normalnego**, lecz nie **Agresywnego**.

Ochrona zmienia się z **Tolerancyjnej** na **Agresywną**.

Należy pamiętać, że wykrywanie agresywne może prowadzić do fałszywych alarmów, a wykrywanie tolerancyjne może narazić sieć na pewnego rodzaju zagrożenia. Zaleca się, aby najpierw ustawić poziom ochrony na maksimum, a następnie, w przypadku zbyt wielu fałszywych alarmów, zmniejszyć do optymalnego poziomu.

Notatka
Po włączeniu ochrony dla określonego typu zagrożenia, wykrywanie jest automatycznie ustawiane na wartość domyślną (poziom **Normalny**).

4. W sekcji **Działania** skonfiguruj, jak HyperDetect powinien reagować na wykrywanie. Użyj rozwijanego menu, aby ustawić działanie, które ma być podjęte w przypadku wykrycia zagrożenia:
   - Dla plików: odmów dostępu, zdezynfekuj, usuń, przeprowadź kwarantannę lub zgłoś pliki.
   - Dla ruchu sieciowego: blokuj lub zgłoś podejrzany ruch.
5. Jeśli chcesz wyświetlić zagrożenia wykryte przy wyższych poziomach ochrony, zaznacz pole wyboru **Rozszerz raportowanie na wyższych poziomach**, znajdujące się obok menu rozwijanego.

Jeśli nie masz pewności co do bieżącej konfiguracji, możesz łatwo przywrócić ustawienia początkowe, klikając przycisk **Resetuj do domyślnego**, znajdujący się w dolnej części strony.

Zaawansowany Anty-Exploit

Notatka
Ten moduł jest dostępny dla:
- Windows dla stacji roboczych

Zaawansowany Anty- Exploit to proaktywna technologia wykrywająca exploity w czasie rzeczywistym. Opierając się na uczeniu maszynowym, chroni przed szeregiem znanych i nieznanych exploitów, w tym ataków bez pamięci plików.

Aby włączyć ochronę przed exploitami, zaznacz pole wyboru **Zaawansowany Anty-Exploit** .

Zaawansowany Anty-Exploit jest ustawiony by działać z zalecanymi ustawieniami. W razie potrzeby możesz dostosować ochronę wg własnych potrzeb. Aby przywrócić ustawienia początkowe, kliknij link **Przywróć domyślne** po prawej stronie nagłówka sekcji.

GravityZone ma ustawienia anty-exploitów zorganizowane w trzech sekcjach:

- **Wykrywanie obejmujące cały system**

  Techniki przeciwdziałające exploitom w tej sekcji monitorują procesy systemowe, które są celem exploitów.

  Aby uzyskać więcej informacji na temat dostępnych technik i sposobu konfigurowania ich ustawień, zobacz „Skonfiguruj skanowanie obejmujące cały system” (p. 280).

- **Predefiniowane aplikacje**

  Zaawansowany moduł Anty-Exploit jest wstępnie skonfigurowany z listą popularnych aplikacji, takich jak Microsoft Office, Adobe Reader lub Flash Player, które są najbardziej narażone na wykorzystanie.

  Aby uzyskać więcej informacji na temat dostępnych technik i sposobu konfigurowania ich ustawień, zobacz „Konfiguracja technik specyficznych dla danej aplikacji” (p. 281).

- **Dodatkowe aplikacje**

  W tej sekcji możesz dodać i skonfigurować ochronę dla wielu innych aplikacji.

  Aby uzyskać więcej informacji na temat dostępnych technik i sposobu konfigurowania ich ustawień, zobacz „Konfiguracja technik specyficznych dla danej aplikacji” (p. 281).

Możesz rozwinąć lub zwinąć każdą sekcję, klikając jej nagłówek. W ten sposób szybko dotrzesz do ustawień, które chcesz skonfigurować.

Skonfiguruj skanowanie obejmujące cały system

W tej sekcji dostępne są następujące opcje:

Technika	Opis
Eskalacja uprawnień	Zapobiega uzyskaniu przez procesy nieautoryzowanych uprawnień i dostępu do zasobów. Domyślna akcja: proces blokowania
Ochrona procesu LSASS	Chroni proces LSASS przed wyciekiem sekretnych informacji, takich jak hashe haseł i ustawienia zabezpieczeń. Działanie domyślne: Blokuje proces

Techniki anti-explit są domyślnie włączone. Aby wyłączyć którąkolwiek z nich, należy wyczyścić pole wyboru.

Opcjonalnie można zmienić podjętą czynność automatycznie po wykryciu. Wybierz działanie dostępne w odpowiednim menu:

- **Zakończ proces**: natychmiast kończy proces.
- **Proces blokowania**: zapobiega uzyskaniu dostępu do nieautoryzowanych zasobów przez złośliwy proces.
- **Tylko raportuj**: GravityZone zgłasza zdarzenie bez podejmowania żadnych działań łagodzących. Szczegóły dotyczące zdarzenia można zobaczyć w powiadomieniu **Zaawansowany Anti-exploit** oraz w raportach z audytu zablokowanych aplikacji i bezpieczeństwa.

Konfiguracja technik specyficznych dla danej aplikacji

Niezależnie od tego, czy są to aplikacje predefiniowane, czy dodatkowe, wszystkie one mają ten sam zestaw technik anti-exploit. Możesz je znaleźć tutaj:

Technika	Opis
Emulacja ROP	Wykrywa próby wykonania stron pamięci dla danych przy użyciu techniki programowania zorientowanego na powrót (ROP). Domyślna akcja: Proces blokowania
Oś Stosu ROP	Wykrywa próby przejęcia przepływu kodu przy użyciu techniki ROP, sprawdzając położenie stosu. Domyślna akcja: Proces blokowania

Technika	Opis
Nielegalne Połączenie ROP	Wykrywa próby przejęcia kontroli nad kodem przy użyciu techniki ROP, sprawdzając wywoływaczy wrażliwych funkcji systemowych. Domyślna akcja: Proces blokowania
Niepoprawny Stos ROP	Wykrywa próby uszkodzenia stosu za pomocą techniki ROP, sprawdzając poprawność wyrównania adresu stosu. Domyślna akcja: Proces blokowania
ROP powrócił do Stosu	Wykrywa próby wykonania kodu bezpośrednio na stosie przy użyciu techniki ROP, sprawdzając zakres adresów zwrotnych. Domyślna akcja: Proces blokowania
ROP wykonał Stos Wykonywalny	Wykrywa próby uszkodzenia stosu za pomocą techniki ROP, sprawdzając ochronę strony stosu. Domyślna akcja: Proces blokowania
Flash Generic	Wykrywa próby wykorzystania Flash Playera. Domyślna akcja: Proces blokowania
Flash Payload	Wykrywa próby wykonania złośliwego kodu w programie Flash Player, skanując obiekty Flash w pamięci. Domyślna akcja: Proces blokowania
Ogólny VBScript	Wykrywa próby wykorzystania VBScript. Domyślna akcja: Proces blokowania
Wykonanie Kodu Powłoki	Wykrywa próby tworzenia nowych procesów lub pobierania plików przy użyciu kodu powłoki. Domyślna akcja: Proces blokowania
Kod powłoki LoadLibrary	Wykrywa próby wykonania kodu za pośrednictwem ścieżek sieciowych przy użyciu kodu powłoki. Domyślna akcja: Proces blokowania
Anty-Debug	Wykrywa próby ominięcia kontroli bezpieczeństwa w celu utworzenia nowych procesów.

Technika	Opis
	Domyślna akcja: Proces blokowania
Kod powłoki EAF (Eksportowanie Filtrowania Adresów)	Wykrywa próby złośliwego kodu w celu uzyskania dostępu do wrażliwych funkcji systemu z eksportu DLL. Domyślna akcja: Proces blokowania
Wątek kodu powłoki	Wykrywa próby wstrzyknięcia złośliwego kodu, weryfikując nowo utworzone wątki. Domyślna akcja: Proces blokowania
Anty-Meterpreter	Wykrywa próby utworzenia odwrotnej powłoki, skanując strony pamięci wykonywalnej. Domyślna akcja: Proces blokowania
Tworzenie procesów zdezaktualizowanych	Wykrywa próby tworzenia nowych procesów przy użyciu przestarzałych technik. Domyślna akcja: Proces blokowania
Tworzenie procesu potomnego	Blokuje tworzenie dowolnego procesu potomnego. Domyślna akcja: Proces blokowania
Wymuszaj funkcję DEP systemu Windows	Wymusza zapobieganie wykonywaniu danych (DEP) w celu blokowania wykonywania kodu ze stron danych. Domyślnie: Wyłączone
Wymuś Relokacje Modułów (ASLR)	Zapobiega ładowaniu kodu w przewidywalnych lokalizacjach, przenosząc moduły pamięci. Domyślnie: Włączone
Pojawiające się Exploity	Chroni przed nowymi pojawiającymi się zagrożeniami lub exploitami. W przypadku tej kategorii stosowane są szybkie aktualizacje, zanim można wprowadzić bardziej kompleksowe zmiany. Domyślnie: Włączone

Aby monitorować inne aplikacje z wyjątkiem predefiniowanych, kliknij przycisk **Dodaj aplikację** dostępny u góry i na dole strony.

Aby skonfigurować ustawienia anty-exploit dla aplikacji:

1. W przypadku istniejących aplikacji, kliknij nazwę aplikacji. W przypadku nowych aplikacji, kliknij przycisk **Dodaj** .

   Nowa strona wyświetla wszystkie techniki i ich ustawienia dla wybranej aplikacji.

   WAŻNE
   Zachowaj ostrożność podczas dodawania nowych aplikacji do monitorowania. Bitdefender nie może zagwarantować zgodności z żadną aplikacją. Dlatego zaleca się przetestowanie funkcji najpierw na kilku niekrytycznych punktach końcowych, a następnie wdrożenie jej w sieci.

2. W przypadku dodawania nowej aplikacji wprowadź jej nazwę i nazwy procesów w dedykowanych polach. Użyj średnika (;), aby oddzielić nazwy procesów.
3. Jeśli chcesz szybko sprawdzić opis techniki, kliknij strzałkę obok jej nazwy.
4. W razie potrzeby zaznacz lub wyczyść pola wyboru technik eksploatacji.

   Użyj opcji **Wszystkie** , jeśli chcesz oznaczyć wszystkie techniki jednocześnie.
5. W razie potrzeby zmień działanie automatyczne po wykryciu. Wybierz działanie dostępne w odpowiednim menu:
   - **Zakończ proces**: natychmiast kończy proces.
   - **Tylko raportuj**: GravityZone zgłasza zdarzenie bez podejmowania żadnych działań łagodzących. Szczegóły wydarzenia możesz wyświetlić w powiadomieniu **Zaawansowany Anty-Exploit** oraz w raportach.

   Domyślnie wszystkie techniki dla predefiniowanych aplikacji są ustawione tak, aby złagodzić problem, podczas gdy dla dodatkowych aplikacji ustawiono tylko raportowanie zdarzenia.

   Aby szybko zmienić akcję wykonaną dla wszystkich technik jednocześnie, wybierz akcję z menu powiązanego z opcją **Wszystkie** .

Kliknij przycisk **Wstecz** w górnej części strony, aby powrócić do ustawień ogólnych Anty-Exploit.

Ustawienia

W tej sekcji możesz skonfigurować ustawienia kwarantanny i zasady wykluczeń podczas skanowania.

- Konfigurowanie Ustawień Kwarantanny
- Konfigurowanie wyjątków skanowania

Kwarantanna

Możesz skonfigurować następujące opcje dla kwarantanny plików z docelowego punktu końcowego:

- **Usuń pliki starsze niż (dni).** Domyślnie wszystkie pliki objęte kwarantanną dłużej niż 30 dni są automatycznie usuwane. Jeżeli chcesz zmienić przedział, wybierz inne opcje z menu.
- **Zgłoś pliki z kwarantanny do Laboratoriów Bitdefender każdej godziny.** Domyślnie pliki kwarantanny są automatycznie przesyłane do Laboratoriów Bitdefender każdej godziny. Możesz edytować przedziały czasu pomiędzy plikami kwarantanny, które zostały wysłane (domyślnie, co godzinę). Przykładowe pliki będą przeanalizowane przez badaczy szkodliwego oprogramowania firmy Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.
- **Ponowne skanowanie kwarantanny po aktualizacjach zawartości zabezpieczeń.** Zaznacz tę opcję, aby automatycznie skanować pliki poddane kwarantannie po każdej aktualizacji zawartości zabezpieczeń. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.
- **Kopiuj pliki do kwarantanny przed zastosowaniem działań dezynfekcji**. Wybierz tę opcję aby zapobiec utracie danych w przypadku fałszywych alarmów i skopiować wszystkie zainfekowane pliki do kwarantanny przed zastosowaniem działań dezynfekcji. Można potem przywrócić legalne pliki ze strony **Kwarantanna**.
- **Zezwalaj użytkownikom na podjęcie czynności dotyczących kwarantanny lokalnej.** Ta opcja kontroluje działania, które użytkownicy punktów końcowych mogą podejmować na lokalnych plikach poddanych kwarantannie przez interfejs Bitdefender Endpoint Security Tools. Domyślnie, użytkownicy lokalni mogą przywracać lub usuwać pliki poddane kwarantannie z komputera przy użyciu opcji dostępnych w Bitdefender Endpoint Security Tools. Po wyłączeniu tej opcji, użytkownicy nie mają dostępu do przycisków czynności z kwarantanny plików z interfejsu Bitdefender Endpoint Security Tools.

Scentralizowana Kwarantanna

Jeśli chcesz zachować pliki kwarantanny z zarządzanych punktów końcowych, w celu przeprowadzenia dalszej analizy, użyj opcji **Scentralizowana kwarantanna**,

która wysyła zarchiwizowaną kopię każdego lokalnego pliku poddanego kwarantannie do zasobów sieciowych.

Po włączeniu tej opcji, każdy plik poddany kwarantannie z zarządzanych punktów końcowych jest kopiowany i pakowany w zabezpieczone hasłem archiwum ZIP do określonej lokalizacji sieciowej. Nazwa archiwum jest skrótem pliku poddanego kwarantannie.

WAŻNE
Limit rozmiaru archiwum to 100 MB Jeśli archiwum przekracza 100 MB, nie zostanie zapisane w udostępnionej lokalizacji w sieci.

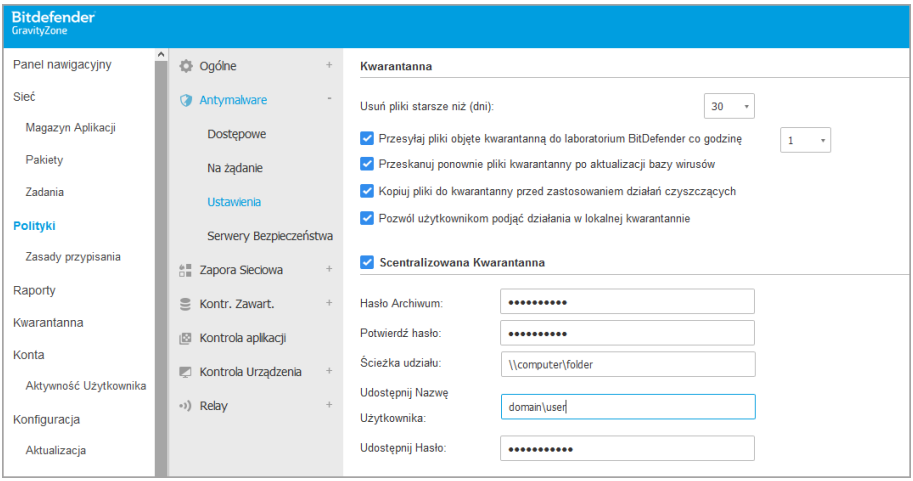
Aby skonfigurować scentralizowane ustawienia kwarantanny, wypełnij następujące pola:

- **Hasło archiwum**: wprowadź hasło wymagane do archiwizacji plików poddanych kwarantannie. Hasło musi zawierać co najmniej jedną wielką liter, co najmniej jedną małą literę i co najmniej jedną cyfrę lub jeden znak specjalny. Potwierdź hasło w podanym polu:
- **Udostępnij ścieżkę**: wprowadź ścieżkę sieciową, w której chcesz zapisać archiwa (na przykład `\\komputer\folder`).
- Do połączenia się z zasobami sieciowymi wymagana jest nazwa użytkownika i hasło. Obsługiwane formaty nazwy użytkownika są następujące:
  - `username@domain`
  - `domain\username`
  - `nazwa użytkownika`.

Aby scentralizowana kwarantanna działała poprawnie, upewnij się, że spełnione są następujące warunki:

- Udostępniona lokalizacja jest dostępna w sieci.
- Punkty końcowe mają łączność z zasobami sieciowymi.
- Poświadczenia logowania są poprawne i zapewniają dostępność wpisywania do zasobów sieciowych.
- Zasoby sieciowe mają wystarczająco dużo miejsca na dysku.

Notatka
Scentralizowana kwarantanna nie dotyczy kwarantanny serwerów poczty.



Scentralizowana Kwarantanna

Jeśli masz skonfigurowaną lokalną instancję Sandbox Analyzer skonfigurowaną w sekcji **Sandbox Analyzer > Czujnik punktu końcowego** możesz wybrać okienko **Automatycznie wysyłaj obiekty z kwarantanny do Sandbox Analyzer**. Wysyłane obiekty mogą mieć maksymalny rozmiar 50 MB.

Wykluczenia

Agent bezpieczeństwa Bitdefender może wykluczyć ze skanowania wskazane typy obiektów. Wykluczenia antymalware mają być stosowane w szczególnych okolicznościach lub zgodnie z zaleceniami Microsoft lub Bitdefender. Aktualna lista wyjątków, zalecana przez Microsoft, znajduje się w tym artykule.

W tej sekcji, możesz konfigurować użycie innych typów wyłączeń dostępnych w agencie bezpieczeństwa Bitdefender.

- **Wbudowane Wykluczenia** są domyślnie włączony i uwzględnione w agencie bezpieczeństwa Bitdefender.

  Możesz wybrać by wyłączyć wbudowane wykluczenia, jeżeli chcesz skanować wszystkie typy obiektów, ale ta opcja wydanie wpłynie na wydajność maszyny i zwiększy czas skanowania.

- Możesz także zdefiniować **Wyłączenia niestandardowe** dla wewnętrznych aplikacji lub dostosowanych narzędzi, zgodnie z Twoimi potrzebami.

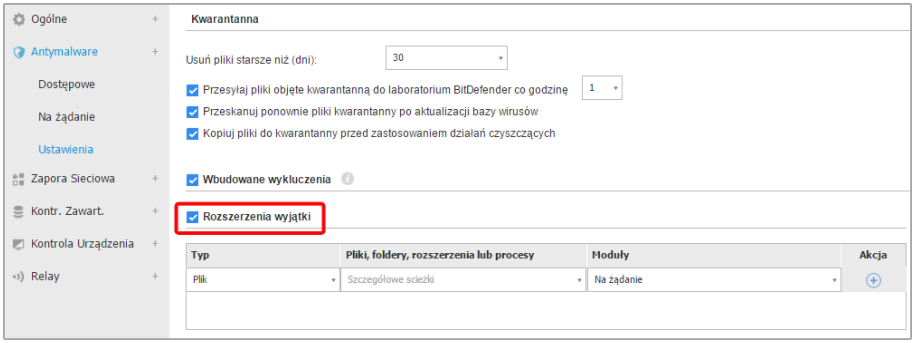
Niestandardowe wykluczenia Antymalware dotyczą jednej lub kilku następujących metod skanowania:

- Skanowanie dostępowe
- Skanowanie na żądanie
- Zaawansowana Kontrola Zagrożeń
- Ochrona przed Atakiem Bezplikowym
- Łagodzenie Skutków Ransomware

WAŻNE

- Jeżeli na komputerze znajduje się plik testowy EICAR służący do okresowego sprawdzania ochrony antymalware, należy pominąć go podczas skanowania na żądanie.
- Dla VMware Horizon View 7 i App Volumes AppStacks, przejdź do Dokument VMware.

Aby wykluczyć określone elementy ze skanowania, wybierz opcję **Wykluczenia niestandardowe** , a następnie dodaj reguły do tabeli poniżej.



Polityki Komputerów i Maszyn Wirtualnych - Niestandardowe Wykluczenia

Aby dodać regułę niestandardowego wyjątku.

1. Wybierz rodzaje wyjątków z menu:
   - **Plik**: tylko określony plik

- **Folder**: wszystkie pliki i procesy w określonym folderze i ze wszystkich jego podfolderów
- **Rozszerzenie**: wszystkie elementy o określonym rozszerzeniu
- **Proces** : dowolny obiekt, do którego dostęp ma wykluczony proces
- **Plik Hash** : plik z określonym hashem
- **Hash certyfikatu**: wszystkie aplikacje pod określonym hashem certyfikatu (odcisk palca)
- **Nazwa Zagrożenia**: każdy element mający nazwę wykrycia (niedostępne dla systemów operacyjnych z Linux).
- **Wiersz Poleceń**: określony wiersz poleceń (dostępne jedynie dla systemów operacyjnych z Windows)

Ostrzeżenie
W bezagentowych środowiskach VMware zintegrowanych z vShield możesz wykluczyć tylko foldery i rozszerzenia. Instalując Bitdefender Tools na maszynach wirtualnych, możesz także wyłączyć pliki i procesy.
W trakcie instalacji, konfigurując pakiet, musisz zaznaczyć pole wyboru **Wdróż końcówkę z vShieldem kiedy środowisko VMware zintegrowane z vShieldem jest wykryte** . Aby uzyskać więcej informacji, zapoznaj się z sekcją **Tworzenie pakietów instalacyjnych** w Instrukcji instalacji.

2. Podaj szczegóły specyficzne dla wybranego typu wykluczenia:

   Plik, Folder albo Proces

   Wprowadź ścieżkę do elementu, który ma zostać wykluczony ze skanowania. Masz kilka przydatnych opcji do napisania ścieżki:

   - W jasny sposób wyznacz ścieżkę.

     Na przykład: `C: emp`

     Aby dodać wykluczenia dla ścieżek UNC, użyj dowolnej składni:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   - Użyj zmiennych systemowych dostępnych w menu rozwijanym.

     Aby wykluczyć proces, musisz również dodać nazwę pliku wykonywalnego aplikacji.

Na przykład:

`%ProgramFiles%` - nie obejmuje folderu Program Files

`%WINDIR%\system32` - wyklucza system folderów32 w folderze Windows

Notatka
Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.

– Użyj symboli wieloznacznych.

Gwiazdka (*) zastępuje zero lub więcej znaków. Znak zapytania (?) zastępuje dokładnie jeden znak. Możesz użyć kilku znaków zapytania aby zdefiniować każdą kombinacje określonej liczby znaków. Na przykład, ??? zastępuje każdą kombinację dokładnie 3 znaków.

Na przykład:

Wykluczenia plików:

`C:\Test\*` - wyklucza wszystkie pliki z folderu Test

`C:\Test\*.png` - wyklucza wszystkie pliki PNG, z folderu testowego

Wykluczenia folderów:

`C:\Test\*` - wyklucza wszystkie foldery z folderu Test

Wykluczenia procesów:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` - wyklucza procesy Microsoft Notes.

Notatka
Wykluczenia procesów nie wspierają dzikich kart w systemach operacyjnych Linux.

Rozszerzenie

Wprowadź jedno lub więcej rozszerzeń plików, które mają być wyłączone ze skanowania, rozdzielając je średnikiem ";". Możesz wprowadzić rozszerzenia poprzedzając je kropką, ale nie musisz. Na przykład, wpisz txt aby wykluczyć pliki tekstowe.

Notatka
W systemach opartych na Linux, w rozszerzeniach plików rozróżniana jest wielkość liter, a pliki o tej samej nazwie, ale z innym rozszerzeniem są uważane za odrębne obiekty. Na przykład, `file.txt` różni się od `file.TXT`.

Skrót pliku, skrót certyfikatu, nazwa zagrożenia lub wiersz poleceń

Wprowadź hash pliku, hash certyfikatu, dokładną nazwa zagrożenia lub wiersza poleceń w zależności od reguły wykluczenia. Możesz użyć jednej pozycji na każde wykluczenie.

3. Wybierz metody skanowania, do których ma zastosowanie reguła. Niektóre wykluczenia mogą dotyczyć skanowania dostępowego, skanowania na żądanie, ATC/IDS, podczas gdy inne mogą być zalecane dla wszystkich trzech modułów.
4. Opcjonalnie, kliknij przycisk **Pokaż uwagi**, aby dodać notatkę o regule w kolumnie **Uwagi**.
5. Kliknij przycisk ⊕ **Dodaj** .

   Do listy zostanie dodana nowa reguła.

Aby usunąć zasadę z listy, kliknij odpowiadający jej przycisk ⊗ **Usuń**.

WAŻNE
Należy pamiętać, że wyjątki skanowania na żądania nie zostaną zastosowane w skanowaniu kontekstowym. Kontekstowe skanowanie jest inicjowane poprzez kliknięcie prawym klawiszem myszy pliku lub folderu i wybranie **Skanuj przy użyciu Bitdefender Endpoint Security Tools**.

Importowanie i Eksportowanie Wyjątków

Jeśli zamierzasz używać ponownie reguł wykluczeń w większej ilości polityk, możesz wybrać, aby je eksportować i zaimportować.

Aby eksportować niestandardowe wyjątki:

1. Kliknij **Eksportuj** w górnej części tabeli wykluczeń.
2. Zapisz plik CSV na swoim komputerze. W zależności od twoich ustawień przeglądarki, plik może być pobierany automatycznie lub zostaniesz poproszony, aby go zapisać do lokalizacji.

Każdy wiersz w pliku CSV odpowiada pojedynczej regule, mając pola w następującej kolejności:

```
<exclusion type>, <object to be excluded>, <modules>
```

Oto dostępne wartości dla pól CSV:

Typ wyjątku:

- 1, dla wyjątków plików
- 2, dla wyjątków folderów
- 3, dla wyjątków rozszerzeń
- 4, dla wyjątków procesów
- 5, dla wyjątków skrótów plików
- 6, dla certyfikatów skótów wykluczeń
- 7, dla wykluczeń nazw zagrożeń
- 8, dla wykluczeń linii poleceń

Obiekt jaki ma być wykluczony:

Ścieżka lub rozszerzenie pliku

Moduły:

- 1, dla skanowania na żądanie
- 2, dla skanowania dostępowego
- 3, dla wszystkich modułów
- 4, dla ATC/IDS

Na przykład, plik CSV zawierający wykluczenia antymalware może wyglądać tak:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Notatka
Ścieżki Windows muszą mieć dwukrotny znak backslash (\). Na przykład, `%WinDir%\\System32\\LogFiles`.

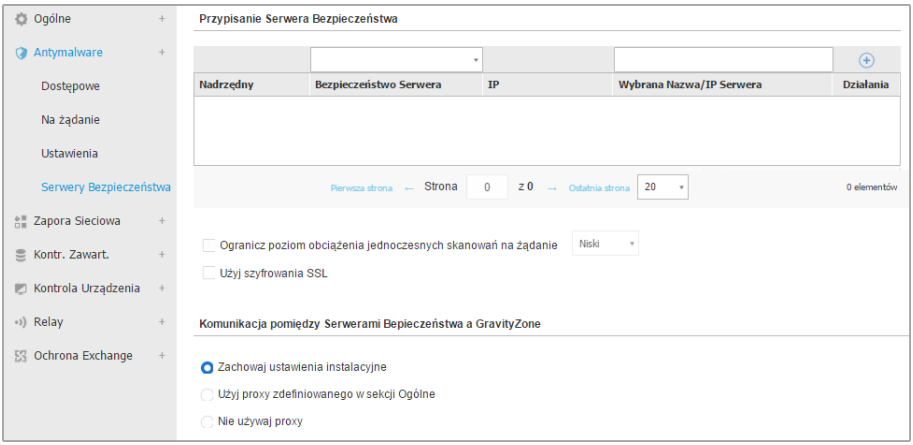
Aby zaimportować niestandardowe wyjątki:

1. Kliknij opcję **Importuj**. Otwiera sie okno **Importuj Wyjątki Polityk**.
2. Kliknij **Dodaj**, a następnie wybierz plik CSV.
3. Kliknij **Zapisz**. Tabela jest zapełniona poprawnymi regułami. Jeśli plik CSV zawiera nieprawidłowe reguły, ostrzeżenie informuje o odpowiednich numerach wierszy.

Security Server

W tej sekcji możesz skonfigurować:

- Przypisywanie Security Server
- Określone ustawienia Security Server



Polityka - Komputerów i Maszyn Wirtualnych - Antymalware - Serwerów Bezpieczeństwa

Przyporządkowanie Security Server

Możesz przypisać jeden lub kilka Security Servers do docelowych punktów końcowych i ustawić priorytet, z którym punktem końcowym wybierać Security Server do wysyłania żądań skanowania.

Notatka
Zaleca się używanie Security Server do skanowania maszyn wirtualnych lub komputerów z niskimi zasobami.

Aby przypisać Security Server do docelowych punktów końcowych, dodaj Security Server, których chcesz użyć, z tabeli **Przypisywanie Security Server**, w następujący sposób:

1. Kliknij listę rozwijaną **Security Server** , a następnie wybierz Security Server.
2. Jeśli Security Server znajduje się w DMZ lub za serwerem NAT, wprowadź FQDN lub IP serwera NAT w polu **Nazwa Niestandardowego Serwera/IP**.

   WAŻNE
   Upewnij się, że przekierowanie portów jest poprawnie skonfigurowane na serwerze NAT, aby ruch z punktów końcowych mógł dotrzeć do Security Server.

3. Kliknij przycisk ⊕ **Dodaj** w kolumnie **Akcje** .

   Security Server został dodany do listy.
4. Powtórz poprzednie kroki, aby dodać inne Security Servers, jeśli są dostępne lub potrzebne.

Aby ustawić priorytet Security Servers:

1. Użyj strzałek w górę i w dół dostępnych w kolumnie **Działania** , aby zwiększyć lub zmniejszyć każdy priorytet Security Server.

   Przypisując więcej Security Servers, ten na górze listy ma najwyższy priorytet i zostanie wybrany jako pierwszy. Jeśli ten Security Server jest niedostępny lub przeciążony, wybierany jest następny Security Server. Skanowany ruch jest przekierowywany do pierwszego dostępnego Security Server i ma odpowiednie obciążenie.
2. Wybierz **Najpierw połącz się z Security Server zainstalowanym na tym samym hoście fizycznym, jeśli jest dostępny, niezależnie od przypisanego priorytetu** dla jednolitego rozmieszczenia punktów końcowych i dla optymalnego opóźnienia. Jeśli ten Security Server jest niedostępny, zostanie wybrany Security Server z listy, zgodnie z priorytetem.

   WAŻNE
   Ta opcja działa tylko z Security Server Multi-Platform i tylko wtedy, gdy GravityZone jest zintegrowany ze środowiskiem wirtualnym.

Aby usunąć Security Server z listy, kliknij odpowiedni przycisk ⊗ **Usuń** w kolumnie **Działania** .

Ustawienia Security Server

Przypisując politykę do Security Servers, możesz skonfigurować dla nich następujące ustawienia:

- **Ogranicz liczbę jednoczesnych skanowań na żądanie**.

  Uruchamianie wielu zadań skanowania na maszynach wirtualnych współdzielących ten sam magazyn danych na żądanie, może stworzyć burze skanowania antymalware. Aby temu zapobiec i zezwolić na uruchomienie tylko określonej liczby zadań skanowania jednocześnie:

  1. Wybierz opcję **Ogranicz liczbę jednoczesnych skanowań na żądanie** .
  2. Wybierz poziom dozwolonych jednoczesnych zadań skanowania z menu rozwijanego. Możesz wybrać predefiniowany poziom lub wprowadzić wartość niestandardową.

     Wzór na znalezienie maksymalnego limitu zadań skanowania dla każdego wstępnie zdefiniowanego poziomu to: `N = a x MAX(b ; vCPUs - 1)`, gdzie:

     - `N` = maksymalny limit zadań skanowania
     - `a` = współczynnik mnożący o następujących wartościach: `1` - dla Niski; `2` - dla Średni; `4` - dla Wysoki
     - `MAX(b;vCPU-1)` = funkcja zwracająca maksymalną liczbę slotów skanowania dostępnych w Security Server.
     - `b` = domyślna liczba slotów skanowania na żądanie, która obecnie jest ustawiona na cztery.
     - `vCPUs` = liczba wirtualnych CPUs przypisanych do Security Server

     Na przykład:

     Dla Security Server z 12 procesorami i wysokim poziomem równoczesnych skanów, mamy limit:

     `N = 4 x MAX(4; 12-1) = 4 x 11 = 44` równoczesne zadania skanowania na żądanie.

- **Włącz reguły powinowactwa dla Security Server Multi-Platform**

Określ działanie, które powinien wykonać Security Server, gdy jego host przejdzie w tryb konserwacji:

– Jeśli jest włączona, Security Server pozostaje powiązany z hostem i GravityZone wyłącza go. Po zakończeniu konserwacji GravityZone automatycznie uruchamia ponownie Security Server.

  To jest zachowanie domyślne.

– Jeśli jest wyłączone, Security Server jest przenoszony do innego hosta i kontynuuje działanie. W tym przypadku nazwa Security Server zmienia się w Control Center, aby wskazać byłego hosta. Zmiana nazwy trwa do momentu przeniesienia Security Server z powrotem do macierzystego hosta.

  Jeśli zasoby są wystarczające, Security Server może wylądować na hoście, na którym zainstalowany jest inny Security Server.

  WAŻNE
  Ta opcja nie działa, jeśli Security Server jest również używany przez HVI.

- **Użyj szyfrowania SSL**

  Włącz tę opcję, jeśli chcesz zaszyfrować połączenie między docelowymi punktami końcowymi a określonymi urządzeniami Security Server.

  Domyślnie GravityZone używa samopodpisanych certyfikatów bezpieczeństwa. Możesz je zmienić za pomocą własnych certyfikatów na stronie **Konfiguracja > Certyfikaty** w Control Center. Więcej informacji znajduje się w rozdziale "Konfiguruj ustawienia Control Center" w Instrukcji instalacji.

- **Komunikacja między Security Servers a GravityZone**

  Wybierz jedną z dostępnych opcji, aby zdefiniować preferencje serwera proxy dla komunikacji między wybranymi komputerami Security Server i GravityZone:

  – **Zachowaj ustawienia instalacyjne**, w celu zachowania tych samych ustawień proxy zdefiniowanych wraz z paczką instalacyjną.

  – **Użyj zdefiniowanego w Głównej sekcji proxy**, aby użyć ustawień zdefiniowanych dla aktualnej polityki, pod sekcją **Ogólne > Ustawienia**.

  – **Nie używaj serwera proxy** , gdy docelowe punkty końcowe nie komunikują się z określonymi komponentami Bitdefender za pośrednictwem serwera proxy.

7.2.4. Sandbox Analyzer

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów

Sandbox Analyzer zapewnia potężną warstwę ochrony przed zaawansowanymi zagrożeniami, wykonując automatyczną, szczegółową analizę podejrzanych plików, które jeszcze nie zostały podpisane przez silniki antimalware Bitdefender.

W tej sekcji możesz skonfigurować następujące:

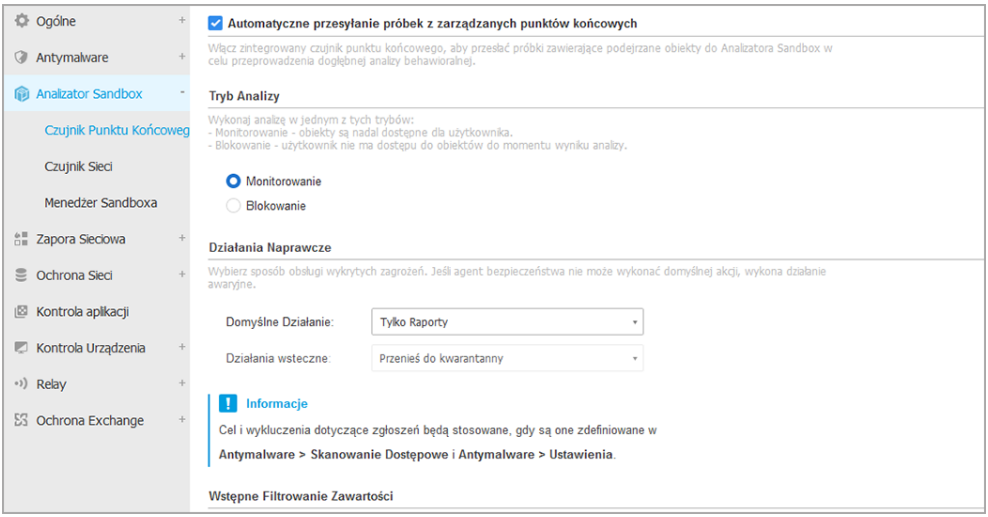
- Przesłanie poprzez czujnik punktu końcowego
- Przesłanie poprzez sensor sieciowy
- Przesłanie poprzez sensor ICAP
- Ustawienia Menedżera Piaskownicy

W ustawieniach polityki możesz również skonfigurować automatyczne wysyłanie ze scentralizowanej kwarantanny. Szczegółowe informacje znajdują się w „Scentralizowana Kwarantanna” (p. 285).

Po szczegółowe informacje na temat ręcznego przesyłania, zajrzyj do „Ręczne Wysyłanie” (p. 474). Aby uzyskać szczegółowe informacje o wysyłaniu z API, odnieś się do rozdziałów **Piaskownica** i **Portal Piaskownicy** w Przewodniku API GravityZone (On-Premises).

Czujnik Punktu Końcowego

Bitdefender Endpoint Security Tools może działać jako czujnik zasilający dla Sandbox Analyzer z punktów końcowych z Windows.



Polityki > Sandbox Analyzer > Czujnik punktu końcowego

Aby skonfigurować automatyczne przesyłanie przez sensor punktu końcowego:

1. W **Ustawienia połączenia**, wybierz jedną z opcji:
   - **Użyj chmury Sandbox Analyzer** - czujnik punktu końcowego prześle próbki do instancji Sandbox Analyzer hostowanej przez Bitdefender, zależnie od regionu.
   - **Użyj lokalnej instancji Analizatora Sandbox** - czujnik punktu końcowego prześle próbki do instancji Sandbox Analyzer On-Premises. Wybierz preferowaną instancję Sandbox Analyzer z rozwijanego menu.

   Jeśli Twoja sieć znajduje się za serwerem proxy lub zaporą sieciową, możesz skonfigurować serwer proxy do łączenia się z Sandbox Analyzer przez zaznaczenie pola wyboru **Użyj konfiguracji proxy**.

   Należy wypełnić następujące pola:
   - **Serwer** — IP serwera proxy
   - **Port** - port używany do połączenia z serwerem proxy.
   - **Nazwa użytkownika** – nazwa użytkownika rozpoznawana przez proxy.
   - **Hasło** - poprawne hasło dla określonego użytkownika.

2. Zaznacz pole wyboru **Automatyczne przesyłanie próbek z zarządzanych punktów końcowych**, aby umożliwić automatyczne przesyłanie podejrzanych plików do Sandbox Analyzer.

   WAŻNE

   - Sandbox Analyzer wymaga Skanowania Dostępowego. Upewnij się, że masz włączony moduł **Antymalware> Skanowanie Dostępowe**.
   - Sandbox Analyzer wykorzystuje te same cele i wykluczenia, jak te zdefiniowane w **Antymalware > Skanowanie Dostępowe**. Konfigurując Sandbox Analyzer, sprawdź dokładnie ustawienia Skanowania Dostępowego.
   - Aby uniknąć fałszywych alarmów (nieprawidłowego wykrycia legalnych aplikacji), można skonfigurować wykluczenia według nazwy pliku, rozszerzenia, rozmiaru pliku i ścieżki pliku. Aby uzyskać więcej informacji na temat Skanowania Dostępowego, przejdź do „Antymalware" (p. 257).
   - Limit przesyłania plików lub archiwum wynosi 50 MB.

3. Wybierz **Moduł Analizy**. Dostępne są dwie opcje:
   - **Monitorowanie**. Użytkownik może uzyskać dostęp do pliku podczas analizy sandbox, ale zaleca się, aby nie wykonywać go do momentu otrzymania wyniku analizy.
   - **Blokowanie**. Użytkownik nie może wykonać pliku, dopóki wynik analizy nie zostanie zwrócony do punktu końcowego z Klastra Sandbox Analyzer przez Portal Sandbox Analyzer.
4. Określ **Działania Naprawcze**. Takie działania zostają podjęte, gdy Sandbox Analyzer wykryje zagrożenie. Dla każdego Modułu analizy masz podwójną konfigurację, składającą się z jednego działania domyślnego i jednego działania awaryjnego. Sandbox Analyzer wykonuje początkowo działanie domyślne, a następnie (jeśli działanie awaryjne nie może zostać wykonane) działanie awaryjne.

   Gdy uzyskujesz dostęp sekcji po raz pierwszy, dostępne są następujące konfiguracje:

   Notatka
   W tej konfiguracji zaleca się zastosowanie działań awaryjnych.

   - W module **Monitorowanie**, działaniem domyślnym jest **Tylko Raportuj**, a opcja działania awaryjnego jest wyłączona.

- W module **Blokowanie**, działaniem domyślnym jest **Kwarantanna**, a działaniem awaryjnym jest opcja **Usuń**.

Sandbox Analyzer zapewnia następujące działania naprawcze:

- **Dezynfekuj**. Usuwa złośliwy kod z zainfekowanych plików.
- **Usuń**. Usuwa cały wykryty plik z dysku.
- **Kwarantanna**. Przenosi wykryte pliki z ich obecnej lokalizacji do folderu kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami kwarantanny ze strony **Kwarantanna** w Control Center.
- **Tylko raport**. Sandbox Analyzer tylko raportuje wykryte zagrożenia, ale nie podejmuje żadnych działań.

Notatka
Zależnie od domyślnego działania, działanie alarmowe może być niedostępne.

5. Obie domyślne i alternatywne akcje są ustawione w trybie **Tylko Raporty**.
6. W obszarze **Wstępne Filtrowanie Treści** dostosuj poziom ochrony przed potencjalnymi zagrożeniami. Czujnik punktu końcowego posiada wbudowany mechanizm filtrowania zawartości, który określa, czy podejrzany plik musi zostać zdetonowany w Sandbox Analyzer.

   Obsługiwane typy obiektów to: aplikacje, dokumenty, skrypty, archiwa, wiadomości e-mail. Aby uzyskać więcej informacji na temat obsługiwanych typów obiektów, zobacz „Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania” (p. 520).

   Użyj przełącznika głównego, znajdującego się na górze listy zagrożeń, aby wybrać unikalny poziom ochrony przed wszystkimi obiektami lub wybierz poszczególne poziomy, aby dokładnie doprecyzować ochronę.

   Ustawienie modułu na określonym poziomie skutkuje określoną liczbą przesłanych próbek.

   - **Tolerancyjne**. Czujnik punktu końcowego automatycznie przesyła do Sandbox Analyzer tylko obiekty o najwyższym prawdopodobieństwie bycia złośliwym i ignoruje pozostałe obiekty.

- **Normalny**. Czujnik punktu końcowego znajduje równowagę między przesłanymi i ignorowanymi obiektami i wysyła do Sandbox Analyzer oba obiekty, z większym i mniejszym prawdopodobieństwem bycia złośliwymi.
- **Agresywny**. Czujnik punktu końcowego przesyła do Sandbox Analyzer prawie wszystkie obiekty, niezależnie od ich potencjalnego ryzyka.

W dedykowanym polu można zdefiniować wyjątki dla typów obiektów, których nie chcemy przesyłać do Sandbox Analyzer.

Można również zdefiniować granice wielkości przesyłanych obiektów poprzez zaznaczenie odpowiedniego pola wyboru i wprowadzenie dowolnych wartości pomiędzy 1 KB a 50 MB.

7. Pod **Profil detonacji**, dostosuj poziom złożoności analizy behawioralnej, jednocześnie wpływając na przepustowość Sandbox Analyzer. Na przykład, jeśli jest ustawiony na **Wysoki**, Sandbox Analyzer wykonałby dokładniejszą analizę na mniejszej liczbie próbek w tym samym przedziale czasu niż na **Średni** lub **Niski**.

Sandbox Analyzer obsługuje wysyłanie plików lokalnych za pomocą punktów końcowych z rolą przekaźnika, które mogą łączyć się z różnymi adresami Portalu Sandbox Analyzer w zależności od regionu. Szczegółowe informacje na temat ustawień konfiguracyjnych przekaźnika znajdują się w „Relay” (p. 348).

Notatka
Serwer proxy skonfigurowany w ustawieniach połączeń Sandbox Analyzer zastąpi wszelkie punkty końcowe z rolą przekaźnika.

Czujnik Sieci

W tej sekcji możesz skonfigurować automatyczne wysyłanie przykładów ruchu sieciowego do Sandbox Analyzer poprzez sensor sieciowy. Ten moduł potrzebuje, aby Urządzenie wirtualne Ochrona Sieci najdowało się w sieci i było skonfigurowane z Sandbox Analyzer On-Premises

Aby skonfigurować automatyczne przesyłanie przez sensor sieciowy:

1. Wybierz pole wyboru **Automatyczne przesyłanie próbek dla sensora sieciowego**, aby włączyć automatyczne przesyłanie podejrzanych plików do Sandbox Analyzer.
2. W obszarze **Wstępne Filtrowanie Treści** dostosuj poziom ochrony przed potencjalnymi zagrożeniami. Sensor sieciowy ma wbudowany mechanizm

filtrowania treści, który określa, czy podejrzany plik wymaga detonacji w Sandbox Analyzer.

Obsługiwane typy obiektów to: aplikacje, dokumenty, skrypty, archiwa, wiadomości e-mail. Aby uzyskać więcej informacji na temat obsługiwanych typów obiektów, zobacz „Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania" (p. 520).

Użyj przełącznika głównego, znajdującego się na górze listy zagrożeń, aby wybrać unikalny poziom ochrony przed wszystkimi obiektami lub wybierz poszczególne poziomy, aby dokładnie doprecyzować ochronę.

Ustawienie modułu na określonym poziomie skutkuje określoną liczbą przesłanych próbek.

- **Tolerancyjne**. Sensor sieciowy automatycznie przesyła do Sandbox Analyzer tylko obiekty z najwyższym prawdopodobieństwem bycia złośliwym i ignoruje pozostałe obiekty.
- **Normalny**. Sensor sieciowy znajduje balans pomiędzy przesłanymi, a ignorowanymi obiektami i przesyła do Sandbox Analyzer oba obiekty z wyższym i niższym prawdopodobieństwem bycia złośliwymi.
- **Agresywny**. Sensor sieciowy przesyła do Sandbox Analyzer prawie wszystkie obiekty, niezależnie od ich potencjalnego ryzyka.

W dedykowanym polu można zdefiniować wyjątki dla typów obiektów, których nie chcemy przesyłać do Sandbox Analyzer.

Można również zdefiniować granice wielkości przesyłanych obiektów poprzez zaznaczenie odpowiedniego pola wyboru i wprowadzenie dowolnych wartości pomiędzy 1 KB a 50 MB.

3. Pod **Ustawienia Połączenia**, wybierz preferowaną instancję Sandbox Analyzer dla przesyłania zawartości sieciowej.

   Jeśli Twoja sieć znajduje się za serwerem proxy lub zaporą sieciową, możesz skonfigurować serwer proxy do łączenia się z Sandbox Analyzer przez zaznaczenie pola wyboru **Użyj konfiguracji proxy**.

   Należy wypełnić następujące pola:

   - **Serwer** — IP serwera proxy
   - **Port** - port używany do połączenia z serwerem proxy.
   - **Nazwa użytkownika** – nazwa użytkownika rozpoznawana przez proxy.

- **Hasło** - poprawne hasło dla określonego użytkownika.

4. Pod **Profil detonacji**, dostosuj poziom złożoności analizy behawioralnej, jednocześnie wpływając na przepustowość Sandbox Analyzer. Na przykład, jeśli jest ustawiony na **Wysoki**, Sandbox Analyzer wykonałby dokładniejszą analizę na mniejszej liczbie próbek w tym samym przedziale czasu niż na **Średni** lub **Niski**.

Sensor ICAP

W tej sekcji możesz skonfigurować automatyczne przesyłanie do Sandbox Analyzer przez sensor ICAP.

Notatka
Sandbox Analyzer wymaga Security Server skonfigurowanego do skanowania network-attached storage (NAS) urządzeń, które używają protokołu ICAP. Po szczegóły zajrzyj do„Ochrona pamięci" (p. 386)

1. Wybierz pole wyboru **Automatyczne przesyłania próbek z sensora ICAP**, aby włączyć automatyczne przesyłanie podejrzanych plików do Sandbox Analyzer.
2. W obszarze **Wstępne Filtrowanie Treści** dostosuj poziom ochrony przed potencjalnymi zagrożeniami. Sensor sieciowy ma wbudowany mechanizm filtrowania treści, który określa, czy podejrzany plik wymaga detonacji w Sandbox Analyzer.

   Obsługiwane typy obiektów to: aplikacje, dokumenty, skrypty, archiwa, wiadomości e-mail. Aby uzyskać więcej informacji na temat obsługiwanych typów obiektów, zobacz „Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania" (p. 520).

   Użyj przełącznika głównego, znajdującego się na górze listy zagrożeń, aby wybrać unikalny poziom ochrony przed wszystkimi obiektami lub wybierz poszczególne poziomy, aby dokładnie doprecyzować ochronę.

   Ustawienie modułu na określonym poziomie skutkuje określoną liczbą przesłanych próbek.

   - **Tolerancyjne**. Sensor ICAP automatycznie przesyła do Sandbox Analyzer tylko obiekty z najwyższym prawdopodobieństwem bycia złośliwymi i ignoruje pozostałe obiekty.

- **Normalny**. Sensor ICAP znajduje balans pomiędzy przesłanymi i zignorowanymi obiektami i wysyła do Sandbox Analyzer oba obiekty z wyższym i niższym prawdopodobieństwem bycia złośliwym.
- **Agresywny**. Sensor ICAP przesyła do Sandbox Analyzer prawie wszystkie obiekty, niezależnie od potencjalnego ryzyka.

W dedykowanym polu można zdefiniować wyjątki dla typów obiektów, których nie chcemy przesyłać do Sandbox Analyzer.

Można również zdefiniować granice wielkości przesyłanych obiektów poprzez zaznaczenie odpowiedniego pola wyboru i wprowadzenie dowolnych wartości pomiędzy 1 KB a 50 MB.

3. Pod **Ustawienia Połączenia**, wybierz preferowaną instancję Sandbox Analyzer dla przesyłania zawartości sieciowej.

   Jeśli Twoja sieć znajduje się za serwerem proxy lub zaporą sieciową, możesz skonfigurować serwer proxy do łączenia się z Sandbox Analyzer przez zaznaczenie pola wyboru **Użyj konfiguracji proxy**.

   Należy wypełnić następujące pola:

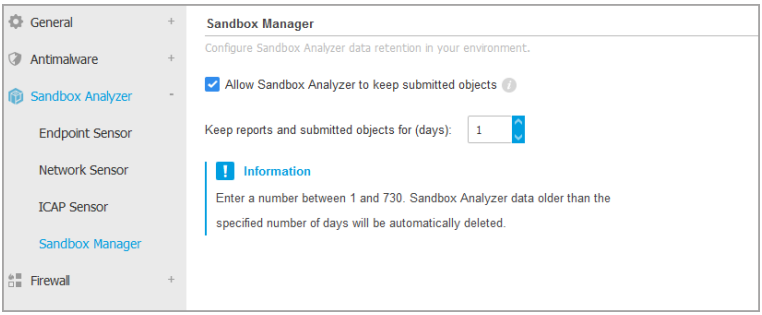
   - **Serwer** — IP serwera proxy
   - **Port** - port używany do połączenia z serwerem proxy.
   - **Nazwa użytkownika** – nazwa użytkownika rozpoznawana przez proxy.
   - **Hasło** - poprawne hasło dla określonego użytkownika.
4. Pod **Profil detonacji**, dostosuj poziom złożoności analizy behawioralnej, jednocześnie wpływając na przepustowość Sandbox Analyzer. Na przykład, jeśli jest ustawiony na **Wysoki**, Sandbox Analyzer wykonałby dokładniejszą analizę na mniejszej liczbie próbek w tym samym przedziale czasu niż na **Średni** lub **Niski**.

Menedżer Sandboxa

W tej sekcji konfigurujesz przechowywanie danych dla instancji Sandbox Analyzer:

- Zaznacz pole wyboru **Zezwól, aby Sandbox Analyzer trzymał przesłane obiekty**. To ustawienie pozwoli ci na korzystanie z opcji **Ponownie prześlij do analizy** w obszarze wysyłania w interfejsie raportowania Sandbox Analyzer
- Określ liczbę dni przez którą Sandbox Analyzer ma przechowywać raporty i przesłane obiekty w magazynie danych. Maksymalna ilość danych jaką możesz

wprowadzić to 730. Po wygaśnięciu określonego okresu, wszystkie dane zostaną usunięte.



Polityki > Sandbox Analyzer > Menedżer Sandbox

7.2.5. Zapora Sieciowa

Notatka
Ten jest dostępny dla stacji roboczych z Windows.

Zapora Sieciowa chroni punkty końcowe przed przychodzącymi i wychodzącymi próbami nieautoryzowanego połączenia.

Funkcjonalność zapory opiera się na profilach sieciowych. Profile bazują na zaufanych poziomach, które są zdefiniowane dla każdej sieci.

Zapora sieciowa wykrywa każde nowe połączenie, porównuje adapter informacji dla tych połączeń z informacjami od istniejącego profilu i zastosowuje prawidłowy profil. W celu uzyskania szczegółowych informacji jak stosować profile, zobacz „Ustawienia Sieci” (p. 308).

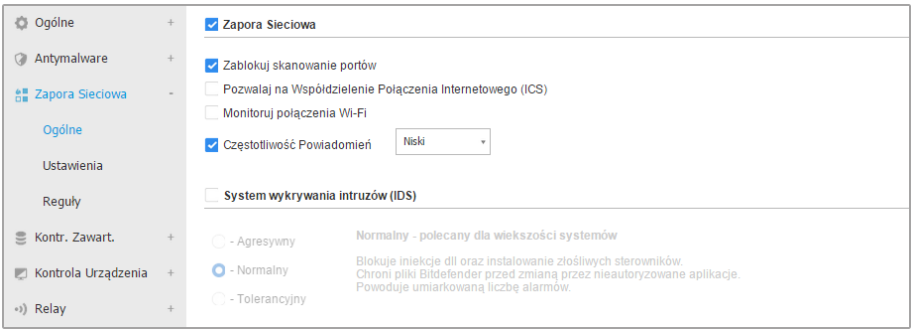
WAŻNE
Moduł Zapory Sieciowej jest dostępny jedynie dla wspieranych stacji roboczych Windows.

Ustawienia są zorganizowane w poniższych sekcjach:

- Ogólne
- Ustawienia
- Reguły

Ogólne

W tej sekcji możesz włączyć lub wyłączyć zaporę sieciową programu Bitdefender, a także skonfigurować ustawienia ogólne.



Polityki Komputerów i Maszyn Wirtualnych - Ustawienia Ogólne Zapory Sieciowej

- **Zapora Sieciowa.** Użyj pola wyboru aby włączyć lub wyłączyć Zaporę Sieciową.

  Ostrzeżenie
  Jeżeli wyłączysz zaporę sieciową, komputery będą podatne na ataki sieciowe i Internetowe.

- **Zablokuj skanowanie portów.** Operacja skanowania portów jest często wykorzystywana przez hakerów w celu znalezienia otwartych portów na komputerze. Napastnicy mogą włamać się do komputera, jeśli znajdą słabo zabezpieczony lub podatny port.
- **Pozwalaj na Współdzielenie Połączenia Internetowego (ICS).** Wybierz tę opcję aby ustawić zaporę sieciową tak aby dopuszczała udostępnianie połączenia internetowego.

  Notatka
  Ta opcja nie włącza automatycznie ICS w systemie użytkownika.

- **Monitoruj połączenia Wi-Fi.** Agent bezpieczeństwa Bitdefender może poinformować użytkownika połączonego do sieci Wi-Fi gdy nowy komputer dołącza do jego sieci. Aby wyświetlić informacje na ekranie użytkownika, wybierz tę opcję.

- **Częstotliwość Powiadomień.** Agent Bezpieczeństwa Bitdefender utrzymuje dziennik zdarzeń zależnie od użycia modułu Zapory Sieciowe (włączanie/wyłączanie zapory, blokowanie ruchu, modyfikowanie ustawień) lub generowane poprzez wykrytą aktywność tego modułu (skanowanie portów, blokowanie prób połączenia lub ruchu zgodnie z zasadami). Wybierz opcje z **Częstotliwość Powiadomień** aby określić jak wiele informacji powinien zawierać dziennik.
- **System Wykrywania Włamań.** Wykrywanie/Zapobieganie włamań sprawdza system pod kątem podejrzanych działań (na przykład: nieautoryzowany dostęp do plików programu Bitdefender, wstrzykiwanie bibliotek DLL, próby logowania naciskanych klawiszy itp.).

  Notatka
  Ustawienia polityki Systemu Wykrywania Włamań (IDS) mają zastosowanie tylko do Endpoint Security (starszego agenta zabezpieczeń). Agent Bitdefender Endpoint Security Tools integruje funkcje Systemu Wykrywania Włamań oparte na hoście w module Zaawansowanej Kontroli Zagrożeń (ATC).

  Konfigurowanie Systemu Wykrywania Włamań:

  1. Użyj pola wyboru aby włączyć lub wyłączyć system wykrywania włamań(IDS).
  2. Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

  Aby zapobiec wykryciu legalnych aplikacji przez System Wykrywania Włamań, dodaj **regułę wyjątku procesu ATC/IDS** dla aplikacji w sekcji **Antymalware > Ustawienia > Niestandardowe Wyjątki**.

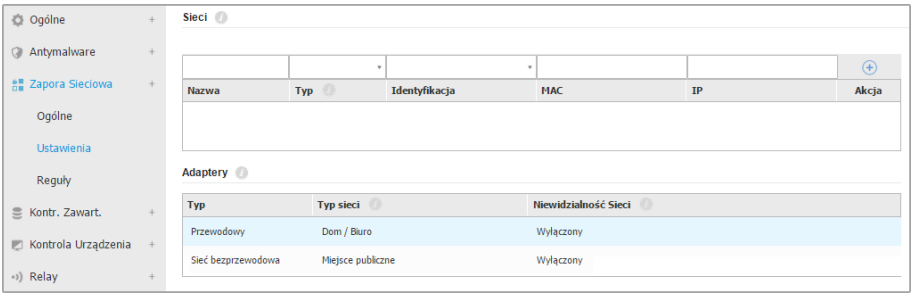
WAŻNE
System Wykrywania Włamań dostępny jest jedynie dla klientów Endpoint Security.

Ustawienia

Zapora automatycznie stosuje profil w oparciu o poziom zaufania. Możesz zachować różne poziomy zaufania dla połączeń sieciowych w zależności od architektury sieci lub typu adaptera stosowanego do łączenia się z siecią. Dla przykładu, jeżeli posiadasz podsieci wewnątrz firmowej sieci, możesz ustawić poziom zaufania dla każdej z podsieci.

Ustawienia są zorganizowane w poniższych tabelach:

- Sieci
- Adaptery



Polityki - Ustawienia Zapory Sieciowej

Ustawienia Sieci

Jeżeli pragniesz by zapora sieciowa zastosowała odmienne profile dla kilku segmentów sieciowych wewnątrz posiadanej firmy, musisz określić zarządzane sieci w tabeli **Sieci**. Wypełnij pola tabeli **Sieci** jak opisano poniżej w dokumencie:

- **Nazwa.** Wprowadź nazwę, po której możesz rozpoznać sieć na liście.
- **Typ.** Wybierz z menu rodzaj profilu przypisanego do sieci.

  Agent ochrony Bitdefender automatycznie stosuje jeden z czterech profili sieciowych dla każdej wykrytego połączenia sieciowego na punkcie końcowym, aby zdefiniować opcje podstawowego filtrowania ruchu. Typy profili:

  - **Zaufana** sieć. Wyłącza Zaporę sieciową dla odpowiedniego urządzenia.
  - Sieć **domowa/biurowa**. Pozwala na ruch pomiędzy komputerami w sieci lokalnej, podczas gdy pozostały ruch był filtrowany.
  - Sieć **publiczna**. Cały ruch jest filtrowany.
  - **Nie Zaufana** sieć. Kompletnie blokuje ruch sieciowy i Internet przy pomocy odpowiednich adapterów.
- **Identyfikacja.** Wybierz z meny metodę w jaki sposób sieć będzie identyfikować się agent bezpieczeństwa Bitdefender. Sieci mogą być zidentyfikowane przez trzy metody: **DNS**, **Brama Sieciowa** i **Sieć**.
  - **DNS**: identyfikuje punkty końcowe wykorzystując określony DNS.

- **Brama**: identyfikuje wszystkie punkty końcowe komunikując je przy pomocy określonej bramy.
- **Sieć**: identyfikuje wszystkie punkty końcowe z określonego segmentu sieciowego, definiując je określonym adresem.

- **MAC**. Użyj tego pola aby określić adres MAC serwera DNS lub bramy, która nakłada ograniczanie na sieć, zależnie od wybranej metody identyfikacyjnej.

  Musisz wprowadzić adres MAC w formacie szesnastkowym, oddzielanych myślnikami (-) lub dwukropkami (:). Dla przykładu, oba zapisy `00-50-56-84-32-2b` oraz `00:50:56:84:32:2b` są prawidłowymi adresami.

- **IP.** Użyj tego pola żeby zdefiniować konkretny adres IP w sieci. Formaty IP zależą od metod identyfikacji jak następuje:
  - **Sieć.** Wprowadź numer sieciowy w formacie CIDR. Dla przykładu, `192.168.1.0/24`, gdzie `192.168.1.0` jest adresem sieciowy a `/24`jest maską sieciową.
  - **Brama.**Wprowadź adres IP bramy.
  - **DNS.** Wprowadź adres IP serwera DNS.

Jak zdefiniujesz sieć, naciśnij przycisk **Dodaj** po prawej stronie tabeli aby dodać ją do listy.

Ustawienia Adapterów

Jeżeli sieć, która nie została zdefiniowana w tabeli **Sieci** została wykryta, agent bezpieczeństwa Bitdefender wykryje adaptera sieciowego i zastosuje odpowiedni profil połączenia.

Pola w tabeli **Adaptery** są opisane w poniższy sposób:

- **Typ.** Wyświetl rodzaje adapterów sieciowych. Agent Bezpieczeństwa Bitdefender może wykryć trzy predefiniowane typy adapterów: **Przewodowe**, **Bezprzewodowe** i **Wirtualne** (Prywatna Wirtualna Sieć).
- **Typ sieci.** Opis profil sieci przypisany do konkretnych rodzajów adapterów. Profile sieciowe są opisane w sekcji ustawień sieciowych. Naciskając na pole rodzaju sieci możesz zmienić ustawienia.

  Jeżeli wybierzesz **Pozwól Windowsowi decydować**, dla nowego wykrycia sieciowego po zastosowaniu polityki, agent bezpieczeństwa Bitdefender stosuje

profil dla zapory sieciowej bazujące na klasyfikacji sieciowej Windows, ignorując ustawienia z tabeli **Adaptery**.

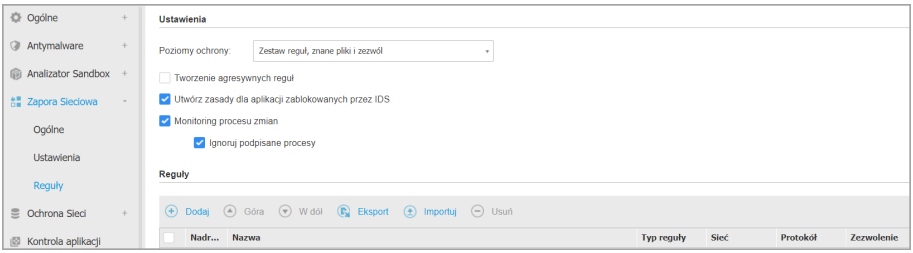
Jeśli wykrywanie oparte na Menadżerze Sieci Windows nie powiedzie się, zostanie podjęta próba wykrywania podstawowego. Profil ogólny użyty jest w przypadkach uważania profilu sieciowego za **Publiczny** a jego ustawienia ukrywania się są **Włączone**.

Gdy punkt końcowy dołączony do usługi Active Directory łączy się z domeną, profil zapory jest automatycznie ustawiony na **Dom/Biuro**, a ustawienia ukrywania są ustawione na **Zdalne** . Jeżeli komputer nie jest w domenie, warunek ten nie ma zastosowania.

- **Wyszukiwanie sieci.** Ukrywa komputer przed złośliwym oprogramowaniem i hakerami w sieci lub Internecie. W razie potrzeby skonfiguruj widoczność komputera w sieci, dla każdego typu adaptera, wybierając jedną z następujących opcji:
  - **Tak.** Każdy w sieci lokalnej i Internecie może pingować i wykryć komputer.
  - **Nie.** Komputer jest niewidoczny w sieci lokalnej i Internecie.
  - **Zdalne.** Komputer nie może być wykryty z internetu. Każdy w sieci lokalnej może pingować i wykryć komputer.

Reguły

W tej sekcji możesz skonfigurować dostęp do sieci aplikacji i reguły ruchu danych egzekwowane przez zaporę. Należy pamiętać, że dostępne ustawienia mają zastosowanie tylko do **Dom/Praca** i **Publiczne** Profile.



Polityki Komputerów i Maszyn Wirtualnych - Ustawienia Zasad Zapory Sieciowej

Ustawienia

Możesz skonfigurować następujące ustawienia:

- **Poziomy ochrony.** Wybrany poziom ochrony określa logikę procesów decyzyjnych zapory sieciowej podczas żądania dostępu aplikacji do usług sieciowych i internetowych. Dostępne są następujące opcje:

  Zestaw reguł i zezwól
  Zastosuj istniejące reguły zapory sieciowej i automatycznie zezwól na wszystkie inne próby połączeń. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

  Zestaw reguł i pytaj
  Zastosuj istniejące reguły zapory sieciowej i powiadom użytkownika o działaniu dla wszystkich innych prób połączeń. Zostanie wyświetlone okno alertu na ekranie użytkownika ze szczegółowymi informacjami o próbie nieznanego połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

  Zestaw reguł i zablokuj
  Zastosuj istniejące reguły zapory sieciowej i automatycznie zabroń wszystkich innych prób połączeń. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

  Zestaw reguł, znane pliki i zezwól
  Zastosuj istniejące reguły zapory sieciowej, automatycznie dopuść próby połączeń, stworzone przez znane aplikacje i automatycznie dopuść wszystkie inne nieznane próby połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

  Zestaw reguł, znane pliki i pytaj
  Zastosuj istniejące reguły zapory sieciowej, automatycznie dopuść próby połączeń, stworzone przez znane aplikacje i powiadom użytkownika o działaniu dla wszystkich innych prób połączenia. Zostanie wyświetlone okno alertu na ekranie użytkownika ze szczegółowymi informacjami o próbie nieznanego połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

  Zestaw reguł, znane pliki i zablokuj
  Zastosuj istniejące reguły zapory sieciowej, automatycznie dopuść próby połączeń, stworzone przez znane aplikacje i automatycznie odmów dostępu

wszystkim innym nieznanym próbom połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

Notatka
Znane pliki należą do dużej kolekcji bezpiecznych, zaufanych aplikacji, które są opracowane i utrzymywane w sposób ciągły przez Bitdefender.

- **Tworzenie agresywnych reguł.** Przy tej opcji zaznaczonej, zapora sieciowa stworzy reguły dla każdego procesu otwierającego aplikacje wymagającą dostępu do sieci lub Internetu.
- **Utwórz zasady dla aplikacji zablokowanych przez IDS.** Wybierając tę opcję, zapora sieciowa automatycznie utworzy zasadę **Odmowa** za każdym razem jak System wykrycia włamań blokuje aplikacje.
- **Monitoruj zmiany procesów.** Wybierz tę opcję, jeśli chcesz, aby program sprawdzał, czy od czasu dodania reguły kontrolującej dostęp do Internetu żadna aplikacja łącząca się z Internetem nie została zmieniona. Jeżeli aplikacja zostanie zmieniona nowa reguła zostanie stworzona zgodnie z istniejącym poziomem ochrony.

Notatka
Zazwyczaj zmiany w aplikacjach powstają na skutek aktualizacji. Istnieje jednak możliwość, że zmiany zostaną dokonane przez aplikacje będące oprogramowaniem złośliwym, w celu zainfekowania komputera lokalnego i innych komputerów pracujących sieci.

Podpisane aplikacje powinny być zaufane i mieć wyższy poziom zabezpieczeń. Możesz wybrać **Ignoruj podpisane procesy** aby automatycznie zezwalać na łączenie się z Internetem zmienionych podpisanych aplikacji.

Reguły

Tabela reguł zawiera reguły istniejącej zapory sieciowej, dostarczając ważnych informacji na temat każdej z nich:

- Odnosi się do nazwy reguły lub aplikacji.
- Protokół, którego dotyczy dana reguła.
- Działanie reguły (dopuszczanie lub blokowanie pakietów).
- Działania jakie możesz podjąć na regule.

- Priorytet reguły.

> **Notatka**
> Takie są reguły zapory wyraźnie wymuszone przez politykę. Dodatkowe przepisy mogą być skonfigurowane na komputerach w wyniku stosowania ustawień zapory.

Liczba domyślnych reguł zapory sieciowej pomaga łatwo zezwolić lub zabronić dostępu dla popularnych rodzajów ruchu. Wybierz wymaganą opcję z menu **Pozwolenie**.

Przychodzący ICMP / ICMPv6
Zezwól lub odmów ICMP/ ICMPv6. Wiadomości ICMP są często używane przez hakerów do ataków na sieci komputerowe. Domyślnie ten typ ruchu będzie dozwolony.

Przychodzące połączenia zdalnego pulpitu
Zezwól lub zabroń innym komputerom łączyć się z pulpitem zdalnym. Domyślnie ten typ ruchu będzie dozwolony.

Wysyłanie wiadomości e-mail
Zezwól na lub zablokuj wysyłanie wiadomości e-mail przez SMTP. Domyślnie ten typ ruchu będzie dozwolony.

Przeglądanie internetu HTTP
Zezwól na przeglądanie lub zabroń przeglądania stron przez HTTP. Domyślnie ten typ ruchu będzie dozwolony.

Drukowanie Sieciowe
Zezwól lub zabroń dostępy do drukarek w innym lokalnym obszarze sieci. Domyślnie ten typ ruchu będzie zabroniony.

Ruch HTTP / FTP związany z Eksploratorem Windows
Zezwól lub zablokuj ruch HTTP i FTP związany z Eksploratorem Windows. Domyślnie ten typ ruchu będzie zabroniony.

Oprócz domyślnych reguł, można utworzyć dodatkowe reguły zapory dla innych aplikacji zainstalowanych na punktach końcowych. Ta konfiguracja jest zarezerwowana dla administratorów z dużą wiedzą na temat sieci.

Aby utworzyć i skonfigurować nową zasadę, kliknij przycisk ⊕ **Dodaj** z górnej strony tabeli. Zapoznaj się z następujące tematy w celu uzyskania większej ilości informacji.

Aby usunąć zasadę z listy, wybierz ją i kliknij przycisk ⊖ **Kasuj** z górnej strony tabeli.

Notatka
Nie można ani usunąć, ani zmodyfikować domyślnej reguły zapory.

Konfigurowanie niestandardowych reguł

Możesz skonfigurować dwa rodzaje reguł zapory sieciowej:

- **Aplikacja bazuje na regułach.** Takie zasady stosują się do konkretnego oprogramowania znalezionego na komputerach klienckich.
- **Połączenie bazuje na regułach.** Takie zasady stosują się do dowolnej aplikacji lub usługi przy użyciu określonego połączenia.

Aby stworzyć i skonfigurować nową regułę, naciśnij przycisk ⊕ **Dodaj** z górnej strony tabeli i wybierz odpowiedni rodzaj reguły z menu. Aby edytować istniejącą regułę, naciśnij nazwę reguły.

Można skonfigurować następujące ustawienia:

- **Nazwa reguły.** Podaj nazwę dla reguły, która będzie na liście reguł w tabeli (na przykład, nazwa aplikacji, której dotyczy reguła).
- **Ścieżka aplikacji** (tylko dla aplikacji bazujących na regułach). Musisz określić ścieżkę do wykluczonych plików aplikacji na docelowych komputerach.
  - Wybierz z menu wcześniej zdefiniowaną lokalizacją j uzupełnij potrzebną ścieżkę. Na przykład, dla aplikacji zainstalowanych w folderze `Program Files`, wybierz `%ProgramFiles%` i uzupełnij ścieżkę dodając backslshs (\) i nazwę foldera aplikacji.
  - Podaj pełną ścieżkę w polu edycji. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.
- **Linia komend** (tylko dla aplikacji bazujących dla reguł). Jeśli chcesz zastosować regułę tylko kiedy określona aplikacja jest uruchomiona przez komendę z interfejsu linii komend Windows, wpisz komendę w polu edycji. W przeciwnym razie pozostaw to pole puste.
- **Aplikacja MD5** (tylko dla aplikacji bazujących na regułach). Jeżeli chcesz regułę do sprawdzenia integracji danych pliku aplikacji bazującej na hash kodzie MD5, podaj go w polu edycji. W innym wypadku pole należy pozostawić puste.

- **Adres lokalny.** Określ lokalny adres IP oraz port, do którego odnosi się dana reguła. Jeśli masz więcej niż jeden adapter sieciowy, możesz odznaczyć pole wyboru **"Dowolny"** i podać konkretny adres IP. Podobnie, aby filtrować połączenia na określonym porcie lub zakresie portów, wyczyść pole wyboru **Dowolny** i wprowadź żądany port lub zakres portów w odpowiednim polu.
- **Adres zdalny.** Określ zdalny adres IP oraz port, do którego odnosi się dana reguła. Aby filtrować ruch w określonym komputerze, odznacz pole **Dowolne** i wpisz jego adres IP.
- **Zastosuj regułę tylko do bezpośrednio połączonych komputerów.** Możesz filtrować dostęp do adresu Mac.
- **Protokół.** Wybierz protokół IP do którego stosowana jest reguła.
  - Jeśli chcesz aby reguła była stosowana dla wszystkich protokołów, zaznacz **"Dowolne"**.
  - Jeśli chcesz zastosować tą regułę do protokołu TCP, wybierz **TCP**.
  - Jeśli chcesz zastosować tę regułę do protokołu UDP, wybierz **UDP**.
  - Jeżeli chcesz regułę do zastosowania określonego protokołu, wybierz protokół z meny **Inne**.

    Notatka

    Numery protokołów IP są przypisane przez organizację Internet Assigned Numbers Authority (IANA). Kompletną listę protokołów IP możesz znaleźć tutaj: http://www.iana.org/assignments/protocol-numbers.

- **Kierunek.** Wybierz kierunek ruchu do którego stosowana jest reguła.

Kierunek	Opis
Wysyłane	Reguła będzie dotyczyła tylko ruchu wychodzącego.
Odbierane	Reguła będzie dotyczyła tylko ruchu przychodzącego.
Oba	Reguła będzie dotyczyła obu kierunków.

- **Wersja IP.** Wybierz wersje IP (IPv4, IPv6 lub dowolną) dla którego ma być stosowana reguła.
- **Sieć.** Wybierz typ sieci, do której stosuje się ta reguła.

- **Zezwolenie.** Wybierz jedno z dostępnych uprawnień:

Zezwolenie	Opis
Zezwól	Podana aplikacja dostanie zezwolenie na dostęp do sieci / internetu pod pewnymi warunkami.
Odmów	Podana aplikacja nie dostanie dostępu do sieci / internetu pod pewnymi warunkami.

Aby dodać regułę, kliknij **Zapisz**.

Dla reguł, które stworzyłeś, użyj strzałek po prawej stronie tabeli aby ustawić priorytet reguł. Reguła z wysokim priorytetem jest bliżej szczytu listy.

Importowanie i Eksportowanie Reguł

Możesz importować i eksportować reguły zapory sieciowej by wykorzystać je w innych firmach lub politykach. Aby eksportować reguły:

1. Kliknij **Eksportuj** w górnej części tabeli reguł.
2. Zapisz plik CSV na swoim komputerze. W zależności od twoich ustawień przeglądarki, plik może być pobierany automatycznie lub zostaniesz poproszony, aby go zapisać do lokalizacji.

WAŻNE

- Każdy wiersz w pliku CSV odpowiada pojedynczej regule i ma wiele pól.
- Pozycja reguł zapory sieciowej w pliku CSV określa ich priorytet. Możesz zmienić priorytet reguły przenosząc cały wiersz.

Dla domyślnego zestawu reguł możesz zmodyfikować następujące elementy:

- **Priorytet** : Ustaw priorytet reguły w dowolnej kolejności, przesuwając wiersz CSV.
- **Uprawnienia**: Modyfikuj pole `set.Permission` używając dostępnych uprawnień:
  - 1 dla **Zezwól**
  - 2 dla **Odmów**

Inne poprawki są odrzucone podczas importu.

Dla niestandardowych reguł zapory, wartości wszystkich pól można konfigurować w następujący sposób:

Pole	Nazwa i Wartość
`ruleType`	**Typ reguły**: 1 dla **Reguła Aplikacji** 2 dla **Reguła połączenia**
`typ`	Wartość dla tego pola jest opcjonalna.
`details.name`	**Nazwa reguły**
`details.applictionPath`	**Ścieżka aplikacji** (tylko dla aplikacji bazujących na regułach)
`details.commandLine`	**Linia komend** (tylko dla aplikacji bazujących dla reguł)
`details.applicationMd5`	**MD5 Aplikacji** (tylko dla aplikacji bazujących na regułach)
`settings.protocol`	**Protokół** 1 dla **Dowolny** 2 dla **TCP** 3 dla **UDP** 4 dla **Inny**
`settings.customProtocol`	Wymagane tylko gdy **Protokół** ustawiony jest na **Inny**. Dla konkretnych wartości, rozważ tę stronę. Wartości 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143 nie są obsługiwane.
`settings.direction`	**Kierunek**: 1 dla **Oba**

Pole	Nazwa i Wartość
	2 dla **Przychodzący** 3 dla **Wychodzący**
`settings.ipVersion`	**Wersja IP**: 1 dla **Dowolny** 2 dla **IPv4** 3 dla **IPv6**
`settings.localAddress.any`	**Adres lokalny** jest ustawiony jako **Dowolny**: 1 dla Prawda 0 lub pusty dla fałsz
`settings.localAddress.ipMask`	**Lokalny Adres** ustawiony jest jako **IP lub IP/Maska**
`settings.remoteAddress.portRange`	**Zdalny Adres** jest ustawiony jako **Port lub zakres portów**
`settings.directlyConnected.enable`	**Zastosuj regułę tylko do bezpośrednio połączonych komputerów**: 1 dla włączony 0 lub pusty dla wyłączony
`settings.directlyConnected.remoteMac`	**Zastosuj regułę tylko dla bezpośrednio połączonych komputerów** z filtrowaniem **Adresu MAC**
`permission.home`	**Sieć** dla której jest zastosowana reguła to **Dom/Biuro**: 1 dla Prawda 0 dla pusty lub Fałsz
`permission.public`	**Sieć** dla której zastosowana jest reguła jest **Publiczna**: 1 dla Prawda

Pole	Nazwa i Wartość
	0 dla pusty lub Fałsz
`permission.setPermission`	Dostępne uprawnienia: 1 dla **Zezwól** 2 dla **Odmów**

Aby importować reguły:

1. Kliknij **Importuj** w górnej części tabeli Reguły.
2. W nowym oknie kliknij **Dodaj** i zaznacz plik CSV.
3. Kliknij **Zapisz**. Tabela jest zapełniona poprawnymi regułami.

7.2.6. Ochrona sieci

Sekcja Ochrona Sieci służy do konfigurowania preferencji dotyczących filtrowania zawartości, ochrony danych dotyczących aktywności użytkownika, w tym przeglądania stron internetowych, poczty e-mail i aplikacji, oraz wykrywania technik ataków sieciowych, które próbują uzyskać dostęp do określonych punktów końcowych. Możesz zastrzec lub zezwolić na dostęp do sieci aplikacji, skonfigurować skanowanie ruchu, antyphishing i reguły ochrony danych.

Należy pamiętać, że skonfigurowane ustawienia Ochrony sieci będą miały zastosowanie do wszystkich użytkowników logujących się na komputerach docelowych.

Ustawienia są zorganizowane w poniższych sekcjach:

- Ogólne
- Kontrola Zawartości
- Ochrona sieciowa
- Ataki Sieciowe

Notatka

- Moduł Kontroli Zawartości jest dostępny dla:
  - Windows dla stacji roboczych
  - macOS
- Moduł Network Attack Defense jest dostępny dla:
  - Windows dla stacji roboczych

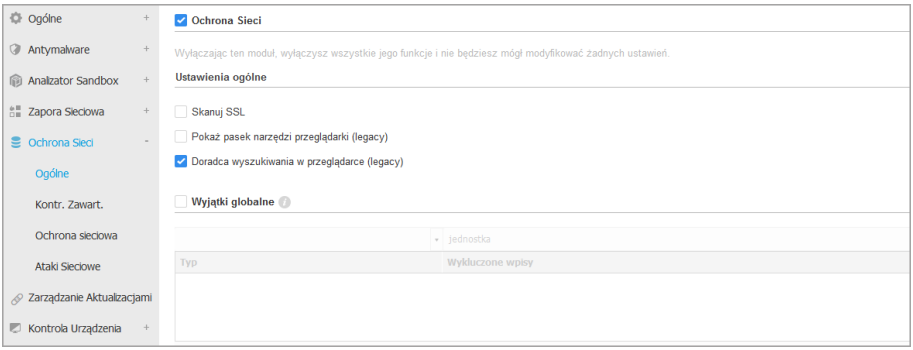
WAŻNE
W przypadku systemu MacOS Kontrola Zawatości opiera się na rozszerzeniu jądra. Instalacja rozszerzenia jądra wymaga twojej zgody na macOS High Sierra (10.13) i starszych. System powiadamia użytkownika, że rozszerzenie systemu z Bitdefender zostało zablokowane. Użytkownik może na to zezwolić na to z ustawień **Bezpieczeństwo & Prywatność**. Dopóki użytkownik nie zaakceptuje rozszerzenia systemu Bitdefender, moduł nie będą działał, a interfejs użytkownika Endpoint Security for Mac pokaże krytyczny problem zachęcający użytkownika do zatwierdzenia.
Aby wyeliminować interwencję użytkownika, możesz wstępnie zatwierdzić rozszerzenie jądra Bitdefender, dodając je do białej listy za pomocą narzędzia do zarządzania urządzeniami przenośnymi. Aby uzyskać szczegółowe informacje na temat rozszerzeń jądra Bitdefender, zapoznaj się z tym artykułem KB.

Ogólne

Na tej stronie możesz skonfigurować takie opcje jak włączenia lub wyłączenie funkcjonalności i konfiguracja wykluczeń.

Ustawienia są zorganizowane w poniższych sekcjach:

- Ustawienia ogólne
- Wyjątki globalne



Polityki Komputerów i Maszyn Wirtualnych - Ochrona Sieci - Ogólne

Ustawienia ogólne

- **Skanuj SSL**. Wybierz tę opcję jeżeli chcesz aby ruch sieciowy Secure Sockets Layer (SSL) był kontrolowany przez moduły ochrony agenta bezpieczeństwaBitdefender.

- **Pokaż pasek narzędzi przeglądarki (legacy)**. Toolbar Bitdefender informuje użytkowników o ocenie stron internetowych, które są przeglądane. Pasek narzędzi produktu Bitdefender nie jest Twoim typowym paskiem narzędzi przeglądarki. Jedynym elementem dodanym do przeglądarki jest mały element przeciągający na górze każdej wyświetlanej strony. Kliknięcie elementu przeciągającego otwiera pasek narzędzi.

  W zależności od tego, jak Bitdefender zaklasyfikuje stronę, jedna z wymienionych ocen pojawi się po lewej stronie paska narzędzi:

  – Wiadomość "Ta strona nie jest bezpieczna" pojawia się na czerwonym tle.

  – Wiadomość "Należy zachować ostrożność" pojawia się na pomarańczowym tle.

  – Wiadomość "Strona jest bezpieczna" pojawia się na zielonym tle.

  Notatka

  – Ta opcja nie jest dostępna dla systemu MacOS.

  – Ta opcja jest usuwana z systemu Windows, zaczynając od nowych instalacji Bitdefender Endpoint Security Tools w wersji 6.6.5.82.

- **Doradca wyszukiwania w przeglądarce (legacy).** Doradca wyszukiwania ocenia rezultaty wyszukiwania w Google, Bing i Yahoo!, a także linki z serwisów Facebook i Twitter poprzez umieszczenie ikony przy każdym rezultacie wyszukiwania: Używane ikony i ich znaczenie:

  Nie powinieneś wchodzić na tę stronę.
  Ta strona może zawierać niebezpieczną treść. Należy zachować ostrożność, jeśli zdecydujesz się ją odwiedzić.
  Ta strona jest bezpieczna.

  Notatka

  – Ta opcja nie jest dostępna dla systemu MacOS.

  – Ta opcja jest usuwana z systemu Windows, zaczynając od nowych instalacji Bitdefender Endpoint Security Tools w wersji 6.6.5.82.

Wyjątki globalne

Możesz wybrać, żeby ominąć ruch związany ze skanowaniem w poszukiwaniu malware gdy są włączone opcje **Ochrona Sieci**

Notatka
Wyjątki zastosowane są do **Skanowanie Ruchu** i **Antyphishing** w sekcji **Ochrona sieci** i do **Network Attack Defense** w sekcji **Ataki Sieciowe**. Wyjątki **Ochrona Danych** są konfigurowane osobno w sekcji **Kontrola Zawartości**.

Aby zdefiniować wykluczenie:

1. Wybierz rodzaje wyjątków z menu.
2. Zależnie od rodzaju wyjątku zdefiniuj ruch jednostek wykluczonych ze skanowania według poniższych:
   - **IP/maska**. Wprowadź adres IP lub maskę dla której nie chcesz skanować ruchu przychodzącego/wychodzącego, wliczając techniki ataków sieciowych.
   - **URL**. Wyklucz ze skanowania określone adresy sieciowe. Weź pod uwagę, że wykluczenia ze skanowania oparte na adresach URL mają zastosowanie w przypadku połączeń HTTP i HTTPS w inny sposób, jak wyjaśniono poniżej.

     Można zdefiniować wykluczanie skanowania oparte na adresach URL w następujący sposób:

     – Podaj adres URL, taki jak `www.example.com/example.html`
       - W przypadku połączeń HTTP tylko określony adres URL jest wykluczony ze skanowania.
       - W przypadku połączeń HTTPS dodanie określonego adresu URL wyklucza całą domenę i jej dowolne subdomeny. Dlatego w tym przypadku można bezpośrednio określić domenę, która ma zostać wykluczona ze skanowania.

     – Użyj symboli wieloznacznych do zdefiniowania wzorców adresów internetowych (tylko dla połączeń HTTP).

       WAŻNE
       Wyjątki z użyciem symboli wieloznacznych nie działają w przypadku połączeń HTTPS.

       Możesz użyć następujących symboli wieloznacznych:

- Gwiazdka (*) zastępuje zero lub więcej znaków.
- Znak zapytania (?) zastępuje dokładnie jeden znak. Możesz użyć kilku znaków zapytania aby zdefiniować każdą kombinacje określonej liczby znaków. Na przykład, ??? zastępuje każdą kombinację dokładnie 3 znaków.

W poniższej tabeli, znajdziesz znaleźć kilka próbek składni dla określonych adresów (URL).

Składnia	Wyjątąk stosowania
www.example*	Dowolny adres URL zaczynający się od www.example (niezależnie od rozszerzenia domeny). Wyjątki nie zostaną zastosowane dla subdomen określonych stron, takich jak subdomain.example.com.
*example.com	Dowolny adres URL kończący się example.com , w tym jego subdomeny.
example.com	Dowolny URL zawierający podany ciąg.
*.com	Dowolna strona zawierająca rozszerzenie domeny .com, w tym ich subdomeny. Użyj tej składni, aby wykluczyć ze skanowania całe domeny na najwyższym poziomie.
www.example?.com	Dowolny adres internetowy rozpoczynający się od www.example?.com, gdzie ? może być zastąpiony dowolnym znakiem. Takie strony internetowe mogą zawierać: www.example1.com lub www.exampleA.com .

Notatka
Możesz użyć adresów URL zależnych od protokołu.

- **aplikacja**. Wyklucza ze skanowania określony proces lub aplikację. Aby zdefiniować wyjątki aplikacji skanowania:
  - Wprowadź pełną ścieżkę aplikacji. Na przykład, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Użyj zmiennych środowiskowych do określenia ścieżki aplikacji. Na przykład: `%programfiles%\Internet Explorer\iexplore.exe`
  - Użyj symboli wieloznacznych, aby określić pewien wzorzec nazw pasujący do aplikacji. Na przykład:
    - `c*.exe` pasuje do wszystkich aplikacji zaczynających się na "c" (chrome.exe).
    - `??????.exe` pasuje do wszystkich aplikacji, których nazwa zawiera cześć znaków (chrome.exe, safari.exe, etc.).
    - `[^c]*.exe` pasuje do wszystkich aplikacji, pomijając te rozpoczynające się na "c".
    - `[^ci]*.exe` pasuje do wszystkich aplikacji, pomijając te rozpoczynające się na "c" lub "i".

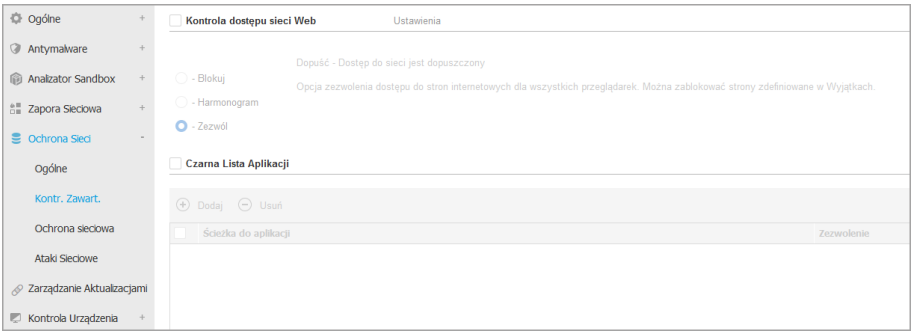
3. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli.

Aby usunąć spis z listy, kliknij odpowiadający mu przycisk ⊗ **Usuń**.

Kontrola Zawartości

Ustawienia Kontroli Zawartości są umieszczone w następujących sekcjach:

- Kontrola dostępu sieci Web
- Czarna Lista Aplikacji
- Ochrona danych



Kontrola dostępu sieci Web

Kontrola dostępu do sieci Web pomaga umożliwiać lub blokować dostęp użytkownikom lub aplikacjom w określonych czasowo przedziałach czasowych.

Strony www blokowane przez kontrolę stron www nie wyświetlają się w przeglądarce. Zamiast tego wyświetlana jest domyślna strona www informująca użytkownika, że dana strona została zablokowana przez kontrolę dostępu stron www.

Użyj przełącznika do zmiany stanu **Kontroli Dostępu do Sieci Web** na włączony lub wyłączony.

Masz trzy opcje konfiguracyjne:

- Wybierz **Pozwól** aby zawsze udzielić dostępu do sieci.
- Wybierz **blokuj** aby nigdy nie udzielać dostępu do sieci.
- Wybierz **Harmonogram** aby umożliwić ograniczenia czasowe w dostępie do stron internetowych w szczegółowym harmonogramie.

Jeżeli zamierzasz dopuścić lub zablokować dostęp do strony internetowej, możesz zdefiniować wyjątki do tych działań dla całych kategorii internetowych lub tylko dla określonych adresów internetowych. Naciśnij **Ustawienia** aby skonfigurować twój harmonogram dostępu do sieci i wyjątki według poniższych zaleceń:

Harmonogram

Aby ograniczyć dostęp do Internetu do określonych przedziałów czasowych dnia na przestrzeni tygodnia:

1. Wybierz z siatki przedziały czasowe, w których chcesz aby dostęp do internetu był zablokowany.

Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu. Naciśnij ponownie na komórkę, aby odwrócić zaznaczenie.

Aby rozpocząć nowe zaznaczenie, naciśnij **Zezwól wszystkie** lub **Zablokuj wszystkie**, w zależności od rodzaju ograniczenia, które chcesz wprowadzić.

2. Kliknij **Zapisz**.

Notatka
Agent Bezpieczeństwa Bitdefender będzie wykonywał aktualizacje co godzinę, bez względu na to czy dostęp do Internetu został zablokowany.

Kategorie

Filtr kategorii sieciowych dynamicznie filtruje dostęp do stron internetowych w oparciu o ich zawartość. Możesz użyć Filtrów Kategorii Web, aby definiować wyjątki dla wybranych działań Kontroli Dostępu Sieci (Zezwalaj lub Blokuj) dla całej kategorii stron internetowych (takich jak gry, treści dla dorosłych lub sieci on-line).

Aby skonfigurować filtr kategorii sieciowych:

1. Włącz **Filtr Kategorii Sieci Web**.
2. W celu szybkiej kontynuacji, naciśnij jeden ze zdefiniowanych profili (**Agresywny**, **Normalny** lub **Tolerancyjny**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór. Możesz zaobserwować zdefiniowane wcześniej działania dostępne dla każdej dostępnej kategorii poprzez rozwinięcie sekcji **Zasady Webowe** umiejscowione poniżej.
3. Jeśli nie jesteś zadowolony z ustawień domyślnych, możesz zdefiniować niestandardowe filtry.
   a. Zaznacz **Własny**.
   b. Kliknij **Zasady Webowe** w celu rozwinięcia odpowiedniej sekcji.
   c. Znajdź kategorię, którą chcesz w na liście i wybierz pożądane działanie z menu. Aby uzyskać więcej informacji na temat dostępnych kategorii witryn, zapoznaj się z tym artykułem KB.
4. Wybierz opcję **Traktuj Kategorie Internetowe jako wyjątki w Dostępie do Sieci** jeżeli chcesz zignorować istniejące ustawienia dostępu do sieci i zatwierdzić tylko Filtr Kategorii Sieciowych.

5. Standardowa wiadomość wyświetlona dla użytkownika, który wchodzi na zastrzeżoną stronę zawiera kategorie odpowiednią dla strony. Odznacz opcję **Pokaż szczegółowe alerty na kliencie**, jeśli chcesz ukryć te informacje przed użytkownikiem.

   Notatka
   Ta opcja nie jest dostępna dla systemu MacOS.

6. Kliknij **Zapisz**.

Notatka

- **Zezwól** zezwolenie na określenie kategorii sieciowej jest również stosowane do konta w przedziałach czasu, w których dostęp do sieci jest zablokowany przez kontrolę dostępu sieciowego.
- **Zezwól** pozwala na pracę tylko kiedy dostęp do sieci jest zablokowany przez Kontrolę Dostępu Sieciowego, kiedy zezwolenie **Blokuj** pozwala na pracę tylko wtedy, kiedy dostęp do sieci jest dopuszczony przez Kontrolę Dostępu Sieciowego.
- Możesz zastąpić uprawnienia kategorii dla indywidualnych adresów sieciowych przez dodawanie ich z przeciwnymi zezwoleniami w **Kontrola Dostępu Sieci > Ustawienia > Wyjątki**. Na przykład, jeżeli adres sieciowy jest zablokowany przez Filtr Kategorii Sieciowych, dodaj regułę sieci dla adresów z zezwoleniami ustawionymi na **Zezwól**.

Wykluczenia

Możesz również zdefiniować reguły sieci aby jawnie blokować lub zezwalać określone adresy sieciowe, zastępując istniejące ustawienia Kontroli Dostępu Sieciowego. Użytkownicy będą w stanie, na przykład, uzyskać dostęp do odpowiedniej strony również podczas przeglądanie stron internetowych są zablokowane przez Kontrolę Dostępu Sieciowego.

Aby stworzyć regułę sieci:

1. Włącz opcję **Użyj Wykluczeń**.
2. Podaj adresy jakie chcesz dopuścić albo zablokować w polu **Adresy Sieciowe**.
3. Wybierz **Zezwól** lub **Zablokuj** z menu **Pozwolenia**.
4. Naciśnij przycisk ⊕ **Dodaj** po prawej stronie tabeli aby dodać adres do listy wyjątków.

5. Kliknij **Zapisz**.

Aby edytować regułę sieci:

1. Naciśnij na adres internetowy jaki chcesz edytować.
2. Zmień istniejący URL.
3. Kliknij **Zapisz**.

Aby usunąć zasady z listy, kliknij odpowiedni przycisk ⊗ **Usuń**.

Czarna Lista Aplikacji

W tej sekcji można skonfigurować aplikację czarnych list, dzięki której można całkowicie zablokować lub ograniczyć dostęp użytkowników do aplikacji na swoich komputerach. W ten sposób można blokować gry, nośniki oraz komunikatory, a także inne rodzaje oprogramowania zwykłego oraz złośliwego.

Aby skonfigurować aplikację czarna lista:

1. Włącz opcję **aplikacja czarna lista**.
2. Określ aplikacje do których chcesz ograniczyć dostęp. Aby ograniczyć dostęp do aplikacji:
   a. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlono okno konfiguracji.
   b. Musisz określić ścieżkę do wykluczonych plików aplikacji na docelowych komputerach. Są na to dwa sposoby:
      - Wybierz z menu wcześniej zdefiniowaną lokalizacją i uzupełnij potrzebną ścieżkę w polu edycji. Na przykład, dla aplikacji zainstalowanych w folderze `Program Files`, wybierz `%ProgramFiles%` i uzupełnij ścieżkę dodając backslshs (\) i nazwę foldera aplikacji.
      - Podaj pełną ścieżkę w polu edycji. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.
   c. **dostęp do harmonogramu**. Harmonogram dostępu do aplikacji podczas określonego czasu w trakcie dnia co tydzień.
      - Wybierz z siatki przedziały czasowe, w których chcesz aby dostęp do aplikacji był zablokowany. Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu. Naciśnij ponownie na komórkę, aby odwrócić zaznaczenie.

- Aby rozpocząć nowe zaznaczenie, naciśnij **Zezwól wszystkie** lub **Zablokuj wszystkie**, w zależności od rodzaju ograniczenia, które chcesz wprowadzić.
- Kliknij **Zapisz**. Do listy zostanie dodana nowa reguła.

Aby usunąć zasadę z listy, wybierz ją i kliknij przycisk ⊗ **Kasuj** z górnej strony tabeli. Aby edytować istniejącą regułę, kliknij ją aby otworzyć okno konfiguracyjne.

Ochrona danych

Ochrona danych przed nieautoryzowanym ujawnieniem danych wrażliwych na podstawie reguł określonych przez administratora.

Notatka
Ta funkja nie jest dostępna dla systemu MacOS.

Możesz utworzyć reguły aby chronić dowolne osobiste lub poufne informacje, takie jak:

- Osobiste informacje klienta
- Szczegóły nazwy i klucza dla wdrożonych produktów i technologii.
- Dane kontaktowe kierownictwa firmy

Chronione infomacje mogą zawierać nawzy, numery telefony, kart kredytowych i kont bankowych itd.

Opierając się na regułach ochrony danych stwórz skanowanie Bitdefender Endpoint Security Tools ruchu sieciowego i poczty wychodzącej, zawierających określone ciągi znaków (np. numery kart kredytowych). Jeżeli znajdzie dopasowanie, strona www lub wiadomość e-mail zostaną zablokowane, aby zapobiec wysłaniu chronionych danych. Użytkownik jest natychmiast informowany o podjętym działaniu przez Bitdefender Endpoint Security Tools przez powiadomienie na stronie lub e-mail.

Aby skonfigurować ochronę danych:

1. Użyj pola wyboru, żeby zaznaczyć Ochronę Danych.
2. Utwórz reguły ochrony danych dla wszystkich wrażliwych danych jakie chcesz ochronić. Aby stworzyć regułę:
   a. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlono okno konfiguracji.

b. Podaj nazwę pod którą reguła będzie przypisana w tabeli reguł. Wybierz sugestywną nazwę, po której administratorzy będą mogli w łatwy sposób zidentyfikować do czego odnosi się ta reguła.

c. Wybierz typ danych, które chcesz chronić.

d. Podaj dane jakie chcesz ochronić (na przykład, numer telefonu firmy wykonawczej lub wewnętrzną nazwę nowego produktu nad którym pracuje firma). Każda kombinacja słów, liter lub ciągów znaków składających się ze znaków alfanumerycznych i znaków specjalnych (takie jak @,# lub $) jest dopuszczalna.

   Upewnij się, z ewprowadziłeś przynajmniej trzy znaki, aby zapobiec omyłkowemu blokowaniu wiadomości i stron internetowych.

   WAŻNE

   Dostarczane informacje są przechowywane w sposób zaszyfrowany na stacjach końcowych, ale mogą być wyświetlone z poziomu konta Control Center. Dla dodatkowego bezpieczeństwa, nie należy wprowadzać wszystkich danych, które chcesz chronić. W tym przypadku, musisz wyczyścić opcje **Dopasuj całe słowa**.

e. Skonfiguruj opcje skanowania ruchu według uznania:

   - **Skanuj ruch internetowy (HTTP)** - skanuje ruch HTTP (strony WWW) i blokuje wysyłane dane, które pasują do tych zapisanych w regule.
   - **Skanuj ruch e-mail (SMTP)** - skanuje ruch SMTP (wiadomości) i blokuje wszystkie wychodzące wiadomości e-mail, które zawierają podane w regule ciągi znaków.

   Możesz wybrać zastosowanie reguły tylko jeśli zawartość reguły zgadza się z całymi słowami lub jeśli zawartość reguły i jakikolwiek wykryty ciąg znaków są identyczne.

f. Kliknij **Zapisz**. Do listy zostanie dodana nowa reguła.

3. Skonfiguruj wyjątki do zasad ochrony danych, dzięki którym użytkownicy będą mogli wysyłać chronione dane do autoryzowanych stron i odbiorców. Wyjątki mogą być stosowane globalnie (dla wszystkich reguł) lub tylko dla określonych reguł. Aby dodać wyjątek:
   a. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlono okno konfiguracji.

b. Podaj adres sieci lub e-mail na którym użytkownicy są upoważnieni do ujawniania chronionych danych.
c. Wybierz rodzaj wyjątków (strony internetowe lub adres e-mail).
d. Z tabeli **Reguły** wybierz reguły ochrony danych w których zostaną zastosowane wyjątki.
e. Kliknij **Zapisz**. Do listy zostanie dodana nowy nowy wyjątek.

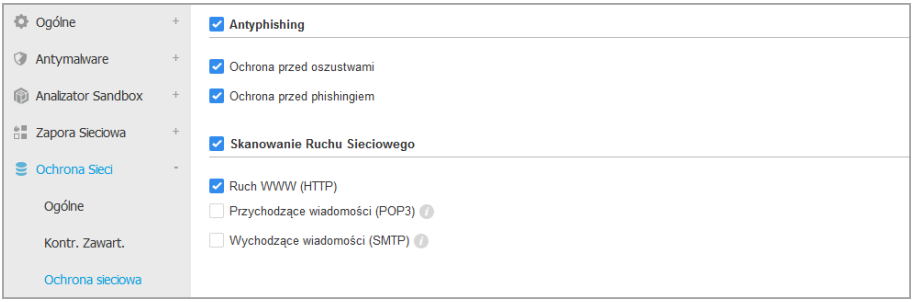
Notatka
Jeżeli e-mail zawierający zablokowane dane jest zaadresowany do wielu odbiorców, to tylko Ci dla których zostały ustawione wyjątki, otrzymają go.

Aby usunąć regułę lub wyjątek z listy, naciśnij przycisk ⊗ **Usuń** po prawej stronie tabeli.

Ochrona sieciowa

Na tej stronie ustawienia są zorganizowane w następujących sekcjach:

- Antyphishing
- Skanowanie Ruchu Sieciowego



Polityki Komputerów i Maszyn Wirtualnych - Ochrona Sieci - Ochrona Sieciowa

Antyphishing

Ochrona Antyphishing automatycznie blokuje znane strony phishingowe aby ustrzec użytkownika przed przypadkowym ujawnieniem prywatnych lub poufnych informacji oszustom internetowym. Zamiast strony phishingu, w przeglądarce zostanie wyświetlona specjalna strona z ostrzeżeniem informująca użytkownika, że wybrana strona jest niebezpieczna.

Zaznacz **Antyphishing** aby aktywować ochronę przed phishingiem. Możliwe jest dalsze dostosowanie Antyphishing przez skonfigurowanie następujących ustawień:

- **Ochrona przed oszustwem**. Wybierz tę opcje jeżeli chcesz rozszerzyć ochronę na inne rodzaje oszustw poza phishingiem. Na przykład, strony internetowe reprezentujące fałszywe firmy, które nie proszą bezpośrednio o informacje prywatne, zamiast tego próbują udawać legalne przedsiębiorstwa i zbierać profity dzięki oszukiwaniu ludzi i przekonywaniu ich do prowadzenia działalności gospodarczej z nimi.
- **Ochrona przed phishingiem**. Zachowaj te opcję wybraną aby ochronić użytkowników przed próbami phishingu.

Jeżeli legalna strona internetowa jest niepoprawnie wykryta jako phishing i zablokowana, możesz dodać ją do białej listy aby zezwolić użytkownikom na dostęp. Na tej liście powinny znajdować się tylko w pełni zaufane strony.

Zarządzaj wyjątkami antyphishing:

1. Przejdź do ustawień **Ogólne** i kliknij **Globalne Wykluczenia**.
2. Podaj adres sieciowy i naciśnij przycisk ⊕ **Dodaj**.

   Jeżeli chcesz wykluczyć całą witrynę, napisz nazwę domeny, na przykład `http://www.website.com`, lub jeżeli chcesz zablokować tylko jedną stronę z witryny podaj jej dokładny adres.

   > **Notatka**
   > Wildcards nie są dopuszczane przy budowaniu adresów ULR.

3. Aby usunąć wyjątek z listy, kliknij odpowiadający mu przycisk ⊗ **Usuń**.
4. Kliknij **Zapisz**.

Skanowanie Ruchu Sieciowego

Przychodzące maile (POP3) i ruch sieciowy są skanowane w czasie rzeczywistym, aby powstrzymać złośliwe oprogramowanie przed zainstalowaniem na punkcie końcowym. Wychodzące wiadomości e-mail (SMTP) są skanowane, aby powstrzymać złośliwe oprogramowanie przed zainfekowaniem pozostałych punktów końcowych. Skanowanie ruchu sieciowego może nieco spowolnić przeglądanie sieci, ale będzie blokować złośliwe oprogramowanie pochodzące z internetu, w tym także przypadkowe pobieranie plików.

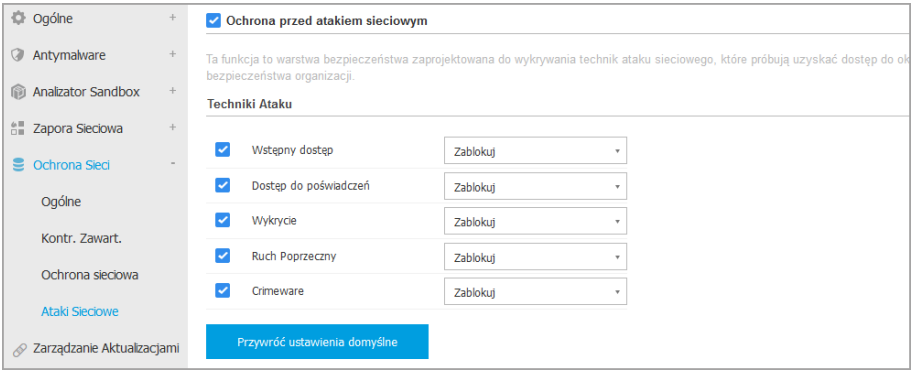
Gdy zostanie znaleziona zainfekowana wiadomość e-mail, jest automatycznie zamieniana z standardową wiadomością e-mail informującą, że oryginalna wiadomość jest zainfekowana. Jeżeli strona internetowa zawiera lub rozprowadza złośliwe oprogramowanie, zostaje automatycznie zablokowana. Specjalna strona z ostrzeżeniem pojawia się aby poinformować użytkownika, że wybrana strona jesd niebezpieczna.

Choć nie jest to zalecane, możesz wyłączyć skanowanie antywirusowe poczty lub ruchu sieciowego, aby zwiększyć wydajność systemu. To nie jest poważne zagrożenie, o ile dostęp na żądanie do plików lokalnych, pozostaje włączony.

Notatka
Opcje **Przychodzące e-maile** i **Wychodzące e-maile** nie są dostępne dla systemu MacOS.

Ataki Sieciowe

Network Attack Defense dostarcza warstwę ochrony bazującą na technologii Bitdefender, która wykrywa i podejmuje akcje przeciwko atakom sieciowym zaprojektowanym do uzyskania dostępu do punktów końcowych poprzez określone techniki takie jak: ataki brute-force, sieciowe exploity i złodzieje haseł.



Polityki Komputerów i Maszyn Wirtualnych - Ochrona Sieci - Ataki sieciowe

Aby skonfigurować Network Attack Defense:

1. Wybierz pole wyboru **Network Attack Defense**, aby włączyć moduł.

2. Zaznacz odpowiednie pola wyboru, aby włączyć ochronę przed każdą kategorią ataku sieciowego. Techniki ataku sieciowego są pogrupowane według bazy wiedzy MITRE ATT&CK następująco:
   - **Wstępny dostęp** - atakujący uzyskuje dostęp do sieci na różne sposoby, w tym przez luki w publicznych serwerach sieciowych. Na przykład: exploity ujawniania informacji, exploity iniekcji SQL, wektory iniekcji drive-by download.
   - **Dostęp do Poświadczeń** - atakujący kradnie poświadczenia takie jak nazwy użytkownika i hasła, aby uzyskać dostęp do systemów. Na przykład: ataki brute-force, nieautoryzowana autoryzacja exploitów, złodzieje haseł.
   - **Wykrycie** - po infiltracji atakujący próbuje uzyskać informacje o systemach i sieci wewnętrznej przed podjęciem decyzji, co dalej. Na przykład: exploity trawersowania przez katalog, exploity trawersowania przez katalog HTTP.
   - **Ruch boczny** - atakujący eksploruje sieć, często przemieszczając się przez wiele systemów, aby znaleźć główny cel. Atakujący może użyć określonych narzędzi do osiągnięcia celu. Na przykład: exploit wstrzykiwania poleceń, exploity Shellshock, exploity podwójnego rozszerzenia.
   - **Crimeware** - ta kategoria obejmuje techniki zaprojektowane w celu automatyzacji cyberprzestępczości. Na przykład, techniki Crimeware to: exploity nuclear, różne oprogramowanie malware, takie jak trojany i boty.
3. Wybierz działania, które chcesz podjąć wobec każdej kategorii technik ataku sieciowego, z następujących opcji:
   a. **Blokuj** - Network Attack Defense zatrzymuje próbę ataku po wykryciu.
   b. **Tylko Raporty** - Network Attack Defense informuje cię o wykrytej próbie ataku, ale nie będzie próbowała jej zatrzymać.

Możesz łatwo przywrócić początkowe ustawienia, klikając przycisk **Przywróć ustawienia domyślne** w dolnej części strony.

Szczegółowe informacje na temat prób ataku sieciowego są dostępne w raporcie Incydenty sieciowe oraz w powiadomieniu o zdarzeniu Incydenty sieciowe.

7.2.7. Zarządzanie Aktualizacjami

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów

Moduł Zarządzania Aktualizacjami uwalnia cię od konieczności aktualizowania punktów końcowych za pomocą najnowszych aktualizacji oprogramowania, automatycznie dystrybuując i instalując aktualizacje dla szerokiej gamy produktów.

Notatka
Możesz sprawdzić listę obsługiwanych dostawców i produktów w tym artykule KB.

Ta sekcja polityki zawiera ustawienia automatycznego wdrażania poprawek. Najpierw skonfigurujesz, jak aktualizacje są pobierane do punktów końcowych, a następnie, które aktualizacje zainstalować i kiedy.

Konfigurowanie Ustawień Pobierania Aktualizaji

Proces rozprowadzanie aktualizacji wykorzystuje serwery buforowania aktualizacji w celu optymalizacji ruchu sieciowego. Punkty końcowe łączą się z tymi serwerami i pobierają aktualizacje za pośrednictwem sieci lokalnej. W celu uzyskania wysokiej dostępności aktualizacji, zaleca się używanie więcej niż jednego serwera.

Aby przypisać Serwery Buforowania Aktualizacji do docelowych punktów końcowych:

1. W sekcji **Ustawienia Pobierania Aktualizacji** kliknij pole w górnej części tabeli. Wyświetlono listę Serwerów Buforowania Aktualizacji.

   Jeśli lista jest pusta, musisz zainstalować rolę Serwera Buforowania Aktualizacji na Przekaźnikach w twojej sieci. Aby uzyskać więcej informacji, zapoznaj się z Instrukcją instalacji.

2. Wybierz serwer z listy.
3. Kliknij przycisk ⊕ **Dodaj** .
4. Jeśli chcesz dodać więcej serwerów, powtórz poprzednie kroki.
5. Użyj strzałek w górę i w dół po prawej stronie tabeli, aby ustalić priorytet serwera. Priorytet zmniejsza się od góry do dołu listy.

   Punkt końcowy żąda aktualizacji od przydzielonych serwerów według ich priorytetu. Punkt końcowy pobiera aktualizację z serwera, na którym znajduje ją jako pierwszy. Serwer, który nie ma żądanej aktualizacji, automatycznie pobierze ją od dostawcy, aby udostępnić ją na przyszłe żądania.

Aby usunąć serwery, których już nie potrzebujesz, kliknij odpowiedni przycisk ⊖ Usuń po prawej stronie tabeli.

Wybierz opcję **Używaj witryn internetowych dostawców jako lokalizacji zastępczej do pobierania aktualizacji**, aby upewnić się, że punkty końcowe otrzymują aktualizacje oprogramowania na wypadek, gdyby serwery buforujące aktualizacje były niedostępne.

Konfigurowanie Skanowania Aktualizacji i Instalacja

GravityZone wykonuje wdrożenie aktualizacji w dwóch niezależnych etapach:

1. Ocena. Kiedy wysyłana jest prośba za pośrednictwem konsoli zarządzania, punkty końcowe skanują brakujące aktualizacje i zgłaszają je.
2. Instalacja. Konsola wysyła agentom listę aktualizacji, które chcesz zainstalować. Punkt końcowy pobiera aktualizacje z Serwera Buforowania Aktualizacji, a następnie instaluje je.

Polityka udostępnia ustawienia automatyzujące te procesy, częściowo lub całkowicie, tak aby były uruchamiane okresowo w oparciu o preferowany harmonogram.

Aby skonfigurować automatyczne skanowanie aktualizacji:

1. Zaznacz pole wyboru **Automatyczne skanowanie aktualizacji**.
2. Użyj opcji planowania aby skonfigurować harmonogram skanowania. Możesz ustawić skanowanie, aby działało codziennie lub w określone dni tygodnia, o określonej godzinie.
3. Wybierz **Inteligentne skanowanie po zainstalowaniu nowej aplikacji/programu**, aby wykryć, kiedy nowa aplikacja została zainstalowana na punkcie końcowym i jakie aktualizacje są dla niej dostępne.

Aby skonfigurować automatyczną instalację aktualizacji:

1. Zaznacz pole wyboru **Zainstaluj aktualizacje automatycznie po skanowaniu**.
2. Wybierz typy aktualizacji do zainstalowania: bezpieczeństwo, inne lub oba.
3. Użyj opcji planowania, aby skonfigurować czas uruchamiania zadań instalacyjnych. Możesz ustawić skanowanie, aby działało natychmiast po zakończeniu skanowania aktualizacji, codziennie lub w określonych dniach tygodnia, o określonej godzinie. Zaleca się instalowanie aktualizacji zabezpieczeń natychmiast po ich wykryciu.

4. Domyślnie wszystkie produkty kwalifikują się do aktualizacji. Jeśli chcesz automatycznie aktualizować tylko zestaw produktów, które uważasz za istotne dla Twojej firmy, wykonaj następujące kroki:
   a. Zaznacz pole wyboru **Konkretny dostawca i produkt**.
   b. Kliknij pole **Dostawca** w górnej części tabeli. Wyświetlana jest lista wszystkich obsługiwanych dostawców.
   c. Przewiń listę i wybierz dostawcę dla produktów, które chcesz zaktualizować.
   d. Kliknij pole **Produkty** w górnej części tabeli. Wyświetlana jest lista wszystkich produktów wybranego dostawcy.
   e. Wybierz produkty, które chcesz zaktualizować.
   f. Kliknij przycisk ⊕ **Dodaj** .
   g. Powtórz poprzednie kroki dla pozostałych dostawców i produktów.

      Jeśli zapomniałeś dodać produkt lub chcesz go usunąć, znajdź sprzedawcę w tabeli, kliknij dwukrotnie pole **Produkty** i wybierz lub odznacz produkt na liście

   Aby usunąć dostawcę ze wszystkimi jego produktami, znajdź go w tabeli i kliknij odpowiedni przycisk ⊖ **Usuń** po prawej stronie tabeli.
5. Z różnych przyczyn punkt końcowy może być w trybie offline, gdy zaplanowana jest instalacja aktualizacji. Wybierz opcję **Jeśli pominięto, uruchom tak szybko, jak to możliwe**, aby zainstalować poprawki natychmiast po tym, gdy punkt końcowy wróci do trybu online.
6. Niektóre aktualizacje, aby zakończyć instalację, mogą wymagać ponownego uruchomienia systemu, . Jeśli chcesz to zrobić ręcznie, wybierz opcję **Odłóż restartowanie**.

WAŻNE
Aby ocena i instalacja zakończyły się powodzeniem na punktach końcowych Windows, należy spełnić następujące wymagania:

- **Zaufane Główne Urzędy Certyfikacji** przechowuje certyfikat **DigiCert Assured ID Root CA**.
- **Pośrednie Urzędy Certyfikujące** obejmują **DigiCert SHA2 Assured ID Code Signing CA**.
- Na punktach końcowych zainstalowane są aktualizacje dla Windows i Windows Server 2008 R2 wspomniane w tym artykule: Microsoft Security Advisory 3033929

7.2.8. Kontrola Aplikacji

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów

Moduł Kontroli Aplikacji dodaje kolejną warstwę ochrony przeciwko wszystkim rodzajom zagrożen malware (ransomware,atakami zero-day, exploitami produktów firm trzecich, trojanami, spyware, rootkitami adware itd.) poprzez blokowanie nieautoryzowanych aplikacji i procesów przed uruchomieniem. Kontrola Aplikacji ogranicza możliwości ataku złośliwego oprogramowania na punkcie końcowym i zapobiega instalacji i działaniu jakichkolwiek niechcianych, niezaufanych lub złośliwych aplikacji.

Kontrola Aplikacji wymusza elastycznośc na politykach, pozwala ci zarządzać aktualizacjami aplikacji z białej listy i zarządzać uprawnieniami.

Kontrola Aplikacji

WAŻNE

- Aby włączyć **Kontrolę Aplikacji** dla twoich obecnie zainstalowanych agentów, uruchom zadanie **Rekonfiguracja klienta** Po zainstalowaniu modułu, można zobaczyć status w oknie **Informacje**.
- Kontrola aplikacji bardzo wpływa na tryb zasilania użytkownika po aktualizacji aplikacji. Na przykład, gdy aplikacja białej listy jest aktualizowana, punkt końcowy przesyła nowe informacje. GravityZone aktualizuje regułę z nowymi wartościami i rozsyła ponownie polityki.

Musisz uruchomić zadanie **Wykrywanie Aplikacji** aby zobaczyć uruchomione aplikacje i procesy w twojej sieci. Aby uzyskać więcej informacji, zapoznaj się z „Wykrywanie Aplikacji” (p. 100). Następnie, możesz zdefiniować reguły Kontroli Aplikacji.

Kontrola Aplikacji działa w dwóch trybach:

- **Tryb Testowy**. Kontrola Aplikacji wykrywa tylko i raportuje aplikacje w Control Center, pozostawiając jest działające jak przedtem. Możesz konfigurować i testować twoje reguły białej listy i polityki, lecz aplikacje nie będą blokowane.
- **Tryb Produkcji**. Kontrola Aplikacji blokuje wszystkie nieznane aplikacje. Procesy systemów operacyjnych Microsoft i Bitdefendera są domyślnie na białej liście. Zdefiniowane aplikacje z białej listy będą dozwolone do uruchomienia. Aby zaktualizować aplikacje z białej listy, musisz zdefiniować aktualizatory. To są wybrane procesy, które mają zezwolenie na edytowanie aplikacji. Aby uzyskać więcej informacji, zapoznaj się z „Magazyn Aplikacji" (p. 192).

Ostrzeżenie

- Aby upewnić się, że dopuszczone aplikacje nie są ograniczone przez Kontrolę Aplikacji, musisz pierw uruchomić Kontrolę Aplikacji w trybie testowym. W taki sposób masz pewność, że reguły Białej Listy i polityki są należycie zdefiniowane.
- Procesy, które już są uruchomione kiedy Kontrola Aplikacji jest ustawiona na **Tryb Produkcji** zostaną zablokowane przy kolejnym restarcie procesu.

Do zarządzania aplikacjami' zezwolenie do uruchomienia:

1. Zaznacz pole wyboru **Kontrola Aplikacji** aby włączyć ten moduł.
2. Zaznacz pole wyboru **Uruchom w Trybie Testowym** aby włączyć lub wyłączyć tryb testowy.

   Notatka

   - W trybie testowym, jesteś powiadamiany jeśli Kontrola Aplikacji zablokuje wybrane aplikacje. Aby uzyskać więcej informacji, odwołaj się do „Rodzaje powiadomień" (p. 485).
   - Powiadomienie **Zablokowane Aplikacje** wyświetli się w obszarze powiadomień, kiedy nowe aplikacje zostaną wykryte i aplikacje z czarnej zostaną zablokowane.

3. Zdefiniuj reguły startowe procesów.

Reguły Startowe Procesów

Kontrola Aplikacji pozwala ci ręcznie autoryzować wybrane aplikacje i procesy, w oparciu o hash pliku wykonywalnego, ścieżkę aplikacji lub signing certificate thumbprint. Możesz też zdefiniować reguły wyjątków.

Notatka
Aby uzyskać niestandardową wartość hasha pliku wykonywalnego lub thumbprint używanego certyfikatu użyj„Narzędzia Kontroli Aplikacji" (p. 519)

Tabela **Reguły Startowe Procesów** informuje cię o istniejących regułach, dostarczających ważnych informacji:

- Priorytet reguły. Reguła z wysokim priorytetem jest bliżej szczytu listy.
- Nazwa i status reguły.
- Aplikacje docelowe i uprawnienie do ich uruchomienia. Cel reprezentuje liczbę warunków, które muszą być spełnione aby reguła została zastosowana, lub liczbę aplikacji lub grup do których reguła ma zastosowanie.

Aby utworzyć proces rozpocznij regułę:

1. Kliknij przycisk ⊕ **Dodaj** górnej części tabeli by otworzyć okno konfiguracyjne.
2. W sekcji **Ogólne** wprowadź **nazwę reguły**.
3. Zaznacz pole wyboru **Włączone** aby aktywować regułę.
4. W sekcji **Cele** określ miejsce reguły:
   - **Specyficzny proces lub procesy**, aby określić proces, który jest dozwolony lub zabroniony przed startem. Możesz autoryzować po ścieżce, hash lub certyfikat. Warunki wewnątrz reguły są dopasowane na podstawie bramki logicznej AND
     - Aby autoryzować aplikację z określonej ścieżki:
       a. Zaznacz **Ścieżka** w kolumnie **Typ**. Określ ścieżkę do obiektu. Możesz podać bezwzględną lub względną ścieżkę i używać symboli wieloznacznych. Symbol gwiazdki (*) dopasowuje dowolny plik wewnątrz katalogu. Podwójna gwiazdka (**) pasuje do wszystkich plików i katalogów w określonym katalogu. Znak zapytania (?) zastępuje dokładnie jeden znak. Można także dodać opis do identyfikacji procesu.

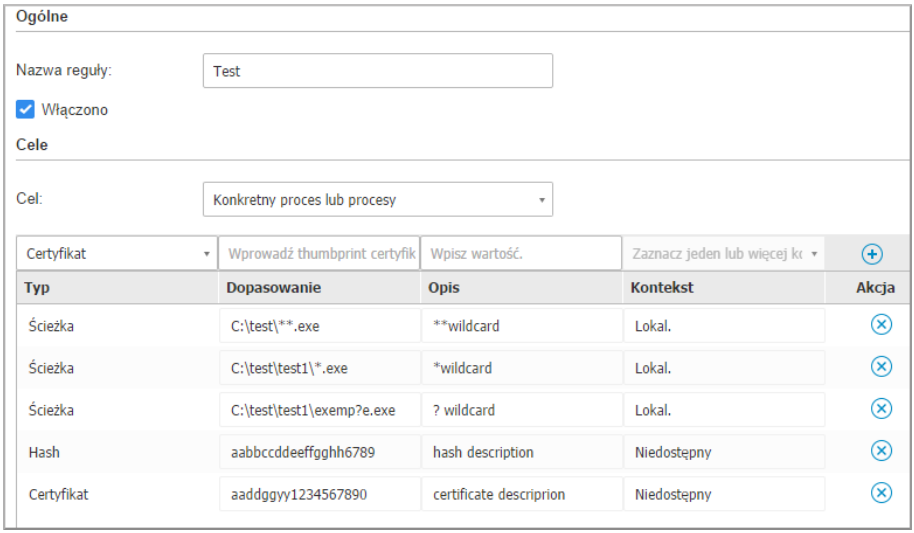
b. Z listy rozwijalnej **Wybierz jeden kontekst lub więcej** można wybierać spośród lokalnych, CD-ROM, usuwalne i sieć. Możesz zablokować aplikacje uruchamiane z przenośnego dysku, lub zezwolić jeśli aplikacja jest wykonywana lokalnie.

– Aby autoryzować aplikacje oparte na HASHu, wybierz **Hash** w kolumnie **Typ** i wpisz wymaganą wartość. Można także dodać opis do identyfikacji procesu.

> **WAŻNE**
> Aby wygenerować wartość HASH, pobierz narzędzie Fingerprint. Aby uzyskać więcej informacji, odwołaj się do „Narzędzia Kontroli Aplikacji” (p. 519)

– Aby autoryzować w oparciu o certyfikat, zaznacz **Certyfikat** i kolumnie **Typ** i wpisz thumbprint certyfikatu. Można także dodać opis do identyfikacji procesu.

> **WAŻNE**
> Aby uzyskać thumbprint certyfikatu, pobierz narzędzie Thumbprint. Aby uzyskać więcej informacji, odwołaj się do „Narzędzia Kontroli Aplikacji” (p. 519)



Reguły aplikacji

Kliknij ⊕**Dodaj**, aby dodać regułę.

- **Magazyn aplikacji lub grup**, aby dodać grupę lub aplikacje wykrytą w twojej sieci. Możesz wyświetlić aplikacje uruchomione w twojej sieci na stronie **Sieć > Magazyn Aplikacji** Aby uzyskać więcej informacji, zapoznaj się z „Magazyn Aplikacji” (p. 192).

  Wstaw aplikację lub nazwę grupy w polu, rozdzielając je przecinkami. Funkcja automatycznego uzupełniania wyświetla propozycje podczas pisania.

5. Zaznacz pole wyboru **Dołącz podprocesu** aby zastosować regułę do zrodzonych procesów podrzędnych.

   Ostrzeżenie
   Podczas ustawiania reguł dla aplikacji przeglądarki, zaleca się, aby wyłączyć tą opcję, aby uniknąć zagrożenia bezpieczeństwa.

6. Opcjonalnie można również określić wyjątki od zasady rozpoczęcia procesu. Dodawanie operacji jest podobne do tej jednej opisanej w poprzednich krokach.
7. W sekcji **Uprawnienia** wybierz czy zezwalasz czy odmawiasz uruchomić reguły.

8. Naciśnij **Zapisz** aby zastosować zmiany.

Aby edytować istniejącą regułę:

1. Kliknij nazwę reguły, aby otworzyć okno konfiguracji.
2. Wprowadź nowe wartości dla opcji które chcesz modyfikować.
3. Naciśnij **Zapisz** aby zastosować zmiany.

Aby ustawić priorytet reguły:

1. Zaznacz pole wyboru pożądanej reguły.
2. Użyj przycisków priorytetu po prawej stronie tabeli:
   - Kliknij przycisk **Góra**, aby wypromować wybraną regułę.
   - Naciśnij przycisk **Dół** aby obniżyć.

Możesz usunąć jedną lub kilka reguł na raz. Wszystko, co musisz zrobić, to:

1. Wybierz reguły, które chcesz usunąć.
2. Kliknij przycisk **Usuń** w górnej części tabeli. Gdy zasada zostanie już usunięta nie będzie już możliwości jej odzyskania.

7.2.9. Kontrola Urządzenia

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów
- macOS

Moduł Kontroli Urządzeń umożliwia zapobieganie wyciekom poufnych danych i infekcją złośliwym oprogramowaniem za pośrednictwem zewnętrznych urządzeń podłączonych punktu końcowego, poprzez zastosowanie blokowania reguł i wykluczeń za pośrednictwem polityk do szerokiego zakresu typów urządzeń.

WAŻNE
W przypadku systemu MacOS Kontrola Urządzeń opiera się na rozszerzeniu jądra. Instalacja rozszerzenia jądra wymaga zgody użytkownika na macOS High Sierra (10.13) i starszych. System powiadamia użytkownika, że rozszerzenie systemu z Bitdefender zostało zablokowane. Użytkownik może na to zezwolić na to z ustawień **Bezpieczeństwo & Prywatność**. Dopóki użytkownik nie zaakceptuje rozszerzenia

systemu Bitdefender, moduł nie będą działał, a interfejs użytkownika Endpoint Security for Mac pokaże krytyczny problem zachęcający użytkownika do zatwierdzenia. Aby wyeliminować interwencję użytkownika, możesz wstępnie zatwierdzić rozszerzenie jądra Bitdefender, dodając je do białej listy za pomocą narzędzia do zarządzania urządzeniami przenośnymi. Aby uzyskać szczegółowe informacje na temat rozszerzeń jądra Bitdefender, zapoznaj się z tym artykułem KB.

Aby użyć modułu Kontroli Urządzeń, musisz po pierwsze zawrzeć go w agencie bezpieczeństwa zainstalowanym na docelowym punkcie końcowym, następnie włączyć opcję **Kontrola Urządzeń** w politykach zastosowanych dla tych punktów końcowych. Po tym, za każdym razem gdy urządzenie zostanie podłączone do zarządzanego punktu końcowego, agent bezpieczeństwa wyśle informacje odnośnie tego zdarzenia do Control Center, zawierającą nazwę urządzenia, jego klasę, identyfikatory i datę oraz czas połączenia.

W poniższej tabeli można znaleźć typy urządzeń obsługiwanych przez Kontrolę Urządzeń w systemach Windows i macOS:

Typ urządzenia	Windows	macOS
Adaptery Bluetooth	x	x
Urządzenia CD-ROM	x	x
Napędy Stacji Dysków	x	Niedostępny
IEEE 1284.4	x	
IEEE 1394	x	
Urządzenia do przetwarzania obrazu	x	x
Modemy	x	Zarządzane w ramach Adapterów Sieciowych
Napędy Taśmowe	x	Niedostępny
Przenośny Windows	x	x
Porty COM/LPT	x	Obsługa portów równoległych i szeregowych
SCSI Raid	x	
Drukarki	x	Obsługuje tylko drukarki podłączone lokalnie
Karta sieciowa	x	x (w tym dongle Wi-Fi)

Typ urządzenia	Windows	macOS
Karty Sieci Bezprzewodowej	x	x
Pamięć Wewnętrzna	x	
Pamięć Zewnętrzna	x	x

Notatka

- W systemie MacOS, jeśli uprawnienie **Niestandardowe** jest wybrane dla określonej klasy urządzenia, będą obowiązywać tylko uprawnienia skonfigurowane dla podkategorii **Inne**.
- W systemie Windows i systemie MacOS Kontrola Urządzeń zezwala lub odmawia dostępu do całego adaptera Bluetooth na poziomie systemu, zgodnie z polityką. Nie ma możliwości ustawienia granularnych wykluczeń na sparowane urządzenie.

Kontrola Urządzeń umożliwia zarządzanie dostępem urządzeń w następujący sposób:

- Zdefiniowanie reguł dostępu
- Zdefiniowanie wykluczeń uprawnień

Reguły

Sekcja **Zasady** umożliwia zdefiniowanie dostępu do urządzeń podłączonych do docelowych punktów końcowych.

Aby ustawić uprawnienia dla pożądanych typów urządzeń:

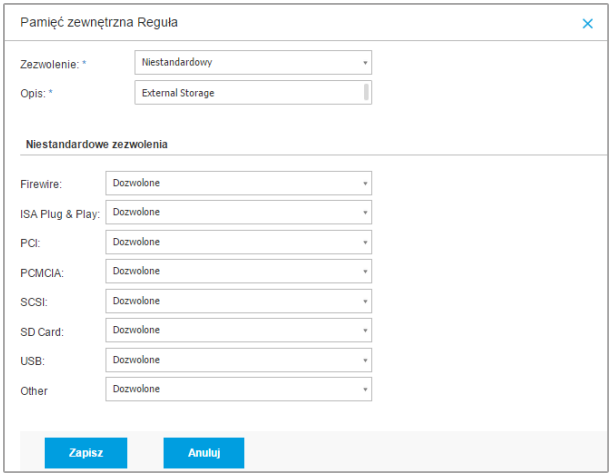
1. Przejdź do **Kontrola Urządzeń > Zasady**.
2. Kliknij nazwę urządzenia w dostępnej tabeli.
3. Wybierz jeden rodzaj uprawnienia z dostępnych opcji. Należy pamiętać, że dostępny zestaw przyzwoleń może różnić się w zależności od typu urządzenia:
   - **Dozwolone**: urządzenia mogące być użyte na docelowym punkcie końcowym.
   - **Zablokowane**: urządzenia nie mogące być użyte na docelowym punkcie końcowym. W tym przypadku, za każdym razem gdy urządzenie zostanie podłączone do punktu końcowego, agent bezpieczeństwa wyświetli powiadomienie oznajmiające, iż urządzenie zostało zablokowane.

     WAŻNE
     Połączone urządzenia wcześniej zablokowane nie są automatycznie odblokowywane ze zmianą uprawnienia na **Dozwolone**. Użytkownik musi

ponownie uruchomić system lub ponownie podłączyć urządzenie, aby móc z niego korzystać.

- **Tylko do odczytu**: tylko funkcje odczytu mogą być użyte dla urządzeń.
- **Niestandardowe**: zdefiniuj rózne uprawnienia dla każdego typu portu z urządzenia, takich jak Firewire, ISA Plug & Play, PCI, PCMCIA, USB, itp. W tym wypadku, lista komponentów dostępnych dla wybranych urządzeń wyświetlana jest i może ustalić uprawnienia dla każdego komponentu.

  Dla przykładu, Zewnętrzne Magazyny, mogą zablokować jedynie USB oraz pozwolić na używanie wszystkich pozostałych portów.



Komputery i Virtualne Maszyny Polityk - Kontrola Sprzętu - Zasady

Wykluczenia

Po ustawieniu zasad dostępu dla różnych typów urządzeń, możesz chcieć wykluczyć konkretne urządzenia lub typy produktów z tych zasad.

Możesz zdefiniować wykluczenia urządzeń:

- Poprzez identyfikatory urządzeń (lub identyfikatory sprzętu) dysygnowane indywidualne urządzenia które chcesz wykluczyć.
- Po identyfikatorze produktu (lub PID) dysygnuje zakres urządzeń produkowanych przez tego samego producenta.

Aby zdefiniować wyjątki dla reguł urządzenia:

1. Przejdź do **Kontrola Urządzeń > Wykluczenia**.
2. Włącz opcję **Wykluczenia**.
3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli.
4. Wybierz metodę, którą chcesz wykorzystać w celu dodawania wykluczeń:
   - **Ręcznie**. W tym przypadku, musisz wprowadzić ID Urządzenia lub ID Produktu, który chcesz wykluczyć, warunkując, że posiadasz listę odpowiednich identyfikatorów:
     a. Wybierz typ wykluczenia (po ID Produktu lub ID Urządzenia).
     b. W polu **Wyjątki**, wprowadź ID które chcesz wykluczyć.
     c. W polu **Opis** wprowadź nazwę, która pomoże Ci zidentyfikować urządzenie lub gamę urządzeń.
     d. Wybierz typ przyzwolenia dla określonych urządzeń (**Dozwolony** lub **Zablokowany**).
     e. Kliknij **Zapisz**.

     Notatka
     Można ręcznie skonfigurować wykluczenia z symbolami wieloznacznymi na podstawie identyfikatora urządzenia, używając składni `wildcards:deviceID`. Użyj znaku zapytania (?), Aby zastąpić jeden znak, oraz gwiazdkę (*), aby zastąpić dowolną liczbę znaków w `IDurządzenia`. Na przykład dla `wildcards:PCI\VEN_8086*`, wszystkie urządzenia zawierające ciąg `PCI\VEN_8086` w ich ID zostaną wykluczone z reguły polityki.

   - **Z Wykrytych Urządzeń**. W tym wypadku, możesz wybrać ID Urządzeń lub ID Produktów aby wykluczyć je z listy wszystkich wykrytych w sieci urządzeń (odnoszące się do konkretnego urządzenia):
     a. Wybierz typ wykluczenia (po ID Produktu lub ID Urządzenia).
     b. w polu tabeli **Wyjątki**, wybierz ID, które chcesz wykluczyć.
        – Dla identyfikatorów Urządzenia, wybierz każde urządzenie do wykluczenia z listy.
        – Dla identyfikatorów produktów, poprzez wybranie urządzenia, które będzie wykluczało wszystkie urządzenia posiadające ten sam Identyfikator Produktu.

c. W polu **Opis** wprowadź nazwę, która pomoże Ci zidentyfikować urządzenie lub gamę urządzeń.
d. Wybierz typ przyzwolenia dla określonych urządzeń (**Dozwolony** lub **Zablokowany**).
e. Kliknij **Zapisz**.

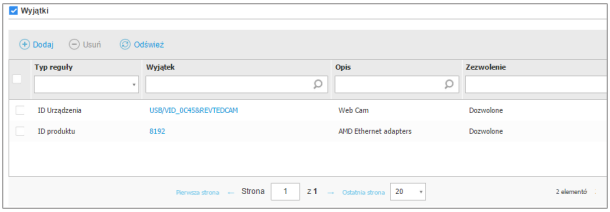
WAŻNE

- Urządzenia już zainstalowane dla punktu końcowego podczas instalacji Bitdefender Endpoint Security Tools zostaną wykryte wyłączenie po ponownym uruchomieniu określonych punktów końcowych.
- Połączone urządzenia wcześniej zablokowane nie są automatycznie odblokowywane przez ustawienie wykluczenia z uprawnieniem **Dozwolone**. Użytkownik musi ponownie uruchomić system lub ponownie podłączyć urządzenie, aby móc z niego korzystać.

Wszelkie wykluczenia urządzeń ukazują się w tabeli **Wykluczenia**.

Aby usunąć wykluczenie:

1. Wybierz je w tabeli.
2. Kliknij przycisk ⊕ **Usuń** w górnej części tabeli.



Polityki Komputerów i Maszyn Wirtualnych - Kontrola Urządzeń - Wyjątki

7.2.10. Relay

Notatka

Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów
- Linux

Ta sekcja pozwala na zdefiniowanie ustawień komunikacji i aktualizacji dla wybranego punktu końcowego z przypisaną rolą relay.

Ustawienia są zorganizowane w poniższych sekcjach:

- Komunikacja
- Aktualizacja

Komunikacja

Zakładka **Komunikacja** zawiera preferencje proxy do komunikacji pomiędzy punktem końcowym relay a komponentami GravityZone.

Jeśli istnieje taka potrzeba, możesz konfigurować niezależnie komunikację pomiędzy docelowymi punktami końcowymi relay i Usługami Bitdefender Cloud / GravityZone, używając następujących ustawień.

- **Zachowaj ustawienia instalacyjne**, w celu zachowania tych samych ustawień proxy zdefiniowanych wraz z paczką instalacyjną.
- **Użyj zdefiniowanego w Głównej sekcji proxy**, aby użyć ustawień zdefiniowanych dla aktualnej polityki, pod sekcją **Ogólne > Ustawienia**.
- **Nie stosuj**, gdy docelowy punkt końcowy nie komunikuje z określonym komponentem Bitdefender za pośrednictwem proxy.

Aktualizacja

Ta sekcja pozwala na zdefiniowane ustawień dla wybranych punktów końcowych z przypisaną rolą relay.

- W sekcji **Aktualizacja** możesz skonfigurować następujące ustawienia:
  - Interwał czasu, podczas sprawdzania aktualizacji przez punkty końcowe relay.
  - Folder zlokalizowany na relayu punktu końcowego gdzie produkty i sygnatury aktualizacji są pobierane może służyć jako mirror. Jeżeli chcesz zdefiniować konkretny folder pobierania, wprowadź jego pełną ścieżkę we właściwym polu.

    WAŻNE
    Zalecane jest definiowanie dedykowanych folderów dla produktu i sygnatury aktualizacji. Unikaj wybierania folderu zawierającego systemowe lub osobiste pliki.

- **Zdefiniuj niestandardową lokalizację aktualizacji**. Domyślną lokalizacją aktualizacji dla agentów relay jest lokalizacja serwera a GravityZone. Możesz określić inne lokalizacje aktualizacji, wpisując adres IP lub nazwę lokalnego hosta jednej lub kilku serwerów aktualizacyjnych w sieci, a następnie skonfigurować ich priorytet za pomocą wyświetlonych przycisków w górę i w dół wyświetlanych nad myszką. Jeżeli pierwsza lokalizacja aktualizacji jest niedostępna, następna zostanie sprawdzona i tak dalej.

  Aby zdefiniować niestandardową lokalizację lokalizacji:

  1. Włącz opcję **Zdefiniuj niestandardową lokalizację aktualizacji**.
  2. Wprowadź adres nowego serwera aktualizacji w polu **Dodaj lokalizację**. Użyj jednej z tych składni:
     - `aktualizacja_serwer_ip:port`
     - `aktualizacja_serwer_nazwa:port`

     Domyślny port 7074.
  3. Jeżeli relay punktu końcowego komunikuje się z lokalnym serwerem aktualizacji przez serwer proxy, wybierz **Użyj Proxy**. Ustawienia proxy definiowane są w sekcji **Ogólne > Ustawienia** będą brane pod uwagę.
  4. Kliknij przycisk **Dodaj** po prawej stronie tabeli.
  5. Użyj strzałek Góra / Dół w kolumnie **Akcja** aby ustawić priorytety zdefiniowanych lokalizacji aktualizacji. Jeżeli pierwsza lokalizacja aktualizacji nie jest dostępna, następna jest brana pod uwagę i tak dalej.

  Aby usunąć lokalizację z listy, kliknij odpowiedni przycisk **Usuń**. Można usunąć domyślną lokalizacje, jednak nie jest to zalecane.

7.2.11. Ochrona Exchange

Notatka
Ten moduł jest dostępny dla Windows dla serwerów.

Security for Exchange otrzymujemy wraz z wysoce konfigurowalnymi ustawieniami, chroniącymi serwery Microsoft Exchange przeciw zagrożeniom takim jak malware, spam i phishing. Wraz z zainstalowaną na serwerze poczty Exchange ochroną możemy również filtrować wiadomości zawierające załączniki oraz zawartość potencjalnie groźną dla polityki bezpieczeństwa twojej firmy.

By zachować wydajność serwerów na normalnym poziomie, ruch wiadomości jest przetwarzany przez filtry Security for Exchange w następującej kolejności:

1. Filtrowanie Antyspam
2. Kontrola Zawartości > Filtrowanie Zawartości
3. Kontrola Zawartości > Filtrowanie Załączników
4. Filtrowanie Antymalware

Ustawienia Security for Exchange są zorganizowane w poniższych sekcjach:

- Ogólne
- Antymalware
- Antyspam
- Kontrola Zawartości

Ogólne

W tej sekcji możesz utworzyć i zarządzać grupami kont wiadomości emailowych, definiować czas przesyłania do kwarantanny oraz blokowanie wskazanych nadawców.

Grupy użytkowników

Control Center pozwala na tworzenie grup użytkowników tak by stosować zróżnicowane zasady skanowania i filtrowania odnoszące się do różnych kategorii użytkowników. Dla przykładu, możesz stworzyć odpowiednie polityki dla sekcji IT, działu sprzedaży lub dla osób kierujących firmą.

Grupy użytkowników są globalnie dostępne, bez względu na użyte polityki lub użytkownika, który je utworzył.

Dla łatwiejszego zarządzania grupami, Control Center automatycznie importuje grupy użytkowników z Windows Active Directory.

Aby utworzyć grupę użytkowników:

1. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Dodatkowe okno jest wyświetlane.
2. Wprowadź nazwę grupy, opis i adresy e-mailowe użytkowników.

Notatka

- Utwórz dużą listę adresów e-mailowych, możesz przekopiować ją z listy pliku tekstowego.
- Dopuszczone separatory list: spacja, przecinek, średnik i ENTER.

3. Kliknij **Zapisz**.

Niestandardowe grupy są edytowalne. Kliknij nazwę grupy by otworzyć okno konfiguracji, gdzie można zmienić szczegóły grupy lub zmodyfikować listę użytkowników.

W celu usunięcia grupy niestandardowej z listy, wybierz grupę i kliknij przycisk ⊖ **Kasuj** w górnej części tabeli.

Notatka
Nie możesz edytować lub usuwać grup Active Directory.

Ustawienia

- **Kasuj pliki z kwarantanny starsze niż (dni).** Domyślnie wszystkie pliki objęte kwarantanną dłużej niż 30 dni są automatycznie usuwane. Jeśli chcesz zmienić ten interwał, wprowadź inne wartości odpowiednie pola.
- **Czarna lista połączeń** Wraz z włączeniem tej funkcji, Serwer Exchange odrzuca wszelkie wiadomości mailowe od zapisanych na listę użytkowników.

  By zbudować czarną listę:
  1. Kliknij link **Edytuj elementy czarnej listy**.
  2. Wpisz adresy e-mail, które chcesz zablokować. Podczas edycji listy, można również użyć następujących symboli wieloznacznych w celu określenia całej domeny e-mail lub wzoru dla adresów e-mail:
     - Gwiazdka (*), zastępując zero, jeden lub więcej znaków.
     - Znak zapytania (?), zastępuje dowolny pojedynczy znak.

     Na przykład, jeśli wpiszesz `*@boohouse.com`, wszystkie adresy e-mail z `boohouse.com` będą zablokowane.
  3. Kliknij **Zapisz**.

Sprawdź IP Domeny (Antyspoofing)

Użyj tego filtra, aby uniemożliwić spamerom spoofowanie adresów e-mail nadawcy i tworzenie wiadomości e-mail, które wyświetlają się jako wysyłane przez kogoś zaufanego. Możesz określić adresy IP upoważnione do wysyłania e-maili do Twoich domen pocztowych oraz, w razie potrzeby, do innych znanych domen pocztowych. Jeśli e-mail wydaje się pochodzić z wymienionych domen, ale adres IP nadawcy nie pasuje do jednego z określonych adresów IP, e-mail zostanie odrzucony.

Ostrzeżenie
Nie należy używać tego filtra, jeśli używasz inteligentnego hosta, usługi filtrowania hostowanego e-maila lub rozwiązania filtrowania bramy e-mail przed serwerami Exchange.

WAŻNE

- Filtr sprawdza tylko nieuwierzytelnione połączenia e-mailowe.
- Zasady dobrego postępowania:
  - Zaleca się, aby stosować ten filtr tylko na serwerach Exchange, które mają bezpośredni kontakt z Internetem. Na przykład, jeśli masz oba serwery Edge Transport i Hub Transport, należy skonfigurować ten filtr tylko na serwerach Edge.
  - Dodaj do swojej listy domen wszystkie wewnętrzne adresy IP dopuszczone do wysłania e-maila przez nieuwierzytelnione połączenia SMTP. Mogą zawierać zautomatyzowane systemy powiadamiania, urządzenia sieciowe, takie jak drukarki, itp.
  - W konfiguracji bazy danych Exchange przy użyciu Grup Dostępności, dodaj także do listy swoich domen adresy IP wszystkich serwerów Hub Transport i skrzynek pocztowych.
  - Należy zachować ostrożność, jeśli chcesz skonfigurować autoryzowane adresy IP dla konkretnych zewnętrznych domen e-mail, które nie są przez Ciebie zarządzane. Jeśli nie uda Ci się utrzymać aktualnej listy adresów IP, wiadomości e-mail z tych domen będą odrzucane. Jeśli korzystasz z kopii zapasowej MX, należy dodać do wszystkich zewnętrznych skonfigurowanych domen pocztowych adresów IP, z których kopia zapasowa MX przekazuje wiadomości e-mail do podstawowego serwera pocztowego.

Aby skonfigurować filtrowanie antyspoof, wykonaj kroki opisane tutaj:

1. Zaznacz pole wyboru **Sparwdź Domenę IP (Antyspoofing)**, aby włączyć filtr.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Pojawia się okno konfiguracji.
3. Wprowadź domenę e-maila w odpowiednim polu.
4. Zapewnia zakres dozwolonych adresów IP, które mają być używane z wcześniej określoną domeną, w formacie CIDR (IP/Maska sieci).
5. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli. Adresy IP są dodane do tabeli.
6. Aby usunąć zakres IP z listy, naciśnij przycisk ⊗ **Usuń** po prawej stronie tabeli.

7. Kliknij **Zapisz**. Domena jest dodana do filtra.

Aby usunąć domenę e-mail z filtra, wybierz ją w tabeli Antyspoofing i kliknij przycisk ⊖ **Usuń** w górnej części tabeli.

Antymalware

Moduł anty-malware chroni serwery poczty Exchange przed wszystkimi rodzajami zagrożeń malware (wirusami, Trojanami, spyware, rootkitami, adware, itp.), poprzez wykrywanie zainfekowanych lub podejrzanych elementów oraz próby dezynfekcji tych plików lub izolowanie infekcji w zależności od określonych operacji.

Skanowanie antymalware odbywa się na dwóch poziomach:

- Poziom Transport
- Exchange Store

Skanowanie Poziomu Transportu

Bitdefender Endpoint Security Tools integruje się agentami przesyłania poczty elektronicznej i skanuje cały ruch wiadomości.

Domyślnie, skanowanie poziomu transportu jest włączone. Bitdefender Endpoint Security Tools filtruje ruch maili jeśli jest to wymagane, informując użytkowników o podjętej czynności poprzez dodanie odpowiedniego komunikatu w treści maila.

Użyj pola wyboru **Filtrowanie anty-malware** aby wyłączyć lub wznowić działanie tej funkcji.

Aby skonfigurować tekst powiadomienia, kliknij łącze **Ustawienia** . Dostępne są następujące opcje:

- **Dodaj stopkę do przeskanowanych e-maili.** Zaznacz to pole wyboru, aby dodać zdanie pojawiające się na dole sprawdzonych wiadomości e-mail. By zmienić domyślny tekst, wpisz swoją wiadomość w polu poniżej.
- **Tekst zastępczy.** Dla wiadomości, w których załączniki zostały usunięte lub przesunięte do kwarantanny, może zostać załączony plik powiadomienia. Aby zmodyfikować domyślny tekst powiadomienia, wprowadź swoją wiadomość w odpowiednim polu.

Filtrowanie anty-malware opiera się na zasadach. Każda wiadomość która trafia na serwer mailowy jest sprawdzana przy pomocy zasad filtrowania anty-malware w kolejności priorytetów do momentu dopasowania do reguły. E-mail jest przetwarzany zgodnie z opcjami określonymi przez te zasady.

Zarządzanie regułami filtrowania

Możesz wyświetlić wszystkie istniejące zasady za-listowane w tabeli, wraz z informacji o ich politykach, statusie i zakresie. Zasady są uporządkowane według priorytetu pierwszeństwa jakie mają zasady z najwyższym jego współczynnikiem.

Każda polityka anty-malware posiada domyślną zasadę, która staje się aktywna wraz z uruchomieniem filtrowania anty-malware. Co musisz wiedzieć na temat domyślnej reguły:

- Nie możesz skopiować, wyłączyć lub usunąć reguły.
- Możesz zmienić tylko ustawienia i akcje skanowania.
- Domyślne priorytetowanie jest zawsze ustawione jako najniższe.

Tworzenie reguł

Masz dwie alternatywy dla tworzenia zasad filtrowania:

- Zacznij z domyślnymi ustawieniami podążając tymi krokami:
  1. Kliknij przycisk ⊕ **Dodaj** górnej części tabeli by otworzyć okno konfiguracyjne.
  2. Konfiguruj ustawienia reguł. W celu uzyskania szczegółowych informacji o opcjach odnieś się do Opcje Zasad.
  3. Kliknij **Zapisz**. Zasada jest wymieniona jako pierwsza w tabeli.
- Wykorzystanie klona niestandardowych zasad jako szablonu, poprzez wykonanie tych kroków:
  1. Wybierz dowolną zasadę z tabeli.
  2. Kliknij przycisk ⊕ **Klonuj** na górnej części tabeli by otworzyć okno konfiguracyjne.
  3. Dostosuj opcje reguł w zależności od potrzeb.
  4. Kliknij **Zapisz**. Zasada jest wymieniona jako pierwsza w tabeli.

Edytowanie Reguł

Aby edytować istniejącą regułę:

1. Kliknij nazwę reguły, aby otworzyć okno konfiguracji.
2. Wprowadź nowe wartości dla opcji które chcesz modyfikować.
3. Kliknij **Zapisz**. Zmiany zostaną wprowadzone po zapisaniu polityki.

Ustalanie zasad priorytetu

Aby zmienić priorytet roli:

1. Wybierz regułę, którą chcesz przenieść.
2. Użyj przycisku ▲ **Up** or ▼ **W dół** z górnej stronie tabeli aby zwiększyć lub zmniejszyć priorytetowanie zasad.

Usuwanie Reguł

Możesz usunąć jedną lub kilka niestandardowych reguł na raz. Wszystko, co musisz zrobić, to:

1. Zaznacz pole wyboru dla zasad które mają zostać usunięte.
2. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Gdy zasada zostanie już usunięta nie będzie już możliwości jej odzyskania.

Opcje Zasad

Dostępne są następujące opcje:

- **Ogólny.** W tej sekcji musisz ustalić nazwę dla zasady, w innym wypadku nie będziesz w stanie jej zapisać. Wybierz pole wyboru **Aktywny** jeśli chcesz by reguła obowiązywała po zapisaniu polityki.
- **Zakres reguł.** Możesz ograniczyć zasadę do stosowania się tylko i wyłącznie do podzbioru e-maili poprzez łączne ustawienie następujących opcji zakresu:
  - **Odnoszenie się do kierunku.** Wybierz kierunek ruchu e-mail, do których ma zostać zastosowana reguła.
  - **Nadawcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko wybranych nadawców. By zawężyć zakres nadawców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Spójrz na wybrane grupy w tabeli po prawej stronie.
  - **Odbiorcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko do wybranych odbiorców. By zawężyć zakres odbiorców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Możesz przeglądać wybrane grupy w tabeli po prawej stronie.

    Zasada obowiązuje, jeśli któryś z adresatów pasuje do twojego wyboru. Jeśli chcesz zastosować regułę tylko wtedy gdy wszyscy odbiorcy są w wybranych grupach, wybierz **Dopasuj wszystkich odbiorców**.

    Notatka
    Adresy w polach **Cc** i **Bcc** również liczą się jako odbiorcy.

    WAŻNE
    Zasady oparte na grupach użytkowników są stosowane tylko do Hub Transportu i Skrzynek e-mail.

- **Opcje.** Skonfiguruj ustawienia skanowania dla wiadomości mailowych odpowiadającym zasadom:
  - **Przeskanowane typy plików.** Użyj tej opcji aby sprecyzować które typy plików chcesz przeskanować. Możesz ustalić skanowanie wszystkich plików (bez

względu na ich rozszerzenie), samych plików aplikacji, lub określonego rozszerzenia, które uważasz za potencjalnie niebezpieczne. Skanowanie wszystkich plików zapewnia najlepszą ochronę, podczas gdy skanowanie jedynie aplikacji jest zalecane dla szybszego skanowania.

> **Notatka**
> Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji" (p. 516).

Jeżeli chcesz skanować tylko pliki o konkretnym rozszerzeniu, masz dwie alternatywy:

- **Zadeklarowane rozszerzenia użytkownika**, tutaj musisz wprowadzić rozszerzenia które mają być skanowane.
- **Wszystkie pliki za wyjątkiem określonych rozszerzeń** tutaj należy podać rozszerzenia które mają zostać pominięte podczas skanowania.

– **Maksymalnym rozmiar załącznika / maila (MB).** zaznacz to pole wyboru i wprowadź wartość w odpowiednim polu aby ustawić maksymalny dopuszczalny rozmiar pliku załącznika lub długości treści maila, który ma być poddawany skanowaniu.
– **Maksymalna głębokość archiwum (poziomy).** Zaznacz pole wyboru i podaj maksymalną głębokość archiwum w odpowiednim polu. Im niższy poziom głębokości, tym większa wydajność i niższy stopień ochrony.
– **Sanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Zaznacz to pole wyboru by skanować w poszukiwaniu złośliwych i niechcianych aplikacji takich jak adware, który może instalować bez wiedzy użytkownika inne oprogramowanie,zmieniać działanie oprogramowania i obniżać wydajność systemu.

- **Akcje.** Możesz określić różne działania dla agenta bezpieczeństwa, aby je automatycznie podjął na plikach, w zależności od rodzaju detekcji.

  Rodzaj detekcji dzieli pliki na trzy kategorie:
  – **Pliki zainfekowane.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI).
  – **Podejrzane pliki.** Te pliki są wykryte jako podejrzane przez analizę heurystyczną i inne techonogię Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach.

- **Nieskanowalne pliki.** Te pliki nie mogą być przeskanowane. Nieskanowalne pliki obejmują, ale nie ograniczają się do chronionych hasłem, zaszyfrowanych lub nadmiernie skompresowanych plików.

Dla każdego rodzaju wykrycia, posiadasz domyślne lub główne działania oraz alternatywne działanie w przypadku awarii jednego z powyższych. Choć nie jest to zalecane, można zmienić ustawienia akcji w odpowiednim menu. Wybierz reakcję, która ma być podjęta:

- **Dezynfekuj.** Usuwa złośliwy kod z zainfekowanego pliku i odbudowuje oryginalny plik. W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.
- **Odrzuć / Usuń email.** Na serwerze z rolą Edge Transport, wykryty email jest odrzucany wraz z kodem błędu 550 SMTP. W każdym innym przypadku, wiadomość email jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Skasuj plik.** Kasuje załączniki w których wystąpiło zdarzenie bez wcześniejszego ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Plik zastępczy.** W miejsce skasowanego pliku umieszczany jest plik tekstowy który powiadamia użytkownika o podjętej czynności.
- **Przenieś plik do kwarantanny.** Przenosi wykryty plik do katalogu kwarantanny i umieszcza plik tekstowy który informuje użytkownika o podjętej czynności. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami w kwarantannie ze strony **Kwarantanna**

> **Notatka**
> Miej na uwadze, że kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni na partycji dysku twardego gdzie zainstalowano agenta. Rozmiar kwarantanny zależy od liczby elementów przechowywanych oraz ich wielkości.

- **Nie podejmuj działania.** Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania. Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny.
- Domyślnie, gdy email pasuje do zakresu reguł, jest przetwarzany wyłącznie ze zgodnymi zasadami, bez sprawdzania pod kątem wszelkich innych zasad.

Jeśli chcesz kontynuować sprawdzanie pod kątem innych zasad, wyczyść pole wyboru **Jeżeli warunki reguł są dopasowane, wstrzymaj przetwarzanie kolejnych reguł**.

Wykluczenia

Jeżeli chcesz by określony ruch email był ignorowany przez zasady filtrowania, możesz zdefiniować wykluczenia skanowania. Aby utworzyć wyjątek:

1. Rozwiń sekcję **Wykluczenia dla Zasad Antymalware**.
2. Kliknij przycisk ⊖ **Dodaj** z sekcji paska narzędzi, co otworzy okno konfiguracji.
3. Konfiguruj ustawienia wykluczeń. W celu uzyskania szczegółowych na temat informacji o opcjach odnieś się do Opcje Zasad.
4. Kliknij **Zapisz**.

Skanowanie Exchange Store

Ochrona Exchange używa Serwisu Webowego Exchange (EWS) od Microsoftu by zapewnić skanowanie skrzynki Exchange i publicznych katalogów bazy danych. Możesz skonfigurować moduł anty-malware by uruchamiać zadania skanowania na żądanie regularnie na obranych bazach danych, zgodnie z wcześniej opisanym harmonogramem.

Notatka

- Skanowanie na żądanie jest dostępne tylko dla serwerów Exchange wraz z zainstalowaną rolą skrzynki pocztowej.
- Miej na uwadze, że skanowanie na żądanie zwiększa zużycie zasobów i zależnie od wybranych opcji skanowania i liczby obiektów do przeskanowania, potrwa odpowiednio długo.

Skanowanie na żądanie wymaga od konta administratora Exchange (konto serwisowe) podszycia się pod użytkownika Exchange i pobrać obiekty docelowe do zeskanowania ze skrzynek pocztowych użytkowników oraz folderów publicznych. Zaleca się, aby w tym celu utworzyć dedykowane konto.

Konto administratora Exchange musi spełniać następujące wymagania:

- Jest członkiem grupy Zarządzania Organizacją (Exchange 2016, 2013 i 2010)
- Jest członkiem grupy Organizacja Administratorów Exchange (Exchange 2007)
- Posiada załączoną skrzynkę mailową.

Umożliwia Skanowanie na żądanie.

1. W sekcji **Zadanie Skanowania** kliknij łącze **Dodaj referencje**
2. Wprowadź nazwę konta serwisowego oraz hasło.
3. Jeśli adres mailowy różni się od nazwy użytkownika, musisz dostarczyć również adres mailowy dla konta serwisowego.
4. Wejdź do URL Serwisu webowego Exchange (EWS) koniecznie, gdy wymiana Automatycznego wykrywania nie działa.

Notatka

- Nazwa użytkownika musi zawierać nazwę domeny, tak jak w `user@domain` lub `domain\user`
- Nie zapomnij zaktualizować referencji w Control Center, za każdym razem, gdy się zmienią.

Zarządzanie Zadaniami skanowania

Zadanie skanowania tabelki pokazuje wszystkie zaplanowane zadania i dostarcza informacji o ich celu i rekurencji.

By utworzyć zadanie skanowania Exchange Store:

1. W sekcji **Zadanie Skanowania** kliknij przycisk ⊕ **Dodaj** znajdujący się na górnej części tabeli, by otworzyć okno konfiguracji.
2. Konfiguruj ustawienie zadania, tak jak opisano w następującej sekcji.
3. Kliknij **Zapisz**. Zadanie jest dodane do listy i zostaje skuteczne w momencie zapisania polityki.

Możesz edytować zadanie w każdym momencie, wystarczy kliknąć nazwę zadania.

Aby usunąć zadanie z listy, wybierz zadanie i kliknij przycisk ⊖ **Kasuj** z górnej strony tabeli.

Ustawienia Zadań Skanowania

Zadania mają szereg ustawień, które można znaleźć opisane w niniejszym dokumencie:

- **Ogólne.** Wprowadź sugestywną nazwę dla zadania.

  Notatka
  Możesz zobaczyć nazwę zadania w osi czasu Bitdefender Endpoint Security Tools.

- **Harmonogram.** Użyj opcji planowania, aby skonfigurować harmonogram skanowania. Możesz ustawić skanowanie aby uruchamiało się co kilka godzin,

dni lub tygodni, rozpoczynając się określonego dnia o ustalonej porze. W przypadku dużych baz danych, zadanie skanowania może zająć dużo czasu i może mieć wpływ na wydajność serwera. W takich przypadkach można skonfigurować zdanie, aby zaprzestało działania po określonym czasie.

- **Cel.** Wybierz kontener i obiekty do skanowania. Możesz wybrać by skanowanie skrzynek pocztowych, publicznych folderów lub obu. Oprócz wiadomości e-mail, możesz skanować inne obiekty takie jak **Kontakty**, **Zadania**, **Spotkania** oraz **Elementy pocztowe**. Możesz ponadto ustawić następujące ograniczenia odnoszące się do skanowanej treści:
  - Tylko nieprzeczytane wiadomości
  - Tylko elementy z załącznikami
  - Tylko nowe pozycje, otrzymały określony przedział czasowy.

  Dla przykładu, możesz wybrać skanowanie tylko e-maili ze skrzyynek pocztowych użytkowników, które otrzymali w ciągu ostatnich siedmiu dni.

  Zaznacz pole wyboru **Wykluczenia**, jeżeli chcesz zdefiniować skanowanie wyjątków. Aby utworzyć wyjątek, użyj pól z nagłówka tabeli w następujący sposób:
  1. Wybierz typ repozytorium z menu.
  2. Zależnie od rodzaju magazynu, określ obiekt jaki ma być wykluczony:

Typ repozytorium	Format obiektu
Skrzynka pocztowa	Adres e-mail
Folder publiczny	Ścieżka folderu, zaczynająca się od źródła
Baza danych	Tożsamość bazy danych

     Notatka
     By posiąść tożsamość bazy danych użyj polecenia shell Exchange:
     `Get-MailboxDatabase | fl name,identity`

     Możesz dodać tylko jedną pozycję naraz. Jeżeli posiadasz kilka pozycji tego samego typu, musisz zdefiniować tyle zasad ile posiadasz pozycji.
  3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli by zapisać wyjątek i dodać go do listy.

  Aby usunąć zasadę wyjątku z listy, kliknij odpowiadający mu przycisk ⊖ **Usuń**.
- **Opcje.** Skonfiguruj ustawienia skanowania dla wiadomości mailowych odpowiadającym zasadom:

- **Przeskanowane typy plików.** Użyj tej opcji aby sprecyzować które typy plików chcesz przeskanować. Możesz ustalić skanowanie wszystkich plików (bez względu na ich rozszerzenie), samych plików aplikacji, lub określonego rozszerzenia, które uważasz za potencjalnie niebezpieczne. Skanowanie wszystkich plików zapewnia najlepszą ochronę, podczas gdy skanowanie jedynie aplikacji jest zalecane dla szybszego skanowania.

  > **Notatka**
  > Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Typy Pliku Aplikacji" (p. 516).

  Jeżeli chcesz skanować tylko pliki o konkretnym rozszerzeniu, masz dwie alternatywy:
  - **Zadeklarowane rozszerzenia użytkownika**, tutaj musisz wprowadzić rozszerzenia które mają być skanowane.
  - **Wszystkie pliki za wyjątkiem określonych rozszerzeń** tutaj należy podać rozszerzenia które mają zostać pominięte podczas skanowania.
- **Maksymalnym rozmiar załącznika / maila (MB).** zaznacz to pole wyboru i wprowadź wartość w odpowiednim polu aby ustawić maksymalny dopuszczalny rozmiar pliku załącznika lub długości treści maila, który ma być poddawany skanowaniu.
- **Maksymalna głębokość archiwum (poziomy).** Zaznacz pole wyboru i podaj maksymalną głębokość archiwum w odpowiednim polu. Im niższy poziom głębokości, tym większa wydajność i niższy stopień ochrony.
- **Sanuj w poszukiwaniu Potencjalnie Niechcianych Aplikacji (PUA).** Zaznacz to pole wyboru by skanować w poszukiwaniu złośliwych i niechcianych aplikacji takich jak adware, który może instalować bez wiedzy użytkownika inne oprogramowanie,zmieniać działanie oprogramowania i obniżać wydajność systemu.

- **Akcje.** Możesz określić różne działania dla agenta bezpieczeństwa, aby je automatycznie podjął na plikach, w zależności od rodzaju detekcji.

  Rodzaj detekcji dzieli pliki na trzy kategorie:
  - **Pliki zainfekowane.** Bitdefender wykrywa pliki jako zainfekowane poprzez rożne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencje (SI).
  - **Podejrzane pliki.** Te pliki są wykryte jako podejrzane przez analizę heurystyczną i inne techonogię Bitdefendera. To dostarcza wysoki poziom

wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzane) w niektórych przypadkach.
- **Nieskanowalne pliki.** Te pliki nie mogą być przeskanowane. Nieskanowalne pliki obejmują, ale nie ograniczają się do chronionych hasłem, zaszyfrowanych lub nadmiernie skompresowanych plików.

Dla każdego rodzaju wykrycia, posiadasz domyślne lub główne działania oraz alternatywne działanie w przypadku awarii jednego z powyższych. Choć nie jest to zalecane, można zmienić ustawienia akcji w odpowiednim menu. Wybierz reakcję, która ma być podjęta:
- **Dezynfekuj.** Usuwa złośliwy kod z zainfekowanego pliku i odbudowuje oryginalny plik. W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. Jest zalecane aby zawsze było to pierwsze działanie wykonywane na zainfekowanych plikach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.
- **Odrzuć / Skasuj e-mail.** Wiadomość e-mail jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Skasuj plik.** Kasuje załączniki w których wystąpiło zdarzenie bez wcześniejszego ostrzeżenia. Wskazane jest, aby unikać tego działania.
- **Plik zastępczy.** W miejsce skasowanego pliku umieszczany jest plik tekstowy który powiadamia użytkownika o podjętej czynności.
- **Przenieś plik do kwarantanny.** Przenosi wykryty plik do katalogu kwarantanny i umieszcza plik tekstowy który informuje użytkownika o podjętej czynności. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Możesz zarządzać plikami w kwarantannie ze strony **Kwarantanna**

> **Notatka**
> Miej na uwadze, że kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni na partycji dysku twardego gdzie zainstalowano agenta. Rozmiar kwarantanny zależy od liczby i rozmiaru przechowywanych e-maili.

- **Nie podejmuj działania.** Żadne działanie nie zostanie podjęte na wykrytych plikach. Te pliki pokażą się jedynie w dzienniku skanowania. Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzane pliki. Możesz zmienić domyślną akcje, w celu przeniesienia podejrzanych plików do kwarantanny.
- Domyślnie, gdy email pasuje do zakresu reguł, jest przetwarzany wyłącznie ze zgodnymi zasadami, bez sprawdzania pod kątem wszelkich innych zasad.

Jeśli chcesz kontynuować sprawdzanie pod kątem innych zasad, wyczyść pole wyboru **Jeżeli warunki reguł są dopasowane, wstrzymaj przetwarzanie kolejnych reguł**.

Antyspam

Moduł anty-spamowy oferuje wielowarstwową ochronę przeciw spamowi i phishingowi poprzez wykorzystanie kombinacji zróżnicowanych filtrów i silników, które określają czy wiadomości są spamem lub nie.

Notatka

- Filtrowanie antyspam jest dostępne dla:
  - Exchange Server 2016/2013 z rolą Edge Transport lub Mailbox
  - Exchange Server 2010/2007 z rolą Edge Transport lub Hub Transport
- Jeżeli posiadasz zarówno role Edge i Hub w swojej organizacji Exchange, zalecane się aby włączyć filtr antyspamowy na serwerze wraz z rolą Edge Transport.

Filtrowanie spamu jest automatycznie włączone dla e-maili przychodzących. Użyj pola wyboru **Filtrowanie Antyspam** aby wyłączyć lub wznowić działanie tej funkcji.

Filtry Antyspamowe

Wiadomości email są porównywane z regułami antyspamowymi w oparciu o grupy nadawców i odbiorców, według kolejności, tak długo aż nie zostaną dopasowane zasady. E-mail jest przetwarzany zgodnie z regułami opcji i działań podejmowanych przy celu wykrywania spamu.

Niektóre filtry antyspamowe są konfigurowalne i można je kontrolować bez względu czy z nich korzystamy czy nie. To jest lista opcjonalnych filtrów:

- **Filtr kodowania.** Wiele wiadomości email zawierających spam jest napisanych cyrylicą lub przy użyciu azjatyckiego kodowania znaków. Filtr zestawu znaków wykrywa tego typu wiadomości i oznacza je jako SPAM.
- **Oznaczona Jednoznaczna Treść Erotyczna.** Spam zawierające treści o charakterze erotycznym musza zawierać wyraźne ostrzeżenie w temacie wiadomości. Filtr wykrywa e-maile zaznacza jako TREŚCI EROTYCZNE: w temacie wiadomości i oznacza jako spam.
- **Filtr URL.** Prawie wszystkie spamowe maile zawierają liczne linki do wielu lokalizacji webowych. Zwykle miejsca te zawierają więcej reklam i oferują możliwość zakupu. Czasami są również używane do phishingu.

Bitdefender utrzymuje bazę danych takich łączy. Filtr URL sprawdza każde łącze URL w treści wiadomości pod kątem zawartych w bazie danych. Jeżeli będzie zgodność, wiadomość mailowa jest oznaczana jako spam.

- **Realtime Blackhole List (RBL).** Jest to filtr, który pozwala na sprawdzanie serwerów poczty nadawców pod kątem serwerów RBL osób trzecich.. Filtry wykorzystują protokoły DNSBL i serwery RBL do filtrowania spamu bazując na reputację jego nadawców.

  Adres serwera poczty jest pobierany z nagłówka e-maila, a jego ważność sprawdzana. Jeżeli adres należy do prywatnej klasy (`10.0.0.0`, `172.16.0.0` do `172.31.0.0` lub `192.168.0.0` do `192.168.255.0`), są ignorowane.

  Sprawdzanie DNS jest wykonywane na domenie `d.c.b.a.rbl.example.com`, gdzie `d.c.b.a` jest odwróconym adresem IP serwera a `rbl.example.com` jest serwerem RBL. Jeśli DNS odpowie, że domena jest ważna, oznacza to że adres IP jest listowany w serwerze RBL oraz konkretny wynik serwera został zwrócony. Ten zapis mieści się w zakresie od 0 do 100, stosownie do poziomu zaufania gwarantowanego przez serwer.

  Zapytanie jest wykonywane dla każdego serwera RBL z listy a wynik zwracany jest każdy dodany do zapisu pośredniego. Gdy wynik uzyska 100, nie będą wykonywane kolejne pytania.

  Jeśli wynik filtowania RBL wynosi 100 lub więcej, wiadomość email uznawana jest za spam i określone działania zostaną podjęte. W innym przypadku, wynik spamu jest przeliczany z wyniku filtra RBL oraz dodawany do globalnego wyniku spamu tego emaila.
- **Filtry Heurystyczne.** Opracowane przez Bitdefender, Heurystyczne filtry wykrywają nowy i nieznany spam. Filtru jest automatycznie przepuszczane przez dużą ilości emaili zawierających spam wewnątrz Laboratorium Antyspamowego Bitdefender. Podczas przeszkalania, uczy się rozróżniać wiadomości spośród tych właściwych i zawierającymi spam w celu rozpoznawania nowych wiadomości zawierających spam poprzez postrzeganie podobieństw, czasami bardzo subtelnych, z wiadomościami, które zostały już zbadane. Filtrowanie zostało zaprojektowane, tak by usprawnić wykrywanie bazujące na sygnaturach, zarazem utrzymując liczbę fałszywych alarmów na bardzo niskim poziomie.
- **Zapytanie o chmurę Bitdefender.** Bitdefender utrzymuje stale rozwijającą się bazę "odcisków palców" wiadomości spamowych, która znajduje się w chmurze. Zapytanie zawierające odcisk palca wiadomości email zostanie wysyłane do serwera w chmurze w celu zweryfikowania na bieżąco czy ten email to spam.

Nawet jeżeli odcisk palca nie został odnaleziony w bazie danych, jest on sprawdzany pod kątem innych zapytań, dopiero po spełnieniu określonych warunków email zostaje oznaczony jako spam.

Zarządzanie Regułami Antyspamu

Możesz wyświetlić wszystkie istniejące zasady za-listowane w tabeli, wraz z informacji o ich politykach, statusie i zakresie. Zasady są uporządkowane według priorytetu pierwszeństwa jakie mają zasady z najwyższym jego współczynnikiem.

Każda polityka antyspam posiada domyślną politykę, która staje się aktywna wraz z uruchomieniem modułu. Co musisz wiedzieć na temat domyślnej reguły:

- Nie możesz skopiować, wyłączyć lub usunąć reguły.
- Możesz zmienić tylko ustawienia i akcje skanowania.
- Domyślne priorytetowanie jest zawsze ustawione jako najniższe.

Tworzenie reguł

Aby stworzyć regułę:

1. Kliknij przycisk ⊕ **Dodaj** górnej części tabeli by otworzyć okno konfiguracyjne.
2. Konfiguruj ustawienia reguł. Aby uzyskać informacje na temat opcji, odwołaj się do „Opcje Zasad” (p. 366).
3. Kliknij **Zapisz**. Zasada jest wymieniona jako pierwsza w tabeli.

Edytowanie Reguł

Aby edytować istniejącą regułę:

1. Kliknij nazwę reguły, aby otworzyć okno konfiguracji.
2. Wprowadź nowe wartości dla opcji które chcesz modyfikować.
3. Kliknij **Zapisz**. Jeżeli reguła jest aktywna, zmiany zaczną obowiązywać, po zapisaniu polityki.

Ustalanie zasad priorytetu

Aby zmienić priorytety reguł, wybierz regułę którą chcesz ustawić i przesuń ją przy pomocy strzałek ⊙ **Do góry** oraz ⊙ **Na dół** w górnej części tabeli. Możesz przesunąć tylko jedną zasadę naraz.

Usuwanie Reguł

Jeśli nie chcesz korzystać już więcej z reguły, wybierz regułę i kliknij przycisk ⊖ **Kasuj** z górnej części tabeli.

Opcje Zasad

Dostępne są następujące opcje:

- **Ogólny.** W tej sekcji musisz ustalić nazwę dla zasady, w innym wypadku nie będziesz w stanie jej zapisać. Wybierz pole wyboru **Aktywny** jeśli chcesz by reguła obowiązywała po zapisaniu polityki.
- **Zakres reguł.** Możesz ograniczyć zasadę do stosowania się tylko i wyłącznie do podzbioru e-maili poprzez łączne ustawienie następujących opcji zakresu:
  - **Odnoszenie się do kierunku.** Wybierz kierunek ruchu e-mail, do których ma zostać zastosowana reguła.
  - **Nadawcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko wybranych nadawców. By zawężyć zakres nadawców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Spójrz na wybrane grupy w tabeli po prawej stronie.
  - **Odbiorcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko do wybranych odbiorców. By zawężyć zakres odbiorców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Możesz przeglądać wybrane grupy w tabeli po prawej stronie.

    Zasada obowiązuje, jeśli któryś z adresatów pasuje do twojego wyboru. Jeśli chcesz zastosować regułę tylko wtedy gdy wszyscy odbiorcy są w wybranych grupach, wybierz **Dopasuj wszystkich odbiorców**.

    Notatka
    Adresy w polach **Cc** i **Bcc** również liczą się jako odbiorcy.

    WAŻNE
    Zasady oparte na grupach użytkowników są stosowane tylko do Hub Transportu i Skrzynek e-mail.

- **Ustawienia.** Kliknij poziom bezpieczeństwa który najlepiej odpowiada twoim potrzebom (**Agresywny**, **Normalny** lub **Tolerancyjny**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

  Dodatkowo, można włączyć różne filtry. Szczegółowe informacje na temat tych filtrów, znajdziesz w „Filtry Antyspamowe” (p. 364).

  WAŻNE
  Filtry RBL wymagają dodatkowej konfiguracji. Możesz skonfigurować filtry po utworzeniu lub edytowaniu reguły. Aby uzyskać więcej informacji, odwołaj się do „Konfigurowanie Filtra RBL” (p. 369)

  Dla uwierzytelnionych połączeń można wybrać czy chcemy obejść lub nie dokonywać skanowania antyspamowego.

- **Akcje.** Istnieje wiele działań, które można podjąć na wykrytych wiadomościach mailowych. Każde działanie ma z kolei kilka możliwych rozwiązań lub działań dodatkowych. Znajdź je opisane tutaj:

  Główne akcje:
  - **Dostarcz e-mail.** Maile dochodzą do skrzynek odbiorców.
  - **Kwaranta e-maili.** Wiadomość zostaje zaszyfrowana i zapisana w katalogu kwarantanny dla Serwera Exchange, bez dostarczania jej do odbiorcy. Możesz zarządzać kwarantanną e-maili na stronie **Kwarantanna**.
  - **Przekierowanie e-maili.** Wiadomości mailowe nie zostają dostarczone do docelowych odbiorców, ale do skrzynki którą zdefiniujemy w odpowiednim polu.
  - **Odrzuć / Usuń email.** Na serwerze z rolą Edge Transport, wykryty email jest odrzucany wraz z kodem błędu 550 SMTP. W każdym innym przypadku, wiadomość email jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.

  Działania drugorzędne:
  - **Integracja z Exchange SCL.** Dodaje nagłówek do wiadomości zawierającej spam, pozwalając Serwerowi Exchange lub Microsoft Outlook na podjęcie działań w zależności od poziomu zaufania mechanizmu spamu (SCL).
  - **Oznacz temat wiadomości jako.** Możesz dodać etykietę do tematu e-maila, aby pomóc użytkownikowi odróżnienie w skrzynce wiadomości zawierających spam.
  - **Dodaj nagłówek e-maila.** Nagłówek jest dodawany do wiadomości wykrytych jako spam. Możesz edytować nazwę nagłówka oraz jego wartość poprzez wprowadzenie pożądanej wartości w odpowiednie pole. Dalej, możesz użyć tych nagłówków e-maili dla utworzenia dodatkowych filtrów.
  - **Zapisz e-mail na dysk.** Kopia e-maila zawierającego spam jest zapisywana jako plik w określonym folderze. Dostarcz kompletną ścieżkę do folderu w odpowiednim polu.

    Notatka
    Ta opcja wspiera tylko e-maile w formacie MIME.

  - **Archiwizuj na koncie.** Kopia wykrytego e-maila jest dostarczana na określony adres mailowy. To działanie dodaje określony adres mailowy do listy e-mailowej Bcc.
- Domyślnie, gdy email pasuje do zakresu reguł, jest przetwarzany wyłącznie ze zgodnymi zasadami, bez sprawdzania pod kątem wszelkich innych zasad. Jeśli chcesz kontynuować sprawdzanie pod kątem innych zasad, wyczyść pole wyboru **Jeżeli warunki reguł są dopasowane, wstrzymaj przetwarzanie kolejnych reguł**.

Konfigurowanie Filtra RBL

Jeżeli chcesz użyć Filtr RBL, musisz dostarczyć listę serwerów RBL.

Aby skonfigurować filtry:

1. Na stronie **Antyspam**, kliknij odnośnik **Ustawienia** aby otworzyć okno konfiguracyjne.
2. Dostarcz adresy IP serwerów DNS do zapytania i kwerendy w odpowiednich polach. Jeśli nie skonfigurowano adresu serwera DNS lub serwer DNS jest niedostępny, filtr RBL korzysta z serwerów DNS systemu.
3. Dla każdego serwera RBL:
   a. Wprowadź nazwę hosta lub adres IP serwera oraz poziom zaufania przypisany do serwera, w polu nagłówku tabeli.
   b. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli.
4. Kliknij **Zapisz**.

Konfigurowanie Białej Listy Nadawców

W przypadku znanych nadawców e-maili, można ominąć proces niepotrzebnego zużywania zasobów serwera, poprzez dodanie ich do listy zaufanych lub zablokowanych nadawców. W ten sposób serwer mailowy będzie zawsze przepuszczał lub blokował przychodzące od tych nadawców wiadomości. Dla przykładu, prowadzisz intensywną dyskusję biznesową z partnerem i chcesz być pewny że otrzymasz wszystkie e-maile. Możesz dodać partnera do tak zwanej białej listy.

Aby zbudować białą listę zaufanych nadawców:

1. Kliknij link **Biała Lista**, aby otworzyć okno konfiguracji.
2. Zaznacz pole wyboru **Biała Lista Nadawców**.
3. Wprowadź adres e-mail w odpowiednim polu. Podczas edycji listy, można również użyć następujących symboli wieloznacznych w celu określenia całej domeny e-mail lub wzoru dla adresów e-mail:

- Gwiazdka (*), zastępując zero, jeden lub więcej znaków.
- Znak zapytania (?), zastępuje dowolny pojedynczy znak.

Na przykład, jeśli wprowadzisz `*.gov`, wszystkie maile przychodzące z domeny `.gov` będą zaakceptowane.

4. Kliknij **Zapisz**.

Notatka
Czarna lista znanych nadawców spamu, użyj opcji **Połączenie czarnej listy** z sekcji **Ochrona Exchange > Ogólne > Ustawienia**.

Kontrola Zawartości

Użyj kontroli zawartości w celu zwiększenia ochrony poczty e-mail poprzez filtrowanie całego ruchu e-mail, który jest niezgodny z zasadami polityk w firmie (niepożądane lub potencjalnie wrażliwe treści).

Ten moduł posiada dwie opcje filtrowania e-mail dla całkowitej kontroli zawartości e-mail.

- Filtrowanie zawartości
- Filtrowanie załączników

Notatka
Filtrowanie zawartości i załączników jest możliwe dla:

- Exchange Server 2016/2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010/2007 z rolą Edge Transport lub Hub Transport

Zarządzanie regułami filtrowania

Kontrola filtrowania zawartości oparta jest na zasadach. Można definiować różne zasady dla różnych użytkowników oraz ich grup. Każdy e-mail który trafia do serwera poczty jest sprawdzany pod kątem zasad filtrowania, kolejności priorytetów do momentu dopasowania do reguły. E-mail jest przetwarzany zgodnie z opcjami określonymi przez te zasady.

Reguły filtrowania zawartości poprzedzają reguły filtrowania załączników.

Reguły filtrowania zawartości i załączników są wymienione w odpowiednich tabelach w kolejności według priorytetu, przy czym pierwsza reguła ma najwyższy priorytet. Dla każdej reguły dostarczane są następujące informacje:

- Priorytet

- Nazwa
- Kierunek ruchu
- Grupy nadawców i odbiorców

Tworzenie reguł

Masz dwie alternatywy dla tworzenia zasad filtrowania:

- Zacznij z domyślnymi ustawieniami podążając tymi krokami:
  1. Kliknij przycisk ⊕ **Dodaj** górnej części tabeli by otworzyć okno konfiguracyjne.
  2. Konfiguruj ustawienia reguł. Aby uzyskać szczegółowe informacje na temat poszczególnych opcji filtrowania zawartości i załączników, zapoznaj się z:
     - Opcje Zasad Filtrowania Zawartości
     - Opcje Zasad Filtrowania Załączników.
  3. Kliknij **Zapisz**. Zasada jest wymieniona jako pierwsza w tabeli.
- Wykorzystanie klona niestandardowych zasad jako szablonu, poprzez wykonanie tych kroków:
  1. Wybierz żądaną regułę z tabeli.
  2. Kliknij przycisk ⊙ **Klonuj** na górnej części tabeli by otworzyć okno konfiguracyjne.
  3. Dostosuj opcje reguły do swoich potrzeb.
  4. Kliknij **Zapisz**. Zasada jest wymieniona jako pierwsza w tabeli.

Edytowanie Reguł

Aby edytować istniejącą regułę:

1. Kliknij nazwę reguły, aby otworzyć okno konfiguracji.
2. Wprowadź nowe wartości dla opcji które chcesz modyfikować.
3. Kliknij **Zapisz**. Zmiany zostaną wprowadzone po zapisaniu polityki.

Ustalanie zasad priorytetu

Aby zmienić priorytet roli:

1. Wybierz regułę, którą chcesz przenieść.
2. Użyj przycisku ⊙ **Up** or ⊙ **W dół** z górnej stronie tabeli aby zwiększyć lub zmniejszyć priorytetowanie zasad.

Usuwanie Reguł

Możesz usunąć jedną lub kilka reguł niestandardowych. Wszystko, co musisz zrobić, to:

1. Wybierz reguły, które chcesz usunąć.

2. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Gdy zasada zostanie już usunięta nie będzie już możliwości jej odzyskania.

Filtrowanie zawartości

Filtrowanie treści pomaga filtrować ruch e-mail na podstawie wcześniej zdefiniowanego ciągu znaków. Ciągi te są porównywane z tematem e-mail lub z zawartością tekstu treści wiadomości. Dzięki Filtrowaniu treści możesz:

- Zablokuj niechcianą zawartość przed dostaniem się do skrzynek pocztowych serwera Exchange.
- Blokuj wychodzące maile zawierające poufne dane.
- Archiwizuj e-maile, które spełniają określone warunki w stosunku innego konta e-mail lub dysku. Dla przykładu, możesz zapisać wiadomości wysłane na adres działu wsparcia twojej firmy do folderu na dysku lokalnym.

Umożliwianie Filtrowania Załączników

Jeżeli chcesz użyć filtrowania zawartości, wybierz pole wyboru **Filtrowanie treści**.

Do tworzenia i zarządzania zasadami filtrowania zawartości, odnieś się do „Zarządzanie regułami filtrowania” (p. 370).

Opcje Zasad

- **Ogólny.** W tej sekcji musisz ustalić nazwę dla zasady, w innym wypadku nie będziesz w stanie jej zapisać. Wybierz pole wyboru **Aktywny** jeśli chcesz by reguła obowiązywała po zapisaniu polityki.
- **Zakres reguł.** Możesz ograniczyć zasadę do stosowania się tylko i wyłącznie do podzbioru e-maili poprzez łączne ustawienie następujących opcji zakresu:
  - **Odnoszenie się do kierunku.** Wybierz kierunek ruchu e-mail, do których ma zostać zastosowana reguła.
  - **Nadawcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko wybranych nadawców. By zawężyć zakres nadawców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Spójrz na wybrane grupy w tabeli po prawej stronie.
  - **Odbiorcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko do wybranych odbiorców. By zawężyć zakres odbiorców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Możesz przeglądać wybrane grupy w tabeli po prawej stronie.

    Zasada obowiązuje, jeśli któryś z adresatów pasuje do twojego wyboru. Jeśli chcesz zastosować regułę tylko wtedy gdy wszyscy odbiorcy są w wybranych grupach, wybierz **Dopasuj wszystkich odbiorców**.

Notatka
Adresy w polach **Cc** i **Bcc** również liczą się jako odbiorcy.

WAŻNE
Zasady oparte na grupach użytkowników są stosowane tylko do Hub Transportu i Skrzynek e-mail.

- **Ustawienia.** Skonfiguruj wyrażenia w celu wyszukiwania ich w e-mailach jak opisano tutaj:
  1. Wybierz fragment wiadomości e-mail która ma zostać sprawdzona:
     - Temat e-maila poprzez zaznaczenie pola wyboru **Filtrowanie po temacie**. Wszystkie e-maile, których temat zawiera którekolwiek z wyrażeń zawartych w odpowiedniej tabeli będą filtrowane.
     - Zawartość treści poprzez zaznaczenie pola wyboru **Filtrowania po zawartości treści**. Wszystkie wiadomości zawierające w swojej treści którekolwiek z wyrażonych definicji będą filtrowane.
     - Zarówno temat jak i treść wiadomości poprzez zaznaczenie obu pól wyboru. Wszystkie wiadomości email których tematy pasują do zestawów zasad z pierwszej tabeli ORAZ treść ich wiadomości zawierające jakiekolwiek sformułowanie z drugiej tablicy będą filtrowane. Na przykład:

       Pierwsza tabela zawiera wyrażenia: `biuletyn` oraz `tygodniowy`. Druga tabela zwiera wyrażenia: `zakupy`, `cena` i `oferta`.

       Wiadomość email, której temat brzmi "Miesięczny **biuletyn** od Twojego ulubionego sprzedawcy zegarków" oraz treść zawierająca frazę "Mamy przyjemność zaprezentować tobie naszą najnowszą **ofertę** zawierającą sensacyjne zegarki w nieodpartych **cenach**." spotka się z regułami i będzie filtrowana. Jeżeli temat będzie brzmiał "Wiadomości od twojego sprzedawcy zegarków", wiadomość email nie będzie filtrowana.
  2. Zbuduj listę warunków wykorzystujących pola z nagłówków tabeli. Dla każdego warunku, wykonaj następujące kroki:
     a. Wybierz typ ekspresji używanej w wyszukiwaniu. Możesz zadecydować by wprowadzić dokładne wyrażenie lub zbudować wzór tekstu z użyciem regularnych wyrażeń.

        Notatka
        Składnia wyrażeń regularnych jest sprawdzana w oparciu o gramatykę ECMAScript.

b. Wprowadź ciąg wyszukiwania w polu **Wyrażenia**.

Na przykład:

i. Wyrażenie `5[1-5]\d{2}([\s\-]?\d{4}){3}` dopasowuje karty bankowe o numerach zaczynających się od pięćdziesiąt jeden przez pięćdziesiąt pięć, ma szesnaście cyfr w grupach po cztery, a grupy mogą być oddzielone spacją lub myślnikiem. Dlatego też, każdy e-mail zawierający numery kart kredytowych w jednym z formatów: `5257-4938-3957-3948`, `5257 4938 3957 3948` or `5257493839573948`, będzie przefiltrowany.

ii. Wyrażenie to wykryje e-maile ze słowami `loteria`, `pieniądze` i `nagroda`, znajdującymi się dokładnie w tej kolejności:

```
(lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
```

Aby wykryć wiadomości e-mail, które zawierają każde z trzech słów, niezależnie od ich kolejności, dodaj trzy wyrażenia regularne w różnej kolejności wyrazów.

iii. Wyrażenie to wykryje e-maile, które zawierają trzy lub więcej wystąpień tego słowa `nagroda`:

```
(prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
```

c. Jeśli chcesz rozróżniać duże litery od małych liter w porównaniach tekstu, zaznacz okno wyboru **Porównywanie dopasowania**. Dla przykładu, w przypadku zaznaczenia pola wyboru, `Biuletyn` nie jest tym samym co `biuletyn`.

d. Jeśli nie chcesz by wyrażenia były dopasowane pod kątem fragmentów słów, zaznacz pole wyboru **Całe słowa**. Dla przykładu, z zaznaczonym oknem wyboru, wyrażenie `Wynagrodzenie Anny` nie będzie pasowało do wyrażenia `Wynagrodzenie Marianny`.

e. Kliknij przycisk ⊕ **Dodaj** z nagłówka kolumny **Akcja** aby dodać warunek dla listy.

- **Akcje.** Istnieje wiele działań, które można podjąć w stosunku e-maili. Każde działanie ma z kolei kilka możliwych rozwiązań lub działań dodatkowych. Znajdź je opisane tutaj:

Główne akcje:

- **Dostarcz e-maile.** Wykryte e-maile docierają do skrzynek odbiorców.
- **Kwarantanna.** Wiadomości zostają zaszyfrowane i zapisane w katalogu kwarantanny dla Serwera Exchange, bez dostarczania jej do odbiorcy. Możesz zarządzać kwarantanną e-maili na stronie **Kwarantanna**.
- **Przekierowanie e-maili.** Wiadomości mailowe nie zostają dostarczone do odbiorców docelowych, ale do skrzynki, którą zdefiniujemy w odpowiednim polu.
- **Odrzuć / Usuń email.** Na serwerze z rolą Edge Transport, wykryty email jest odrzucany wraz z kodem błędu 550 SMTP. W każdym innym przypadku, wiadomość email jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.

Działania drugorzędne:

- **Oznacz temat e-maila jako.** Możesz dodać etykietę do tematu wykrytego e-maila, aby pomóc użytkownikowi filtrowanie wiadomości w kliencie poczty.
- **Dodaj nagłówek do wiadomości e-mailowych.** Możesz nadać nazwę nagłówka i jego wartość w wykrytej wiadomości poprzez wprowadzenie żądanych wartości w odpowiednich polach.
- **Zapisz wiadomość na dysk.** Kopia wykrytego maila jest zapisywana jako plik w określonym folderze na Serwerze Exchange. Jeśli katalog nie istnieje, zostanie utworzony. Musisz dostarczyć kompletną ścieżkę do katalogu w odpowiednim polu.

  Notatka
  Ta opcja wspiera tylko e-maile w formacie MIME.

- **Archiwizuj na koncie.** Kopia wykrytego e-maila jest dostarczana na określony adres mailowy. To działanie dodaje określony adres mailowy do listy e-mailowej Bcc.

- Domyślnie, jeżeli wiadomość email pasuje do warunków zasady, nie jest więcej sprawdzany pod kątem innych warunków. Jeżeli chcesz kontynuować zasady przetwarzania, odznacz pole wyboru **Jeśli warunki reguły są spełnione, przerwij przetwarzanie kolejnych reguł**.

Wykluczenia

Jeżeli chcesz by dla konkretnych grup nadawców i odbiorców nie obowiązywały zasady filtrowania zawartości możesz zdefiniować wyłączenie filtrowania.

Aby utworzyć wyjątek:

1. Kliknij łącze **Wykluczenia** zaraz obok pola wyboru **Filtrowanie Zawartości**. Ta akcja otwiera okno konfiguracyjne.
2. Wprowadź adres email zaufanego nadawcy i/lub odbiorców w odpowiednich polach. Każdy email pochodzacy od zaufanego nadawcy lub wysłany do zaufanego odbiorcy został wykluczony z filtrowania. Podczas edycji listy, można również użyć następujących symboli wieloznacznych w celu określenia całej domeny e-mail lub wzoru dla adresów e-mail:
   - Gwiazdka (*), zastępując zero, jeden lub więcej znaków.
   - Znak zapytania (?), zastępuje dowolny pojedynczy znak.

   Na przykład, jeśli wprowadzisz `*.gov`, wszystkie maile przychodzące z domeny `.gov` będą zaakceptowane.
3. Dla wiadomości e-mail posiadających wielu odbiorców, możesz zaznaczyć pole wyboru **Wyklucz filtrowanie e-maili tylko, gdy wszyscy odbiorcy są zaufani** aby zastosować wykluczenie tylko, gdy wszyscy odbiorcy są zawarci na liście zaufanych odbiorców.
4. Kliknij **Zapisz**.

Filtrowanie załączników

Moduł Filtrowania załączników oferuje funkcję filtrowania załączników. Może on wykryć załączniki o konkretnym wzorcu nazwy lub o konkretnym typie. Używając filtrowania załączników możemy:

- Zablokować potencjalnie niebezpieczne załączniki, takie jak pliki `.vbs` lub `.exe` lub maile zawierające je.
- Blokować załączniki posiadające obraźliwe nazwy lub maile zawierające takie treści.

Umożliwianie filtrowania załączników

Jeśli chcesz użyć filtrowania załączników, zaznacz pole wyboru **Filtrowanie załączników**.

Do tworzenia i zarządzania zasadami filtrowania załączników odnieś się do „Zarządzanie regułami filtrowania” (p. 370).

Opcje Zasad

- **Ogólny.** W tej sekcji musisz ustalić nazwę dla zasady, w innym wypadku nie będziesz w stanie jej zapisać. Wybierz pole wyboru **Aktywny** jeśli chcesz by reguła obowiązywała po zapisaniu polityki.

- **Zakres reguł.** Możesz ograniczyć zasadę do stosowania się tylko i wyłącznie do podzbioru e-maili poprzez łączne ustawienie następujących opcji zakresu:
  - **Odnoszenie się do kierunku.** Wybierz kierunek ruchu e-mail, do których ma zostać zastosowana reguła.
  - **Nadawcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko wybranych nadawców. By zawężyć zakres nadawców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Spójrz na wybrane grupy w tabeli po prawej stronie.
  - **Odbiorcy.** Możesz zadecydować czy zasady mają odnosić się do wszystkich, czy tylko do wybranych odbiorców. By zawężyć zakres odbiorców, kliknij przycisk **Specyficzny** oraz wybierz pożądaną grupę z tabeli po lewej stronie. Możesz przeglądać wybrane grupy w tabeli po prawej stronie.

    Zasada obowiązuje, jeśli któryś z adresatów pasuje do twojego wyboru. Jeśli chcesz zastosować regułę tylko wtedy gdy wszyscy odbiorcy są w wybranych grupach, wybierz **Dopasuj wszystkich odbiorców**.

    Notatka
    Adresy w polach **Cc** i **Bcc** również liczą się jako odbiorcy.

    WAŻNE
    Zasady oparte na grupach użytkowników są stosowane tylko do Hub Transportu i Skrzynek e-mail.

- **Ustawienia.** Określ pliki które są dozwolone lub zabronione w załącznikach e-maili.

  Możesz filtrować załączniki e-maili na podstawie typu pliku lub na podstawie nazwy pliku.

  Aby odfiltrować załączniki w kryterium typów plików, wykonaj następujące kroki:
  1. Wybierz pole wyboru **Wykryj pod kątem typu zawartości**.
  2. Wybierz opcję wykrywania, która jest najbardziej odpowiednia dla Twoich potrzeb:
     - **Tylko następujące kategorie**, gdy masz ograniczoną listę kategorii typów zakazanych kategorii.
     - **Wszystko poza następującymi kategoriami**, gdy masz ograniczoną listę kategorii typów dopuszczonych kategorii.

3. Wybierz kategorię typu pliku twojego zainteresowania z dostępnych na liście. Szczegółowe informacje na temat rozszerzeń z każdej kategorii, uzyskasz odwołując się do „Typy plików filtrowania załączników” (p. 517).

   Jeśli jesteś zainteresowany tylko niektórymi typami plików, zaznacz pole wyboru **Niestandardowe rozszerzenia** i wprowadź listę rozszerzeń we odpowiednim polu.
4. Zaznacz pole wyboru **Włącz wykrywanie poprawnego typu** by sprawdzić nagłówki plików i prawidłowo zidentyfikować załączniki typów plików gdy skanowanie posiada ograniczone rozszerzenia. Oznacza to że rozszerzenie nie może być po prostu nazwane inaczej w celu ominięcia zasady filtrowania załączników.

> **Notatka**
> Wykrywanie prawdziwego typu może być zasobochłonne.

Aby przefiltrować załączniki po ich nazwach, zaznacz pole wyboru **Wykryj po nazwie pliku** i wprowadź w odpowiednim polu nazwę pliku, który chcesz przefiltrować. Podczas edycji listy, możesz również użyć następujących symboli wieloznacznych w celu określenia wzorów:

– Gwiazdka (*), zastępując zero, jeden lub więcej znaków.
– Znak zapytania (?), zastępuje dowolny pojedynczy znak.

Na przykład, jeżeli wprowadzisz `database.*`, wszystkie pliki nazwane `database`, bez względu na rozszerzenie zostaną wykryte.

> **Notatka**
> Jeśli włączysz zarówno typ zawartości i wykrywanie nazwy pliku (bez wykrywania prawdziwego typu pliku), plik musi jednocześnie spełniać warunki dla obu typów wykrycia. Dla przykładu, wybierasz kategorię **Multimedia** i wprowadzasz nazwę pliku `test.pdf`. W tym wypadku e-maila pomijana jest ta reguła, ponieważ plik PDF nie jest plikiem multimedialnym.

Zaznacz pole wyboru **Skanuj wewnątrz archiwów**, aby zapobiec, by zablokowane pliki były ukryte w pozornie nieszkodliwych archiwach, a tym samym przekazując reguły filtrowania.

Skanowanie jest rekurencyjne wewnątrz archiwów i domyślnie przechodzi do czwartego poziomu głębokości archiwum. Możesz zoptymalizować skanowanie, jak opisano tutaj:

1. Wybierz pole wyboru **Maksymalna głębokość archiwum (poziomy)**.
2. Wybierz inną wartość z odpowiedniego menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.

Notatka
Jeśli wybrałeś, aby skanować archiwa, **Skanowanie wewnątrz archiwów** jest wyłączone i wszystkie archiwa są skanowane.

- **Akcje.** Jest kilka akcji, które możesz podjąć w celu wykrycia załączników lub wiadomości zawierających je. Każde działanie ma z kolei kilka możliwych rozwiązań lub działań dodatkowych. Znajdź je opisane tutaj:

  Główne akcje:
  - **Zastąp plik.** Kasuje wykryty plik i zastępuje go plikiem tekstowym, który informuje użytkownika o podjętych czynnościach.

    Aby skonfigurować tekst powiadomienia:
    1. Kliknij link **Ustawienia** zaraz obok pola wyboru **Filtrowanie załącznika**.
    2. Wprowadź tekst powiadomienia tekstowego w odpowiednim polu.
    3. Kliknij **Zapisz**.
  - **Skasuj plik.** Kasuje wykryte pliki bez wcześniejszego ostrzeżenia. Wskazane jest, aby unikać tego działania.
  - **Odrzuca/Kasuje e-maile.** Na serwerze z rolą Edge Transport, wykryte e-maile są odrzucane wraz z kodem błędu SMTP 550. W każdym innym przypadku, wiadomość email jest kasowana bez ostrzeżenia. Wskazane jest, aby unikać tego działania.
  - **Kwaranta e-maili.** Wiadomość zostaje zaszyfrowana i zapisana w katalogu kwarantanny dla Serwera Exchange, bez dostarczania jej do odbiorcy. Możesz zarządzać kwarantanną e-maili na stronie **Kwarantanna**.
  - **Przekierowanie e-maili.** E-mail nie zostaje dostarczony do adresata, ale na adres mailowy określony w odpowiednim polu.
  - **Dostarcz e-mail.** Zezwala na przepuszczenie wiadomości e-mail.

  Działania drugorzędne:
  - **Oznacz temat e-maila jako.** Możesz dodać etykietę do tematu wykrytego e-maila, aby pomóc użytkownikowi filtrowanie wiadomości w kliencie poczty.

- **Dodaj nagłówek do wiadomości e-mailowych.** Możesz dodać nazwę nagłówka i jego wartość w wykrytej wiadomości poprzez wprowadzenie żądanych wartości w odpowiednich polach.
- **Zapisz e-mail na dysk.** Kopia e-maila zawierającego wykrycie jest zapisywana jako plik w określonym folderze na serwerze Exchange. Jeśli katalog nie istnieje, zostanie utworzony. Musisz dostarczyć kompletną ścieżkę do katalogu w odpowiednim polu.

  Notatka
  Ta opcja wspiera tylko e-maile w formacie MIME.

- **Archiwizuj na koncie.** Kopia wykrytego e-maila jest dostarczana na określony adres mailowy. To działanie dodaje określony adres mailowy do listy e-mailowej Bcc.

- Domyślnie, gdy email pasuje do zakresu reguł, jest przetwarzany wyłącznie ze zgodnymi zasadami, bez sprawdzania pod kątem wszelkich innych zasad. Jeśli chcesz kontynuować sprawdzanie pod kątem innych zasad, wyczyść pole wyboru **Jeżeli warunki reguł są dopasowane, wstrzymaj przetwarzanie kolejnych reguł**.

Wykluczenia

Jeśli chcesz by ruch e-maili dla konkretnych nadawców i odbiorców nie był blokowany bez względu na zasady filtrowania załączników, możesz zdefiniować wyłączenia filtrowania.

Aby utworzyć wyjątek:

1. Kliknij łącze **Wykluczenia** zaraz obok pola wyboru **Filtrowanie Zawartości**. Ta akcja otwiera okno konfiguracyjne.
2. Wprowadź adres email zaufanego nadawcy i/lub odbiorców w odpowiednich polach. Każdy email pochodzacy od zaufanego nadawcy lub wysłany do zaufanego odbiorcy został wykluczony z filtrowania. Podczas edycji listy, można również użyć następujących symboli wieloznacznych w celu określenia całej domeny e-mail lub wzoru dla adresów e-mail:
   - Gwiazdka (*), zastępując zero, jeden lub więcej znaków.
   - Znak zapytania (?), zastępuje dowolny pojedynczy znak.

   Na przykład, jeśli wprowadzisz `*.gov`, wszystkie maile przychodzące z domeny `.gov` będą zaakceptowane.

3. Dla wiadomości e-mail posiadających wielu odbiorców, możesz zaznaczyć pole wyboru **Wyklucz filtrowanie e-maili tylko, gdy wszyscy odbiorcy są zaufani** aby zastosować wykluczenie tylko, gdy wszyscy odbiorcy są zawarci na liście zaufanych odbiorców.
4. Kliknij **Zapisz**.

7.2.12. Szyfrowanie

Notatka
Ten moduł jest dostępny dla:

- Windows dla stacji roboczych
- Windows dla serwerów
- macOS

Moduł szyfrowania zarządza pełnym szyfrowaniem dysku na punktach końcowych, wykorzystując odpowiednio BitLocker na Windows i FileVault oraz narzędzie wiersza poleceń diskutil na macOS.

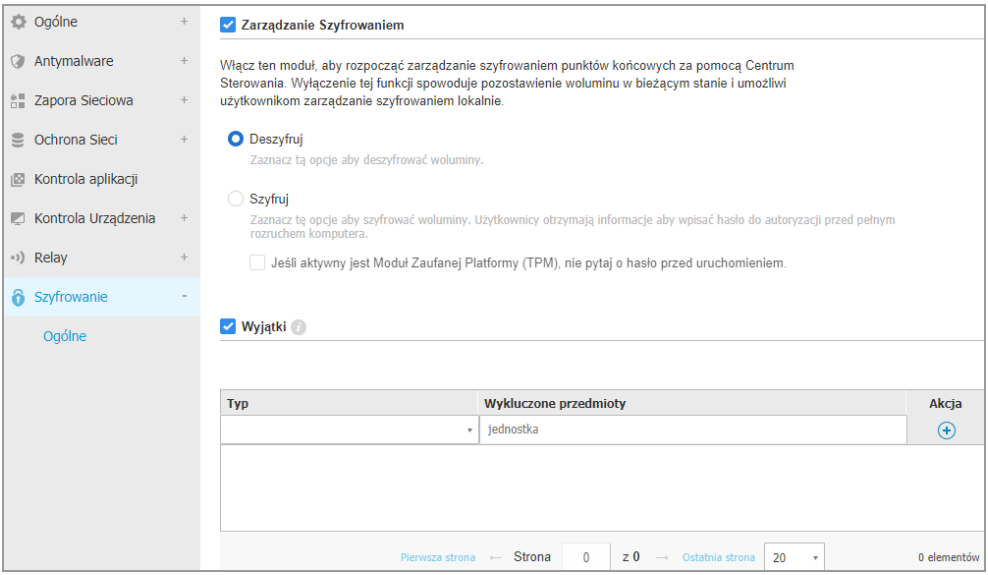
Dzięki temu GravityZone jest w stanie zapewnić stałe korzyści:

- Dane zabezpieczone w przypadku zgubienia lub kradzieży urządzeń
- Szeroka ochrona najpopularniejszych platform komputerowych na świecie dzięki zastosowaniu zalecanych standardów szyfrowania przy pełnym wsparciu Microsoft i Apple.
- Minimalny wpływ na wydajność punktów końcowych dzięki rodzimym narzędziom szyfrującym.

Moduł szyfrowania obsługuje następujące rozwiązania:

- BitLocker wersja 1.2 i nowsza, w punktach końcowych systemu Windows z modułem TPM (Moduł Zaufanej Platformy), dla woluminów rozruchowych i innych.
- BitLocker wersja 1. 2 i nowsza, w punktach końcowych systemu Windows bez modułu TPM, dla woluminów rozruchowych i innych.
- Sejf plików na punktach końcowych systemu MacOS, dla woluminów rozruchowych.
- narzędzie dyskowe na punktach końcowych systemu MacOS, dla woluminów innych niż rozruchowe.

Lista systemów operacyjnych obsługiwanych przez moduł szyfrowania znajduje się w Instrukcji instalacji GravityZone.



Strona szyfrowania

Aby rozpocząć zarządzanie szyfrowaniem punktów końcowych z Control Center, zaznacz pole wyboru **Zarządzanie szyfrowaniem**. Dopóki to ustawienie jest włączone, użytkownicy punktów końcowych nie mogą lokalnie zarządzać szyfrowaniem, a wszystkie ich działania zostaną anulowane lub przywrócone. Wyłączenie tego ustawienia pozostawi woluminy punktów końcowych w ich bieżącym stanie (zaszyfrowane lub niezaszyfrowane), a użytkownicy będą mogli zarządzać szyfrowaniem na swoich komputerach.

Dostępne są trzy opcje do zarządzania procesem szyfrowania/deszyfrowania.

- **Odszyfruj** - odszyfrowuje woluminy i zachowuje je odszyfrowane, gdy na punktach końcowych aktywna jest polityka.
- **Szyfruj** - szyfruje woluminy i zachowuje je zaszyfrowane, gdy na punktach końcowych aktywna jest polityka.

  W opcji Szyfruj możesz zaznaczyć pole wyboru **Jeśli moduł Trusted Platform Module (TPM) jest aktywny, nie pytaj o hasło do szyfrowania** . To ustawienie

zapewnia szyfrowanie w punktach końcowych systemu Windows za pomocą modułu TPM, bez konieczności podawania hasła szyfrowania przez użytkowników. Aby uzyskać więcej informacji idź do „Woluminy Szyfrujące" (p. 383).

- **Wykluczenia**

GravityZone obsługuje metodę Standardowego Zaawansowanego Szyfrowania (AES) z kluczami 128 i 256-bitowymi do Windows i MacOS. Rzeczywisty używany algorytm szyfrowania zależy od konfiguracji systemu operacyjnego.

Notatka
GravityZone wykrywa i zarządza woluminami ręcznie szyfrowanymi za pomocą BitLocker, FileVault i diskutil. Aby rozpocząć zarządzanie tymi woluminami, agent bezpieczeństwa poprosi użytkowników punktu końcowego o zmianę kluczy odzyskiwania. W przypadku korzystania z innych rozwiązań szyfrowania, woluminy muszą zostać odszyfrowane przed zastosowaniem polityki GravityZone.

Woluminy Szyfrujące

Aby zaszyfrować woluminy:

1. Zaznacz pole wyboru **Szyfrowanie** .
2. Wybierz opcję **Szyfruj**.

Proces szyfrowania rozpoczyna się, gdy polityka staje się aktywna na punktach końcowych, z pewnymi cechami charakterystycznymi w systemach Windows i Mac.

Dla Windows

Agent zabezpieczeń domyślnie poprosi użytkowników o skonfigurowanie hasła, aby rozpocząć szyfrowanie. Jeśli komputer ma funkcjonalny moduł TPM, aby rozpocząć szyfrowanie, agent bezpieczeństwa poprosi użytkowników o skonfigurowanie osobistego numeru identyfikacyjnego (PIN). Użytkownik musi wprowadzić hasło skonfigurowane na tym etapie przy każdym uruchomieniu urządzenia, na ekranie uwierzytelniania przed uruchomieniem.

Notatka
Agent bezpieczeństwa umożliwia skonfigurowanie wymagań dotyczących złożoności kodu PIN oraz uprawnień użytkowników do zmiany kodu PIN poprzez ustawienia polityki grupy BitLocker (GPO).

Aby rozpocząć szyfrowanie bez podawania hasła przez użytkownika, zaznacz pole wyboru **Jeśli aktywny jest moduł Zaufanej Platformy (TPM), nie pytaj o hasło przed uruchomieniem**. To ustawienie jest zgodne z punktami końcowymi systemu Windows mającymi TPM i UEFI.

Gdy pole wyboru **Jeśli Moduł Platformy Zaufanej (TPM) jest aktywny, nie pytaj o hasło przed uruchomieniem systemu** jest włączone:

- Na niezaszyfrowanym punkcie końcowym:
  - Szyfrowanie przebiega bez konieczności podawania hasła.
  - Ekran autoryzacji przed uruchomieniem nie pojawia się podczas uruchamiania urządzenia.
- Na punkcie końcowym zaszyfrowanym hasłem:
  - Hasło zostało usunięte.
  - Wolumin pozostaje niezaszyfrowany.
- Zaszyfrowany lub nieszyfrowany punkt końcowy, przy czym moduł TPM nie został wykryty lub nie działa:
  - Użytkownik jest proszony o podanie hasła do szyfrowania.
  - Ekran autoryzacji przed uruchomieniem pojawia się podczas uruchamiania urządzenia.

Gdy pole wyboru **Jeśli Moduł Platformy Zaufanej (TPM) jest aktywny, nie pytaj o hasło przed uruchomieniem systemu** jest włączone:

- Aby rozpocząć szyfrowanie, użytkownik musi podać hasło.
- Wolumin pozostaje niezaszyfrowany.

Dla Mac

Aby rozpocząć szyfrowanie na woluminach rozruchowych, agent bezpieczeństwa poprosi użytkowników o wprowadzenie poświadczeń systemowych. Tylko użytkownicy posiadający lokalne konta z uprawnieniami administratora mogą włączyć szyfrowanie.

Aby rozpocząć szyfrowanie na woluminach nierozruchowych, agent bezpieczeństwa poprosi użytkowników o skonfigurowanie hasła szyfrowania. To hasło będzie wymagane do odblokowania woluminu bez rozruchu przy każdym uruchomieniu komputera. Jeśli komputer ma więcej niż jeden wolumin nierozruchowy, użytkownicy muszą skonfigurować hasło szyfrowania dla każdego z nich.

Woluminy Odszyfrowujące

Aby odszyfrować woluminy na punktach końcowych:

1. Zaznacz pole wyboru **Szyfrowanie** .
2. Wybierz opcję **Odszyfruj**.

Proces odszyfrowania rozpoczyna się, gdy polityka staje się aktywna na punktach końcowych, z pewnymi cechami charakterystycznymi w systemach Windows i Mac.

Dla Windows
Woluminy są odszyfrowywane bez interakcji użytkowników.

Dla Mac
W przypadku woluminów rozruchowych użytkownicy muszą wprowadzić swoje poświadczenia systemowe. W przypadku woluminów nierozruchowych użytkownicy muszą wprowadzić hasło skonfigurowane podczas procesu szyfrowania.

W przypadku gdy użytkownicy punktu końcowego zapomną swoich haseł szyfrowania, potrzebują kluczy odzyskiwania do odblokowania swoich maszyn. Szczegółowe informacje na temat pobierania kluczy odzyskiwania można znaleźć w „” (p. 105).

Wykluczanie Partycji

Możesz stworzyć listę wyjątków od szyfrowania dodając literę dysku, etykiety i nazwy partycji i GUID partycji. Aby stworzyć regułę wykluczania partycji z szyfrowania:

1. Wybierz pole **Wykluczenia**.
2. Kliknij **Typ** i wybierz typ dysku z rozwijanego menu.
3. Wprowadź wartość dysku w polu **Wykluczone obiekty** i rozważ następujące warunki:
   - Dla **Litery Dysku** wprowadź `D:` lub literę dysku z dwukropkiem na końcu.
   - Dla **Etykiety/Nazwy** możesz wprowadzić dowolną etykietę, taką jak `Praca`.
   - Dla **GUID** partycji wprowadź wartość w następujący sposób `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.
4. Kliknij **Dodaj** ⊕ aby dodać wyjątek do listy.

Aby usunąć wyjątek, wybierz obiekt i klinij **Usuń** ⊗.

7.2.13. NSX

W tej sekcji można ustalić politykę, która ma być używana jako profil bezpieczeństwa w NSX. Aby to zrobić:

1. Zaznacz **NSX** pole wyboru, aby ustawić jego widoczność, także w vSphere Client Web.
2. Wpisz nazwę, pod którą będzie można zidentyfikować politykę NSX. Nazwa ta może się różnić od nazwy polityki w GravityZone Control Center. W vSphere pojawi się poprzedzony prefiksem `Bitdefender_`. Wybierz tę nazwę rozsądnie, aby można było ją odczytać po zapisaniu polityki.

7.2.14. Ochrona pamięci

Notatka
Ochrona pamięci masowej jest dostępna dla urządzeń pamięci masowej podłączonych do sieci (NAS) i rozwiązań do udostępniania plików zgodnych z protokołem Internet Content Adaptation Protocol (ICAP).

W tej sekcji możesz skonfigurować Security Server jako usługę skanowania urządzeń NAS i rozwiązań udostępniania plików zgodnych z ICAP, takich jak pliki Nutanix i Citrix ShareFile.

Security Server skanuje dowolne pliki, w tym archiwa, na żądanie urządzeń pamięci masowej. W zależności od ustawień, Security Server podejmują odpowiednie działania na zainfekowanych plikach, takich jak dezynfekcja lub odmowa dostępu.

Ustawienia są zorganizowane w poniższych sekcjach:

- ICAP
- Wykluczenia

ICAP

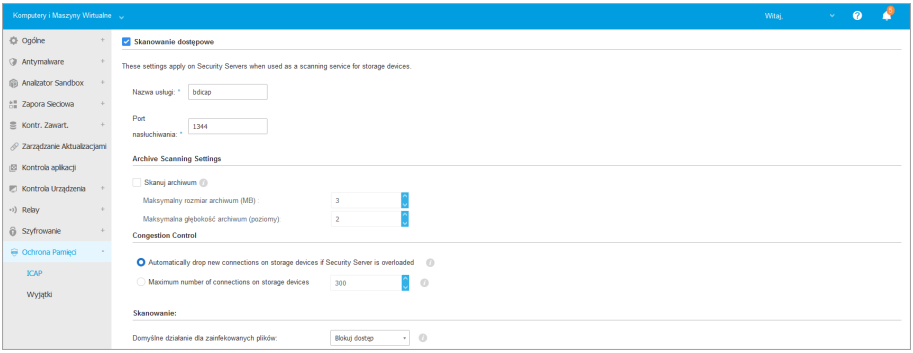
Możesz skonfigurować następujące opcje dla Security Server:

- Zaznacz pole wyboru **SkanowanieDostępowe**, aby włączyć moduł Ochronay Pamięci. Wymagane ustawienia komunikacji między Security Server a urządzeniami pamięci są wstępnie zdefiniowane w następujący sposób:
  - Nazwa usługi: `bdicap`.
  - Port: `1344`.

- W **Ustawienia Skanowania Archiwum** zaznacz pole wyboru **Skanuj Archiwum**, aby włączyć skanowanie archiwów. Skonfiguruj maksymalny rozmiar i maksymalną głębokość skanowanych archiwów.

  Notatka
  Jeśli ustawisz maksymalny rozmiar archiwum na 0 (zero), Security Server skanuje archiwa niezależnie od ich wielkości.

- Pod **Kontrola Przeciążeń** wybierz preferowaną metodę zarządzania połączeniami na urządzeniach magazynujących w przypadku przeciążenia Security Server:
  - **Automatycznie usuwaj nowe połączenia z urządzeń pamięci, jeśli Security Server jest przeciążony**. Kiedy jeden Security Server osiągnie maksymalną liczbę połączeń, urządzenie pamięci przekieruje nadwyżkę do drugiego Security Server.
  - **Maksymalna liczba połączeń na urządzeniach pamięci masowej**. Domyślną wartością jest 300 połączeń.
- W obszarze **Działania Skanowania** dostępne są następujące opcje:
  - **Odmów dostępu** - Security Server odmawia dostępu do zainfekowanych plików.
  - **Dezynfekuj** - Security Server usuwa kod złośliwego oprogramowania z zainfekowanych plików.



Polityki - Ochrona Pamięci - ICAP

Wykluczenia

Jeśli chcesz, aby określone obiekty zostały wykluczone ze skanowania, zaznacz pole wyboru **Wykluczenia**.

Możesz zdefiniować wyjątki:

- Według hasha - identyfikujesz wykluczony plik według hasha SHA-256.
- Według symbolu wieloznacznego - identyfikujesz wykluczony plik według ścieżki.

Konfigurowanie Wykluczeń

Aby dodać wyjątek:

1. Wybierz rodzaje wyjątków z menu.
2. Zależnie od rodzaju wyjątku, określ obiekt jaki ma być wykluczony według poniższych zaleceń:
   - **Hash** - wprowadź skróty SHA-256 oddzielone przecinkami.
   - **Symbol wieloznaczny** - podaj absolutną lub względną ścieżkę, używając znaków wieloznacznych. Symbol gwiazdki (*) dopasowuje dowolny plik wewnątrz katalogu. Znak zapytania (?) zastępuje dokładnie jeden znak.
3. Dodaj opis wykluczenia.
4. Kliknij przycisk ⊕ **Dodaj** . Do listy zostanie dodana nowy wyjątek.

Aby usunąć zasadę z listy, kliknij odpowiadający jej przycisk ⊗ **Usuń**.

Importowanie i Eksportowanie Wyjątków

Jeśli zamierzasz ponownie użyć wykluczeń w większej liczbie polityk, możesz je eksportować i importować.

Aby eksportować wykluczenia:

1. Kliknij **Eksportuj** w górnej części tabeli wykluczeń.
2. Zapisz plik CSV na swoim komputerze. W zależności od twoich ustawień przeglądarki, plik może być pobierany automatycznie lub zostaniesz poproszony, aby go zapisać do lokalizacji.

Każdy wiersz w pliku CSV odpowiada pojedynczemu wykluczeniu, mającemu pola w następującej kolejności:

```
<exclusion type>, <object to be excluded>, <description>
```

Oto dostępne wartości dla pól CSV:

Typ wyjątku:
`1`, dla hasha SHA-256

`2`, dla symboli wieloznacznych

Obiekt jaki ma być wykluczony:
Wartość skrótu lub nazwa ścieżki

Opis
Tekst pomagający zidentyfikować wykluczenie.

Przykład wykluczeń w pliku CSV:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

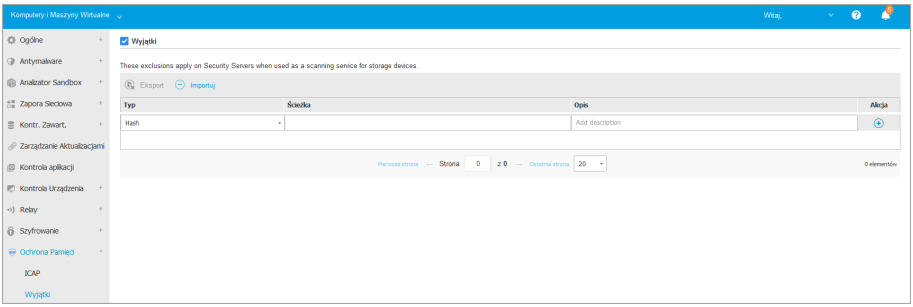
Aby importować wykluczenia:

1. Kliknij opcję **Importuj**. Otwiera sie okno **Importuj Wyjątki Polityk**.
2. Kliknij **Dodaj**, a następnie wybierz plik CSV.
3. Kliknij **Zapisz**. Tabela zawiera ważne wyjątki. Jeśli plik CSV zawiera nieprawidłowe wykluczenia, ostrzeżenie informuje o odpowiednich numerach wierszy.

Edycja Wykluczeń

Aby edytować wykluczenia:

1. Kliknij nazwę wykluczenia w kolumnie **Ścieżka** lub opis.
2. Edytuj wykluczenie.
3. Po zakończeniu naciśnij `Wprowadź`.



Polityki - Ochrona Pamięci - ICAP

7.3. Polityki Urządzenia Przenośnego

Ustawienia polityki mogą zostać wstępnie skonfigurowane podczas tworzenia polityki. Później, możesz je zmienić, w zależności od potrzeb, kiedy tylko chcesz.

Aby skonfigurować ustawienia polityki:

1. Przejdź do strony **Polityki**.
2. Wybierz **Urządzenia Mobilne** z selektor odsłon.
3. Naciśnij nazwę polityki. To otworzy stronę ustawień polityki.
4. Skonfiguruj ustawienia polityki według uznania. Ustawienia pogrupowano w następujące kategorie:
   - Ogólne
     - Szczegóły
   - Zarządzanie urządzeniami
     - Bezpieczeństwo
     - Hasło
     - Tryby

   Możesz wybrać kategorię ustawień używając menu po lewej stronie.
5. Naciśnij **Zapisz** aby zapisać zmiany i zastosować je na urządzeniach przenośnych. Aby opuścić stronę polityki bez zapisywania zmian, naciśnij **Anuluj**.

7.3.1. Ogólne

Kategoria **Ogólne** zawiera opisowe informacje na temat wybranej polityki.

Szczegóły

Strona Szczegółów wyświetla ogólne szczegóły polityki:

- Nazwa polityki
- Użytkownik, który stworzył politykę
- Data i czas utworzenia polityki.
- Data i czas ostatniej modyfikacji polityki

Możesz zmienić nazwę polityki poprzez dodanie nowej nazwy w odpowiednim polu. Polityki powinny mieć sugestywne nazwy tak by administratorzy mogli szybko je zidentyfikować.

Notatka
Domyślnie, tylko użytkownik, który stworzył politykę może ją modyfikować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

7.3.2. Zarządzanie urządzeniami

Ustawienia zarządzania urządzeniami pozwalają na zdefiniowanie opcji bezpieczeństwa dla urządzeń przenośnych, blokowanie ekranu hasłem i kilku profili dla każdej polityki urządzenia przenośnego.

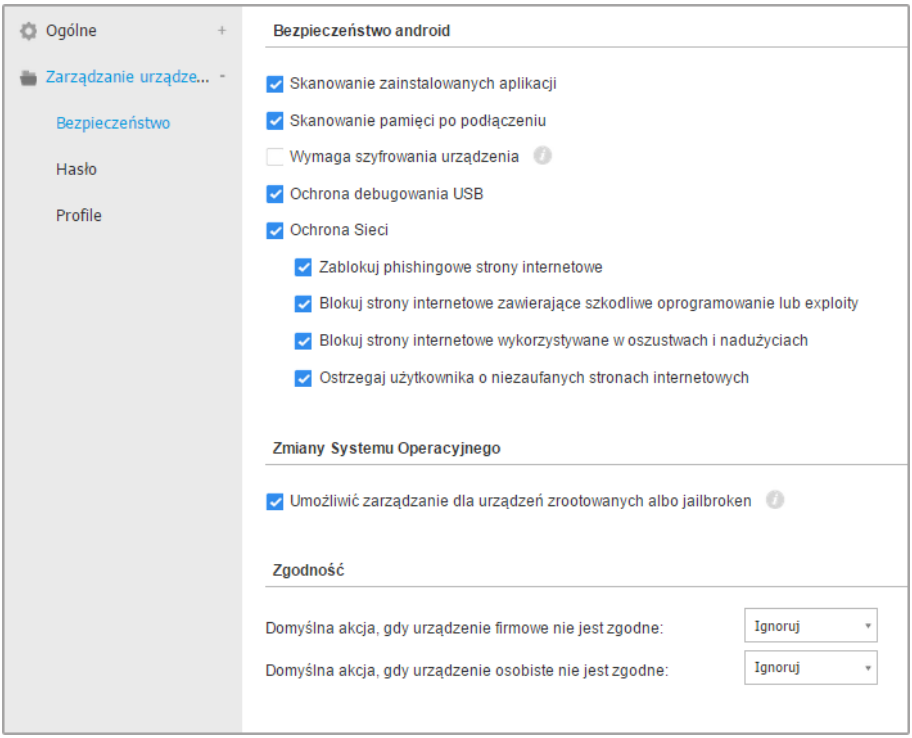
Ustawienia są zorganizowane w poniższych sekcjach:

- Bezpieczeństwo
- Hasło
- Tryby

Bezpieczeństwo

W tej sekcji możesz skonfigurować różne ustawienia bezpieczeństwa dla urządzeń przenośnych, wliczając w to skanowanie antymalware dla urządzeń Android, zarządzania urządzeniami zrootowanymi i po jailbreaku lub działaniami na niezgodnych urządzeniach.

WAŻNE
Skanowanie antymalware odbywa się w chmurze, dlatego urządzenia przenośne muszą mieć dostęp do internetu.



Polityki urządzeń Przenośnych - ustawienia Bezpieczeństwa

Bezpieczeństwo android

- Wybierz **Skanuj aplikacje w trakcie instalacji** jeżeli chcesz uruchomić skanowanie, gdy chcesz uruchomić skanowanie w trakcie instalacji nowych aplikacji na zarządzanych urządzeniach przenośnych.
- Wybierz **Skanowanie zamontowanego dysku** jeżeli chcesz rozpocząć skanowanie każdego zamontowanego dysku.

Ostrzeżenie

Jeżeli znaleziono złośliwe oprogramowanie, użytkownik zostanie powiadomiony aby je usunąć. Jeżeli użytkownik nie usunie wykrytego malware przez godzinę od wykrycia, urządzenie przenośne zostaje uznane za niezgodne i automatyczne

zostaje zastosowane wybrane działanie wykonywane przy niezgodności (Ignoruj, Zabroń Dostępu, Zablokuj, Wyczyść, Odłącz).

- Wybierz **Wymagane szyfrowanie urządzenia** aby powiadomić użytkownika aby aktywował funkcję szyfrowania dostępną w systemie Android. Szyfrowanie chroni dane przechowywane na urządzeniach z Androidem, łącznie z kontami, ustawieniami, pobranymi aplikacjami, mediami i innymi plikami, z nieautoryzowanym dostępem. do zaszyfrowanych danych można uzyskać dostęp tylko z zewnętrznych urządzeń, używając hasła do odblokowania.

  WAŻNE

  – Szyfrowanie urządzenia jest dostępne od systemu Android 3.0 albo nowszego. Nie wszystkie modele urządzeń wspierają szyfrowanie. Sprawdź okno **Szczegóły Urządzenia Przenośnego** aby zobaczyć informacje o wsparciu dla szyfrowania.

  – Szyfrowanie może wpłynąć na wydajność urządzenia.

  Ostrzeżenie

  – Szyfrowanie urządzenia jest nieodwracalne, a jedynym sposobem, aby powrócić do stanu niezaszyfrowanego jest wyczyszczenie urządzenie.

  – Użytkownicy powinni zrobić kopię zapasową swoich danych przed aktywacją szyfrowania urządzenia.

  – Użytkownicy nie powinni zakłócać szyfrowania plików, ponieważ mogą stracić niektóre albo wszystkie dane.

  Jeżeli włączysz tę opcję, GravityZone Mobile Client wyświetli się trwały powiadomienie informujące użytkownika aby aktywował szyfrowanie. Użytkownik musi nacisnąć przycisk **Rozwiąż** aby przejść do ekranu szyfrowania i rozpocząć proces. Jeżeli szyfrowanie nie zostało aktywowane przez siedem dni od otrzymania powiadomienia, urządzenie będzie niezgodne.

  Aby włączyć szyfrowanie na urządzeniu Android:

  – Bateria musi być w 80% naładowana.

  – Urządzenie musi być podłączone do czasu zakończenia szyfrowania.

  – Użytkownik musi ustawić hasło odblokowania spełniające wymogi złożoności.

Notatka

- Urządzenia Android używają tego samego hasła do odblokowania ekranu i odblokowania szyfrowania zawartości.
- Szyfrowanie wymaga hasła, PIN lub FACE aby odblokować urządzenie, blokując inne ustawienia blokowania ekranu.

Proces szyfrowania może zająć godzinę albo dłużej, podczas których urządzenie może restartować się kilka razy.

Możesz sprawdzić status szyfrowanie dysku dla każdego urządzenia przenośnego w oknie **Szczegóły urządzenia przenośnego**.

- Urządzenia Android podczas debugowania USB mogą być połączone z PC przez kabel USC, dopuszczający zaawansowaną kontrolę nad ich aplikacjami i systemem operacyjnym. W tym przypadku, bezpieczeństwo urządzeń przenośnych może być zagrożone. Domyślnie włączona opcja **Ochrona debugowania USB** uniemożliwia korzystanie z urządzeń w trybie debugowania USB. Jeżeli użytkownik aktywuje debugowanie USB, urządzenie automatycznie staje się niezgodne i zostają podjęte niezgodne działania. Jeżeli niezgodnym działaniem jest **Ignoruj**, użytkownik jest powiadamiany o niebezpiecznym ustawieniu.

  Jednak, można wyłączyć tę opcję dla urządzeń przenośnych, które wymagają pracy w trybie debugowania USB (takie jak urządzenia mobilne wykorzystywane do tworzenia i testowania aplikacji mobilnych).

- Wybierz **Bezpieczeństwo Sieci** aby włączyć funkcje zabezpieczenia sieci na urządzeniu Android.

  Zabezpieczenie sieci skanuje w chmurze każdy dostępny adres URL i zwraca status bezpieczeństwa do GravityZone Mobile Client. Status bezpieczeństwa URL może być: czysty, oszustwo, malware, phishing lub niezaufane.

  GravityZone Mobile Client może podjąć konkretne działania w oparciu o stan bezpieczeństwa URL:

  – **Zablokuj phishingowe strony internetowe**. Gdy użytkownik próbuje uzyskać dostęp do strony internetowej zawierającej phishing GravityZone Mobile Client blokuje dany adres URL i wyświetla zamiast niego stronę ostrzeżenia.

  – **Blokuj strony internetowe zawierające szkodliwe oprogramowanie lub exploity**. Gdy użytkownik próbuje uzyskać dostęp do strony internetowej

zawierającej malware lub exploity GravityZone Mobile Client blokuje dany adres URL i wyświetla zamiast niego stronę ostrzeżenia.

– **Blokuj strony internetowe wykorzystywane w oszustwach i nadużyciach**. Rozszerza ochronę na inne rodzaje oszustw niż phishing (na przykład fałszywe deppozty, fałszywe darowizny, zagrożenia w mediach społecznościowych i tak dalej). Gdy użytkownik próbuje uzyskać dostęp do oszukańczych strony internetowych GravityZone Mobile Client blokuje dany adres URL i wyświetla zamiast niego stronę ostrzeżenia.

– **Ostrzegaj użytkownika o niezaufanych stronach internetowych**. Gdy uzytkownik próbuje uzyskać dostęp do strony internetowej, która została wcześniej shakowana do celów phishingowych lub niedawno rozprowadzała wiadomości spamowe albo phishingowe, yświetli się komunikat ostrzegawczy pop-up, strona nie zostanie zablokowana.

WAŻNE
Funkcje Web Security działają tylko na Androidzie 5 i tylko z Chrome i wbudowaną przeglądarką Android.

Zmiany Systemu Operacyjnego

Rozpatrywane zagrożenie bezpieczeństwa dla sieci korporacyjnych, zrootowanych lub jailbreak urządzeń automatycznie są klasyfikowane jako niekompatybilne.

- Wybierz **Dopuść zarządzanie zrootowanymi i po jailbreaku urządzeniami** Jeżeli chcesz zarządzać tymi urządzeniami z Control Center. Należy zauważyć, że ponieważ takie urządzenia są domyślnie niezgodne, są automatycznie zastosowane wybrane Niezgodne działania tak długo jak są wykrywane. Dlatego aby móc zastosować ustawienia polityki bezpieczeństwa lub uruchomić zadania na nich, musisz ustawić aby ignorować niezgodne działania.
- Jeżeli wyczyściłeś pole wyboru przy **Dopuść zarządzanie urządzeniem zrootowanym lub po jailbreaku**, automatycznie odłączyłeś urządzenie zrootowane lub po jailbreaku z sieci GravityZone. W tym przypadku aplikacja GravityZone Mobile Client wyświetla komunikat informujący, ze urządzenie jest zrootowane / po jailbreaku. Użytkownik może nacisnąć przycisk OK, który przekierowuje do strony rejestracyjnej. Jak tylko urządzenie jest niezrootowane / nie jest po jailbreaku lub polityka jest ustawiona żeby dopuszczać zarządzanie zrootowanymi / po jailbreaku urządzeniami, może ono być ponownie włączone

(z tym samym tokenem dla urządzeń Android / z nowym tokenem dla urządzeń iOS).

Zgodność

Możesz skonfigurować określone działania, które maj,a zostać automatycznie wykonane na urządzeniach wykrytych jako niezgodne bazujących na własności urządzenia (enterprise lub personal).

Notatka
Podczas dodawania nowego urządzenia w Control Center, pojawi się monit aby określić właściciela urządzenia (enterprise lub personal). Pozwala GravityZone zarządzać urządzeniami przenośnymi osobistymi i przedsiębiorstwa osobno.

- Niezgodne kryteria
- Niezgodne akcje

Niezgodne kryteria

Urządzenie deklaruje niezgodność w następujących sytuacjach:

- **Urządzenia Android**
  - Urządzenie jest zrootowane.
  - GravityZone Mobile Client nie jest urządzeniem administratora.
  - Malware nie zostało usunięte przez godzinę od wykrycia.
  - Polityka nie spełnia:
    - Użytkownik nie ustawiał hasła blokowania ekranu przez 24 godziny po pierwszym powiadomieniu.
    - Użytkownik nie zmieniał hasła blokowania ekranu w określonym czasie.
    - Użytkownik nie aktywował szyfrowania urządzenia przez siedem dni po pierwszym powiadomieniu.
    - Debugowanie USB jest włączone na urządzeniu, gdy polityka ochrony debugowania USB jest włączona.
- **urządzenia iOS**
  - Urządzenie po jailbreaku.
  - GravityZone Mobile Client został odinstalowany z urzadzenia przenośnego.

- Polityka nie spełnia:
  - Użytkownik nie ustawiał hasła blokowania ekranu przez 24 godziny po pierwszym powiadomieniu.
  - Użytkownik nie zmieniał hasła blokowania ekranu w określonym czasie.

Domyślna akcja, gdy urządzenie nie jest zgodne

Kiedy urządzenie jest niezgodne, uzytkownik jest proszony, aby rozwiązać problem zgodności. Użytkownik musi wykonać wymaganych zmian w określonym czasie, w przeciwnym razie zostanie zastosowana wybrana akcja dla urządzeń niezgodnych (Ignorowanie, Odmowa Dostępu, Zablokowanie, Wyczyszczenie, Odłączenie).

Możesz zmienić akcje dla niezgodnych urządzeń w polityce w każdej chwili. Nowa akcja jest zastosowana w niezgodnym urządzeniu gdy polityka zostanie zapisana.

Wybierz z odpowiedniego menu rodzaj akcji dla każdego posiadanego urządzenia, która zostanie podjeta kiedy zostanie zdeklarowana niezgodność urządzenia:

- **Ignoruj**. Tylko powiadomienia użytkownika, że urządzenie nie jest zgodne z polityką użytkowania urządzenia przenośnego.
- **Blokuj dostęp**. Urządzenie blokuje dostęo do sieci korporacyjnych przez usunięcie Wi-Fi i ustawienia VPN, lub trzyma wszystkie inne ustawienia zdefiniowane w polityce. Ustawienia blokowania zostaną przywrócone gdy urządzenie będzie zgodne.

  WAŻNE
  Gdy urządzenie jest wyłączone dla GravityZone Mobile Client, urządzenie staje się niezgodne i automatycznie zostaje zastosowana akcja **Odmowa dostępu**.

- **Zablokuj**. Natychmiast blokuje ekran urządzenia.
  - W systemie Android ekran jest blokowany hasłem generowanym przez GravityZone tylko wtedy, gdy nie skonfigurowano zabezpieczenia blokady na urządzeniu. Nie spowoduje to zastąpienia już skonfigurowanej opcji ekranu blokady, takiej jak Wzór, PIN, Hasło, Odcisk Palca lub Smart Lock.
  - Na iOS, jeżeli urządzenie ma zablokowany ekran hasłem, użytkownik jest proszony o odblokowanie.
- **Wyczyść**. Przywracając ustawienia fabryczne urządzenia przenośnego, trwale usuwa wszystkie dane użytkownika.

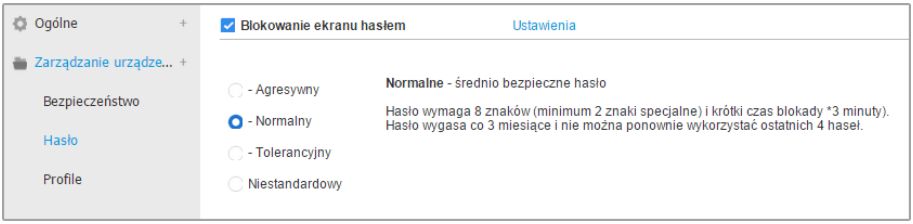
Notatka
Wyczyść nie usuwa danych z obecnie zamontowanych urządzeń (kart SD).

- **Odłącz**. Urządzenie jest natychmiast usuwane z sieci.

Notatka
Aby ponownie zarejestrować urządzenia przenośne, które zostało odłączone, musisz dodać urządzenie ponownie w Centrum Kontroli. Urządzenie musi zostać ponownie zarejestrowane nowym tokenem aktywacyjnym. Przed ponownym zapisaniem urządzenia, upewnij się, ze warunki, które doprowadziły do odłączenia urządzenia nie będą już działać lub zmień ustawienia polityki, aby umożliwić zarządzanie urządzeniem.

Hasło

W tej sekcji możesz wybrać, aby aktywować funkcję blokowania ekranu hasłem dostępną dla urządzeń przenośnych.



Polityki Urządzeń Przenośnych - Ustawienia Hasła Ochrony

Gdy ta funkcja zostanie włączona, na ekranie pojawi się powiadomienie dla użytkownika, żeby ustawił hasło blokowania ekranu. Użytkownik musi podać hasło zgodne z kryteriami hasła zdefiniowanymi w polityce. Hasło zostało ustawione przez użytkownika, wszystkie powiadomienia dotyczące tego problemu zostały wyczyszczone. Wiadomość zawiadamiająca o podaniu hasła wyświetli się za każdą próbą odblokwoania ekranu.

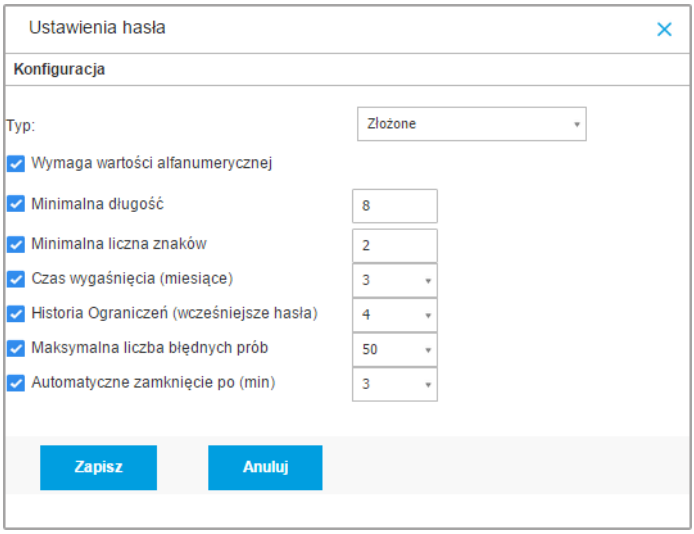
Notatka
Jeżeli użytkownik nie ustawi hasła, gdy jest o to proszony, urządzenie może być używane bez hasła blokowania ekranu przez 24 godziny od pierwszego

powiadomienia. Wiadomość o podaniu hasła blokowania ekranu będzie wyświetlana co 15 minut.

Ostrzeżenie
Jeżeli użytkownik nie ustawi hasła przez 24 godziny po pierwszym powiadomieniu, urządzenie przenośne stanie się niezgodne i zostanie zastosowana wybrana akcja dla niezgodnych urządzeń.

Aby skonfigurować ustawienia hasła blokowania ekranu:

1. Zaznacz pole wyboru **Hasło blokowania ekranu**.
2. Wybierz hasło poziomu bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.
3. dla zaawansownej konfiguracji, wybierz **Niestandardowy** poziom ochrony i naciśnij odnośnik **Ustawienia**.



Polityki urządzeń przenośnych - Ustawienia zaawansowane ochrony hasłem

Notatka

Aby zobaczyć wymagania konfiguracyjne hasła wcześniej zdefiniowanego poziomu bezpieczeństwa, wybierz poziom i naciśnij odnośnik **Ustawienia**. Jeżeli zmieniasz jakąś opcje, poziom bezpieczeństwa hasła zmieni się automatycznie na **Niestandardowy**.

Opcje Niestandardowe.

- **Typ**. Możesz wprowadzić wymaganie by hasło było proste albo złożone. Kryteria złożoności hasła są zdefiniowane w urządzeniu przenośnym OS.
  - W urządzeniu Android, złożone hasło musi zawierać przynajmniej jedna literę, jedną cyfrę i znak specjalny.

    Notatka
    Złożone hasło jest wspierane przez Android 3.0 lub nowszy.

  - Na urządzeniach iOS, złożone hasła nie pozwalają na kolejne powtarzające się znaki (takie jak abcdef, 12345 lub aaaaa, 11111).

  W zależności od wybranej opcji, gdy użytkownik ustawia hasło blokowania ekranu, system operacyjny sprawdza czy wymagane kryteria są spełnione.
- **Wymaga wartości alfanumerycznej**. Wymaga hasła zawierającego litery i cyfry.
- **Minimalna długość** . Wymaga hasła zawierającego minialną liczbę znaków, które określasz w odpowienim polu.
- **Minimalna liczna znaków**. Wymaga hasła zawierającego minimalną liczbę niealfanumerycznych znaków (np. #, $ lub @), które możesz określić w odpowiednim polu.
- **Czas wygaśnięcia (miesiące)**. Zmusza użytkownika do zmiany hasla blokowania ekranu w okreslonych przedziałach czasu (co miesiac). Na przykład, jeżeli wpiszesz 3, użytkownik będzie proszony aby zmienić hasło blokowania ekranu co 3 miesiące.

  Notatka
  W Androidzie, ta funkcja jest obsługiwana w wersji 3.0 lub późniejszej.

- **Historia Ograniczeń (wcześniejsze hasła)**. Wybierz lub podaj wartość w odpowiednim polu aby określić ilość ostatnich haseł jakie nie mogą być ponownie użyte. Na przykład, jeżei wpiszesz 4, użytkownik nie może ponownie

wykorzystac hasłą, które pasuje do jednego z czterech ostatnio uzywanych haseł.

Notatka
W Androidzie, ta funkcja jest obsługiwana w wersji 3.0 lub późniejszej.

- **Maksymalna liczba błędnych prób**. Określ ile razy użytkownik może podać nieprawidłowe hasło.

  Notatka
  Na urządzeniu iOS, gdy liczba jest większa niż 6L po sześciu błędnych próbach, uzytkownik będzie musiał odczekać zanim bedzie mógł wprowadzić hasło ponpownie. Czas jaki użytkownik musi odczekać po podaniu nieprawidłowego hasła, zwiększa się przy każdej nieudanej próbie.

  Ostrzeżenie
  Jeżeli użytkownik przekroczy maksymalna próbę nieudanytch prób odblokowania ekranu, urządzenie zostanie wymazane (wszystkie dane zostaną usuniete).

- **Automatyczne zamknięcie po (min)**. Ustaw przedział nieaktywności (w minutach) po którym urządzenie się automatycznie zablokuje.

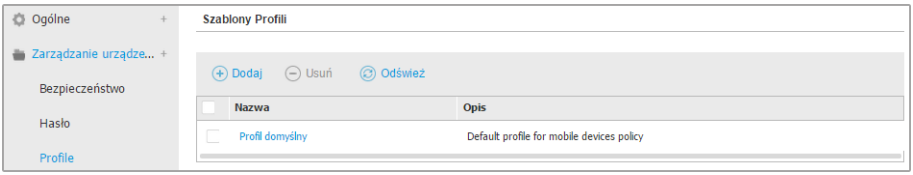
  Notatka
  Urządzenie iOS ma predefiniowana listę dla automatycznego czasu blokady i nie pozwala na własne wartości. Kiedy przypisana polityka jest niezgodna z automatycznymi wartościami blokady, urządzenie wymusza kolejny bardziej restrykcyjny okres czasu dostępny na liście. Na przykład, jezeli polityka automatycznego blokowania jest ustawionba na trzy minuty, urządzenie zostanie automatycznie zablokowane po dwóch minutach nieaktywności.

Kiedy zmieniasz politykę, przy wyborze wyższego poziomu bezpieczeństwa dla hasła blokowania ekranu, użytkownicy zostaną powiadomieni o zmianie hasła według nowych kryteriów.

Jeżeli wyczyścisz opcje **Blokowanie ekranu hasłem**, użytkownicy odzyskają pełny dostęp dla ustawień odblokowywania ekranu w ich urządzeniach przenośnych. Istniejące hasło pozostanie aktywne, dopóki użytkownik nie zdecyduje się go zmienić albo usunąć.

Tryby

W tej sekcji możesz stworzyć, edytować i usunąć używane profile dla urządzeń przenośnych. Używanie profili pomoże ustawić Wi-Fi i VPN i egzekwować kontrolę dostępu do sieci na zarządzanych urządzeniach przenosnych.



Polityki Urządzeń Przenośnych - Szablony Polityki

Możesz skonfigurować jeden lub więcej profili, ale tylko jden może być aktywny w tym samym czasie na urządzeniu.

- Jeżeli konfigurujesz tylko jeden profil, polityka automatycznie zastosuje się do wszystkich urządzeń do których jest przypisana.
- Jeżeli konfigurujesz kilka profili, pierwszy na liście zostanie automatycznie zastosowany do wszystkich urządzeń do których jest przypisany.

Uzytkownicy mogą zobaczyć przypisane profile i ustawienia skonfigurowane dla każdego profilu w aplikacji GravityZone Mobile Client. Użytkownicy nie mogą zmieniać istniejących ustawień w profilach, ale mogą przełączać się między profilami jeżeli kilka z nich jest niedostępne.

Notatka
Przełączanie profilu wymagania połączenia Internetowego.

Aby stworzyć nowy profil:

1. Kliknij przycisk **Dodaj** po prawej stronie tabeli. Wyświetlanie strony konfiguracji profilu.
2. Skonfiguruj ustawienia profilu według uznania. Aby uzyskać szczegółowe informacje, odwołaj się do:
   - „Szczegóły” (p. 403)
   - „Sieci” (p. 403)
   - „Dostęp Sieciowy” (p. 406)

3. Kliknij **Zapisz**. Nowy profil dodano do listy.

Aby usunąć jeden lub kilka profili, wybierz odpowiednie pole wyboru i naciśnij przycisk ⊖ **Usuń** po prawej stronie tabeli.

Aby zmienić ustawienia profilu, naciśnij nazwę, zmień ustawienia jakie potrzebujesz i naciśnij **Zapisz**.

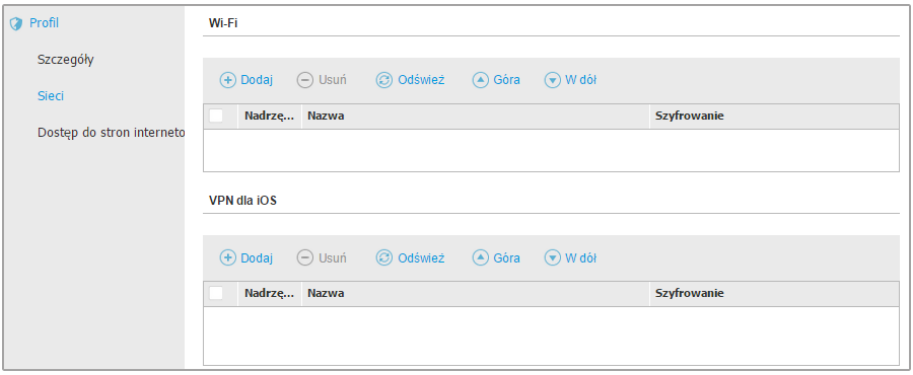
Szczegóły

Strona **Szczegóły** zawiera ogólne informacje dotyczące profilu:

- **Nazwa**. Podaj odpowiednia nazwę profilu. Profile powinny mieć sugestywne nazwy tak by administratorzy mogli szybko je zidentyfikować.
- **Opis**. Podaj szczegółoy opis profilu. Ta opcja może pomóc administratorowi łatwo odróżnić profil od kilku innych.

Sieci

W tej sekcji możesz określić ustawienia jednego lub kilku sieci Wi-Fi lub VPN. Ustawienia VPN są dostepne tylko dla urządzeń iOs.



Polityki Urządzeń Przenośnych - Ustawienia połączeń profili sieciowych

WAŻNE
Przed zdefiniowaniem połączeń Wi-Fi i VPN, upewnij się że masz wszystkie potrzebne informacje (hasła, ustawienia proxy, itd.).

Urządzenia przenośne przypisane do odpowiedniego profilu automatycznie połączą się ze zdefiniowana siecią, gdy znajdzie się w zasięgu. Możesz ustawić priorytet

gdy kilka sieci zostanie stworzonych, biorąc pod uwagę fakt, że tylko jedna sieć może być używana w tym samym czasie. Gdy pierwsza sieć nie jest dostępna, urządzenie przenośne łączy się z następną siecią, itd.

Aby ustawić priorytet sieci:

1. Zaznacz pole żądanej sieci.
2. Użyj przycisków priorytetu po prawej stronie tabeli:
   - Naciśnij przycisk **Góra** aby wypromować wybraną siec.
   - Naciśnij przycisk **Dół** aby obniżyć.

- **Wi-Fi**

  Możesz dodać dowolną liczbę sieci Wi-Fi. Aby dodać sieć Wi-Fi:

  1. W sekcja **Wi-Fi**, naciśnij przycisk **Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
  2. Pod zakładką **Ogólne**, możesz skonfigurować szczegóły połączenia Wi-Fi:
     - **Nazwa (SSID)**. Podaj nazwę nowej sieci Wi-Fi.
     - **Bezpieczeństwo**. Wybierz opcje określone dla poziomu bezpieczeństwa sieci Wi-Fi:
       - **Brak**. Wybierz opcje kiedy łączysz się z publiczną siecią Wi-Fi (poświadczenia nie są wymagane).
       - **WEP**. Wybierz tę opcje aby ustawić połaćzeniue Protokołu Szyfrowania Sieci (WEP). Podaj wymagane hasło dla tego rodzaju sieci w odpowiednim polu wyświetlonym poniżej.
       - **WPA/WPA2 Personal**. Wybierz tę opcję jeżeli sieć Wi-Fi jest zabezpieczona używając Wi-Fi Protected Access (WPA). Podaj wymagane hasło dla tego rodzaju sieci w odpowiednim polu wyświetlonym poniżej.
  3. Pod zakładką **TCP/IP**, możesz skonfigurować ustawienia TCP/IP dla połączenia Wi-Fi: Każde połączenie używa IPv4 lub IPv6 albo obu.
     - **Konfigurowanie IPv4**. Jeżeli chcesz użyć metody IPv4, wybierz sposób przypisania IP z odpowiedniego menu.

       DHCP: Jeżeli adres IP jest przypisany automatycznie przez serwer DHCP. Jeżeli potrzebne, dostarcz ID Klienta DHCP w kolejnym polu.

Wyłączone: wybierz tę opcję jeżeli nie chcesz używać protokołu IPv4.

- **Konfigurowanie IPv6**. Jeżeli chcesz użyć metody IPv6, wybierz sposób przypisania IP z odpowiedniego menu.

  DHCP: Jeżeli adres IP jest przypisany automatycznie przez serwer DHCP.

  Wyłączone: wybierz tę opcję jeżeli nie chcesz używać protokołu IPv6.

- **Serwery DNS**. Podaj adres przynajmniej jednego serwera DNS dla sieci.

4. W zakładce **Proxy** skonfiguruj ustawienia proxy dla połączenia Wi-Fi. Zaznacz żądaną metodę konfiguracji z menu **Rodzaj**:
   - **Wyłączony**. Wybierz tę opcje jeżeli sieć Wi-fi ma ustawienia proxy.
   - **Ręczne**. Wybierz tę opcje aby ręcznie określić ustawienia proxy. Podaj nazwę hosta dla serwera proxy i port, który nasłuchuje połączeń. Jeżeli serwer proxy wymaga uwierzytelnienia, wybierz pole **Uwierzytelnienie** i podaj nazwę użytkownika i hasło w kolejnych polach.
   - **Automatyczne**. Wybierz tę opcję, aby pobrać ustawienia proxy z pliku Auto Konfiguracji (PAC) opublikowanego w lokalnej sieci. Podaj adres pliku PAC w polu **URL**.
5. Kliknij **Zapisz**. Nowe połączenie Wi-Fi zostało dodane do listy.

- **VPN dla iOS**

  Możesz dodać dowolną liczbę VPN. Aby dodać VPN:

  1. W sekcja **VPN dla iOS**, naciśnij przycisk ⊕ **Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
  2. Zdefiniuj ustawienia VPN w oknie **Połączenie VPN**:

     Ogólne:

     - **Nazwa**. Podaj nazwę połączenia VPN.
     - **Szyfrowanie**. Dostępny protokół uwierzytelniania dla połączenia tego typu to **IPSec**, który wymaga uwierzytelnienia użytkownika przez hasło lub maszynę uwierzytelnienia przez wspólne hasło.
     - **Serwer**. Podaj adres serwera VPN.
     - **Użytkownik**. Podaj nazwę użytkownika VPN.
     - **Hasło**. Wprowadź hasło VPN.

- **Nazwa grupy**. Podaj nazwę grupy.
- **Tajne**. Wprowadź wstępnie współdzielony klucz.

Proxy:

W tej sekcji możesz skonfigurować ustawienia proxy dla połączenia VPN. Zaznacz żądaną metodę konfiguracji z menu **Rodzaj**:

- **Wyłączony**. Wybierz tę opcje jeżeli połączenie VPN nie ma ustawień proxy.
- **Ręczne**. Ta opcja pozwala na ręczne określenie ustawie proxy:
  - **Serwer**: podaj nazwę hosta proxy.
  - **Port**: podaj numer portu proxy.
  - Jeżeli serwer proxy wymaga uwierzytelnienia, wybierz pole **Uwierzytelnienie** i podaj nazwę użytkownika i hasło w kolejnych polach.
- **Automatyczne**. Zaznacz tę opcję, aby pobrać ustawienia proxy z pliku Auto Konfiguracji (PAC) opublikowanego w lokalnej sieci. Podaj adres pliku PAC w polu **URL**.

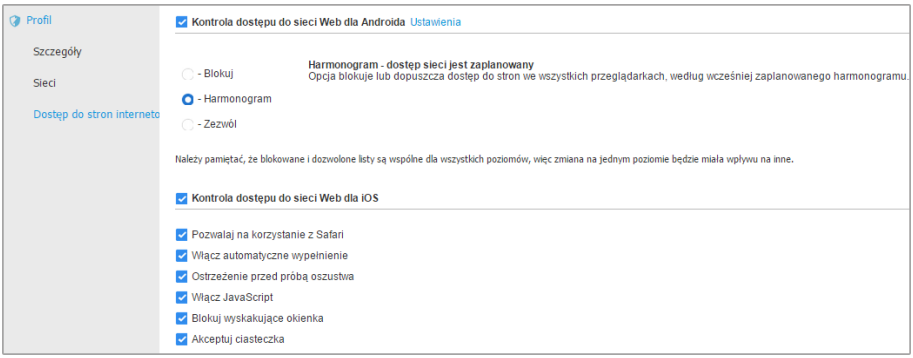
3. Kliknij **Zapisz**. Nowe połączenie VPN zostanie dodane do listy.

Aby usunąć jeden lub kilka sieci, wybierz odpowiednie pole wyboru i naciśnij przycisk ⊖ **Usuń** po prawej stronie tabeli.

Aby zmienić ustawienia sieci, naciśnij nazwę, zmień ustawienia jakie potrzebujesz i naciśnij **Zapisz**.

Dostęp Sieciowy

W tej sekcji możesz skonfigurować kontrolę dostępu do sieci dla urządzeń Android i iOS.



Polityki Urządzeń Przenośnych - Ustawienia profili kontroli dostepu

- **Kontrola dostępu do sieci Web dla Androida.** Włącz tę opcję, aby filtrować dostęp internetowy do przeglądarki Chrome i wbudowanej przeglądarki Android. Możesz ustawić ograniczenia czasowe w dostępie do strony internetowej, a także zezwolić lub zablokować dostęp do określonych stron internetowych. Strony www blokowane przez kontrolę stron www nie wyświetlają się w przeglądarce. Zamiast tego wyświetlana jest domyślna strona www informująca użytkownika, że dana strona została zablokowana przez kontrolę dostępu stron www.

  WAŻNE
  Kontrola Dostępu do Internetu dla Androida działa tylko do systemu Android 5 i tylko z Chrome i wbudowaną przeglądarką Android.

  Masz trzy opcje konfiguracyjne:

  – Wybierz **Pozwól** aby zawsze udzielić dostępu do sieci.
  – Wybierz **blokuj** aby nigdy nie udzielać dostępu do sieci.
  – Wybierz **Harmonogram** aby umożliwić ograniczenia czasowe w dostępie do stron internetowych w szczegółowym harmonogramie.

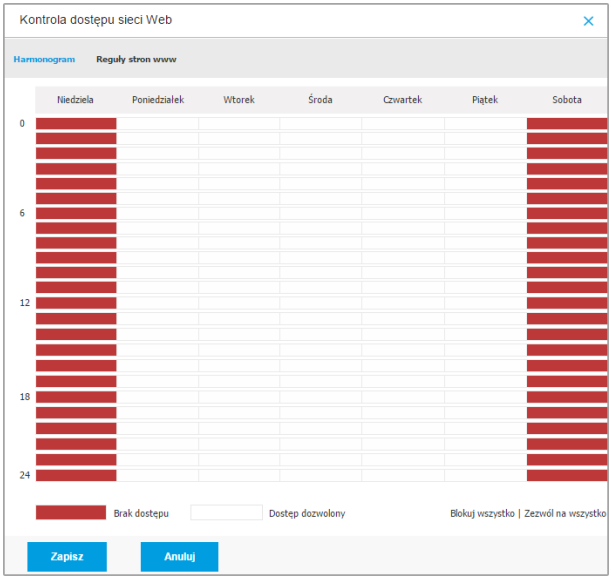
  Jeżeli wybierasz żeby dopuścić lub zablokować dostęp do strony internetowej, możesz zdefiniować wyjątki do tych działań dla całych kategorii internetowych lub tylko dla określonych adresów internetowych. Naciśnij **Ustawienia** aby skonfigurować twój harmonogram dostępu do sieci i wyjątki według poniższych zaleceń:

Harmonogram

Aby ograniczyć dostęp do internetu o określonych porach dnia, cotygodniowo:

1. Wybierz z siatki przedziały czasowe, w których chcesz aby dostęp do internetu był zablokowany.

   Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu. Naciśnij ponownie na komórkę, aby odwrócić zaznaczenie.



Polityki Urządzeń Przenośnych - Harmonogram dostepu do sieci

   Aby rozpocząć nowe zaznaczenie, naciśnij **Zezwól wszystkie** lub **Zablokuj wszystkie**, w zależności od rodzaju ograniczenia, które chcesz wprowadzić.

2. Kliknij **Zapisz**.

Reguły stron www

Możesz również zdefiniować reguły sieci aby jawnie blokować lub zezwalać określone adresy sieciowe, zastępując istniejące ustawienia Kontroli Dostępu Sieciowego. Użytkownicy będą w stanie, na przykład, uzyskać

dostęp do odpowiedniej strony również podczas przeglądanie stron internetowych są zablokowane przez Kontrolę Dostępu Sieciowego.

Aby stworzyć regułę sieci:

1. Wybierz **Użyj wyjątków** aby włączyć wyjątki sieci.
2. Podaj adresy jakie chcesz dopuścić albo zablokować w polu **Adresy Sieciowe**.
3. Wybierz **Zezwól** lub **Zablokuj** z menu **Pozwolenia**.
4. Naciśnij przycisk ⊕ **Dodaj** po prawej stronie tabeli aby dodać adres do listy wyjątków.
5. Kliknij **Zapisz**.

Aby edytować regułę sieci:

1. Naciśnij na adres internetowy jaki chcesz edytować.
2. Zmień istniejący URL.
3. Kliknij **Zapisz**.

Usuń regułę sieci:

1. Przesuń kursor nad adres sieciowy, który chcesz usunąć.
2. Kliknij przycisk ⊗ **Usuń** .
3. Kliknij **Zapisz**.

Użyj znaków do określenia wzorów adresów:

– Gwiazdka (*) zastępuje zero lub więcej znaków.

– Znak zapytania zastępuje dokładnie jeden znak. Możesz użyć kilku znaków zapytania aby zdefiniować każdą kombinacje określonej liczby znaków. Na przykład, ??? zastępuje każdą kombinację dokładnie 3 znaków.

W poniższej tabeli, znajdziesz znaleźć kilka próbek składni dla określonych adresów.

Składnia	Zastosowanie
`www.example*`	Dowolna strona internetowa rozpoczynająca się `www.example` (niezależnie od rozszerzenia domeny).

Składnia	Zastosowanie
	Zasady nie zostaną zastosowane dla subdomen określonych stron, takich jak `subdomain.example.com`.
`*example.com`	Dowolna strona strona kończy się `example.com`, w tym strony i ich subdomeny.
`*Ciąg*`	Dowolna strona której adres zawiera określony ciąg.
`*.com`	Dowolna zawierająca `.com` rozszeżenie domeny, w tym strony i ich subdomeny. Użyj tej składni, aby wykluczyć ze skanowania całe domeny na najwyższym poziomie.
`www.example?.com`	Dowolny adres internetowy rozpoczynający się od `www.example?.com`, gdzie ? może być zastąpiony dowolnym znakiem. Takie strony internetowe mogą zawierać: `www.example1.com` lub `www.exampleA.com` .

- **Kontrola dostępu do sieci Web dla iOS.** Włącz tę opcje aby zarzącać centralnie ustawieniami wbudowanej przeglądarki iOS (Safari). Użytkownicy urządzeń przenośych nie będą już mogli zmienić odpowiednich ustawień na ich urządzeniach.
  - **Pozwalaj na korzystanie z Safari**. Ta opcja pomaga kontrolować używanie przeglądarki Safari na urządzeniach przenośnych. Wyłączenie opcju usuwa skrót Safari z interfejsu iOS, to ustrzega użytkowników przed dostępem do interneto przez Safari.
  - **Włącz auto uzupełnianie** Wyłącz te opcję jeżeli chcesz uchronić przeglądarkę przed przechowywaniem wpisów, które mogą zawierać wrażliwe informacje.
  - **Ostrzeżenie przed próbą oszustwa**. Wybierz te opcję aby upewnić się, że użytkownicy są ostrzegani, gdy próbują uzyskać dostęp do fałszywych stron internetowych.
  - **Włącz JavaScript**. Wyłącz tę opcję jeżeli chcesz aby Safari ignorowało javascript na stronach.

- **Blokuj wyskakujące okienka**. Wybierz opcję aby zapobiec automatycznemu wyskakiwaniu okien.
- **Akceptuj ciasteczka**. Safari domyślnie dopuszcza ciasteczka. Wyłącz tę opcje jeżeli chcesz zapobiec przechowywaniu informacji przez strony w przeglądarce.

WAŻNE
Kontrola dostępu do sieci nie jest obsługiwana na iOS 13.

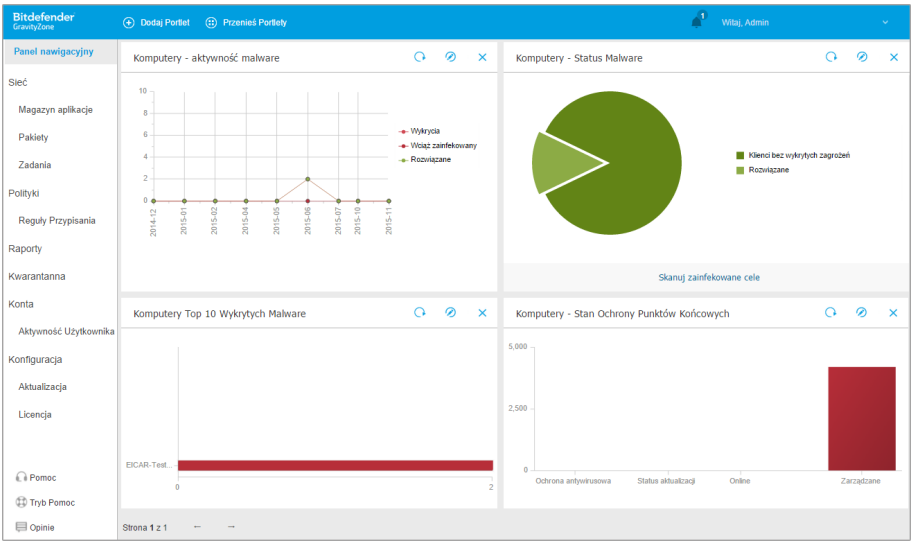
8. MONITOROWANIE PANELU

Prawidłowa analiza zabezpieczeń twojej sieci wymaga dostępu do danych i korelacji. Posiadanie scentralizowanych informacji o zabezpieczeniach pozwoli Ci monitorować i zapewnić zgodność z politykami bezpieczeństwa, szybko identyfikować problem, analizować zagrożenia i podatności.

8.1. Panel nawigacyjny

Panel Control Center jest wizualnie dostosowywany i zapewnia szybki przegląd bezpieczeństwa dla wszystkich chronionych punktów końcowych oraz przegląd statusu sieci.

Portlety panelu wyświetlają różne informacje bezpieczeństwa w czasie rzeczywistym, używając łatwych do przeczytania wykresów, pozwalając w ten sposób szybko zidentyfikować wszystkie problemy, które mogą wymagać uwagi.



Panel

To jest to co potrzebujesz, żeby wiedzieć o portletach w Panelu:

- Control Center ma kilka wstępnie zdefiniowanych portletów w panelu.

- Każdy portlet w panelu zawiera szczegółowy raport w tle, dostępny za pomocą jednego kliknięcia na wykresie.
- Jest kilka rodzajów portletów zawierających różne informacje o ochronie twoich punktów końcowych, takich jak status aktualizacji, status malware, aktywność zapory sieciowej.

  Notatka
  Domyślnie, portlety odzyskują dane z bieżącego dnia, i w przeciwieństwie do raportów, nie mogą być z okresu dłuższego niż miesiąc.

- Informacje wyświetlane poprzez portlety odnoszą się wyłącznie do punktów końcowych twojego konta. Możesz dostosować każdy obiekt portletu oraz preferencje przy użyciu komendy **Edytuj Portlet**.
- Kliknij pozycje legendy wykresu, gdy jest dostępna, aby ukryć lub wyświetlić odpowiednią zmienną na wykresie.
- Portlety są wyświetlane w czterech grupach. Użyj poziomo przewijanego paska lub klawiszy góra/dół by nawigować pomiędzy grupami portletów.
- Dla kilku typów raportów, posiadasz opcję natychmiastowego uruchomienia określonego zadania na docelowym punkcie roboczym, bez posiadania go na stronie **Sieć** w celu uruchomienia zadania (dla przykładu, skanowanie zainfekowanego punktu końcowego lub jego aktualizacja). Użyj przycisk u dolnej części portletu aby podjąć dostępne działanie.

Panel łatwo konfigurować, bazuje on na indywidualnych preferencjach. MożeszEdytoiwać ustawienia portletu, dodaj dodatkowe portlety, usuń lub zmień pozycję istniejących portletów.

8.1.1. Odświeżanie Danych Portletów

Aby upewnić się, że portlety wyświetlają ostatnie informacje, naciśnij ikonę **Odśwież** na pasku tytułowym.

Aby zaktualizować informacje we wszystkich portletach na raz kliknij przycisk **Odśwież Portlety** na górze pulpitu.

8.1.2. Edytowanie ustawień portletów

Niektóre portlety oferują informacje o stanie, podczas innego raportu w wydarzeniach bezpieczeństwa w ostatnim czasie. Możesz sprawdzić i skonfigurować okres raportowania dla portletów naciskając ikonę **Edytuj Portlet** na pasku tytułu.

8.1.3. Dodawanie nowego portletu

Możesz dodać inne portlety aby uzyskać potrzebne informacje.

Aby dodać nowe portlety:

1. Przejdź do strony **Panel**.
2. Kliknij przycisk **Dodaj Portlet** w górnej części konsoli. Wyświetlono okno konfiguracji.
3. W zakładce **Szczegóły**, skonfiguruj szczegóły portletu:
   - Typ Punktu Końcowego (**Komputery**, **Maszyny Wirtualne** lub **Urządzenia Mobilne**)
   - Rodzaje raportów w tle
   - Sugestywna nazwa portletu
   - Przedział czasowy do zgłoszenia wydarzenia.

   Aby uzyskać więcej informacji o dostępnych rodzajach raportów, odwołaj się do „Typy Raportu” (p. 415)
4. W zakładce **Cele**m wybierz obiekty sieciowe i grupy zawierające.
5. Kliknij **Zapisz**.

8.1.4. usuwanie Portletu

Możesz w łatwy sposób usunąć każdy portlet naciskając ikonę **Usuń** na pasku tytułu. Jeżeli usuniesz portlet, nie będziesz mógł go już więcej odzyskać. Jednak, możesz utworzyć inny portlet z takimi samymi ustawieniami.

8.1.5. Zmiana Układu Portletów

Możesz ułożyć portlety w panelu aby lepiej dostosować go do swoich potrzeb. Aby zmienić układ portletów:

1. Przejdź do strony **Panel**.
2. Przeciągnij i upuść portlet do żądanej pozycji. Wszystkie pozostałe portlety pomiędzy nowymi i starymi pozycjami są przenoszone by zachować ich porządek.

> **Notatka**
> Możesz przenieść portlety tylko przy użyciu już podjętych pozycji.

9. UŻYWANIE RAPORTÓW

Control Center dopuszcza utworzenie i zobaczenie scentralizowanych raportów w statusie bezpieczeństwa zarządzanych obiektów sieciowych. Raporty można używać do różnych celów, m.in.:

- do monitorowania i zapewnienia zgodności z polityką bezpieczeństwa danej organizacji.
- do kontrolowania i oceny stanu zabezpieczeń sieci.
- do identyfikowania problemów z bezpieczeństwem sieci, zagrożeń i luk.
- Monitorowanie incydentów bezpieczeństwa.
- zapewniając kierownictwu wyższego szczebla łatwe do zinterpretowania dane na temat bezpieczeństwa sieciowego.

Kilka różnych rodzajów raportów są dostępne więc możesz łatwo dostać informacje, które potrzebujesz. Informacje są przedstawione w formie interaktywnych wykresów i tabel, co pozwala na szybkie sprawdzenie statusu bezpieczeństwa sieci i zidentyfikowanie problemów.

Raporty mogą obejmować dane z całej sieci zarządzanych obiektów sieciowych lub jedynie z określonych grup. W ten sposób z jednego raportu możesz uzyskać:

- Dane statystyczne dotyczące wszystkich lub wybranych grup zarządzanych obiektów sieciowych.
- Szczegółowe informacje dla każdego zarządzanego obiektu sieciowego.
- Lista komputerów z określonymi kryteriami (np. z wyłączoną ochroną antymalware).

Niektóre raporty również pomagają w szybkim rozwiązaniu problemów odnalezionych w twojej sieci. Dla przykładu, możesz bez wysiłku zaktualizować wszystkim obranym obiektom sieciowym prawo do raportowania, bez potrzeby uruchamiania zadania aktualizacji z zakładki strony **Sieci**.

Wszystkie raporty są dostępne w Control Center ale możesz zapisać je na swój komputer lub wysłać na e-mail.

Dostępne formaty zawierające Przenośny format dokumentu (PDF) i wartości oddzielone przecinkami (CSV).

9.1. Typy Raportu

Różne rodzaje raportów są dostępne dla każdego typu punktu końcowego:

- Komputer i Raporty Wirtualnej Maszyny

- Raporty Exchange
- Raporty urządzeń przenośnych

9.1.1. Komputer i Raporty Wirtualnej Maszyny

Oto dostępne typy raportów dla maszyn fizycznych i wirtualnych:

Aktywność antyphishingowa

Informuje Ciebie o aktywności modułu Antyphishing Bitdefender Endpoint Security Tools. Możesz zobaczyć liczbę zablokowanych witryn phishingowych na wybranych punktach końcowych i użytkownika, który był zalogowany w czasie ostatniego wykrycia. Klikając na łącze z kolumny **Zablokowane Strony** możesz również zobaczyć adresy URL stron, ile razy były blokowane oraz kiedy nastąpiła ostatnia blokada.

Zablokowane aplikacje

Informuje o aktywności następujących modułów: Antymalware, Firewall, Kontrola Zawartości, Kontrola Aplikacji,Zaawansowany Anty-Exploit, ATC/IDS i HVI. Możesz zobaczyć liczbę zablokowanych aplikacji na wybranych punktach końcowych i użytkownika, który był zalogowany w czasie ostatniego wykrycia.

Kliknij numer przyporządkowany do celu, aby wyświetlić dodatkowe informacje o zablokowanych aplikacjach, liczbie zdarzeń, które wystąpiły oraz datę i czas ostatniego zdarzenia.

Z tego raportu, możesz szybko zlecić modułom ochrony zezwolenie zaznaczonej aplikacji na uruchomienie się na docelowym punkcie końcowym:

- Kliknij przycisk **Dodaj wyjątek**, aby zdefiniować wyjątki w następujących modułach: Antymalware, ATC, kontrola zawartości, firewall i HVI. Okno potwierdzenia pojawi się, informując Ciebie o nowej regule, która będzie modyfikować istniejącą politykę dla danego punktu końcowego.
- Kliknij przycisk **Dodaj regułę**, aby zdefiniować reguły dla aplikacji lub procesu w Kontroli aplikacji. W oknie konfiguracyjnym zastosuj regułę do istniejącej polityki. Komunikat poinformuje Cię o nowej regule, która będzie modyfikować politykę przypisaną do konkretnego punktu końcowego. Raport też wyświetla liczbę prób dostępu i jeśli moduł działa w trybie testowym lub produkcyjnym.

Zablokowane strony

Informuje Ciebie o aktywności modułu Kontroli Stron WWW Bitdefender Endpoint Security Tools. Dla każdego celu, możesz zobaczyć liczbę

zablokowanych stron. Klikając tę liczbę, możesz wyświetlić dodatkowe informacje, jakie jak:

- Adres URL witryny i kategoria
- Liczba prób dostępu na stronę
- Data i czas ostatniej próby, jak również użytkownik, który był zalogowany w momencie wykrywania.
- Powód do blokowania, który obejmuje harmonogram dostępu, wykrywanie malware, dodawanie do czarnej listy i filtrowanie po kategoriach.

Ochrona danych

Informuje Ciebie o aktywności modułu Ochrony Danych Bitdefender Endpoint Security Tools. Możesz zobaczyć liczbę zablokowanych e-maili na wybranych punktach końcowych, a także użytkownika, który był zalogowany w czasie ostatniego wykrycia.

Aktywność Kontroli Urządzeń

Inforumuje o wydarzeniu które miało miejsce podczas uzyskania dostępu do punktu końcowego poprzez monitorowane urządzenie. Dla każdego wybranego punktu końcowego, możesz wyświetlić liczbę dopuszczonych / zabronionych prób dostępu oraz zdarzeń typu tylko do odczytu. Jeśli wystąpiło zdarzenie dodatkowe informacje można uzyskać klikając odpowiednie numery. Szczegóły znajdują się:

- Użytkownik zalogowany na maszynie
- Typ i ID urządzenia
- Dostawca urządzenia i ID produktu
- Data i czas wydarzenia.

Status Szyfrowania Punktów Końcowych

Dostarcza danych dotyczących statusu szyfrowania na punktach końcowych. Wykres kołowy pokazuje liczbę maszyn zgodnych i niezgodnych z ustawieniami reguł szyfrowania.

Tabela pod wykresem kołowym zawiera takie informacje jak:

- Nazwa punktu końcowego.
- W pełni zatwierdzona Nazwa Domeny (Full Qualified Domain Name - FQDN)
- IP Maszyny.

- System operacyjny.
- Zgodność Polityki Urządzenia:
  - **Zgodne** - gdy wszystkie woluminy są zaszyfrowane lub niezaszyfrowane zgodnie z polityką.
  - **Niezgodny** - gdy status woluminów nie jest zgodny z przypisaną polityką (np. tylko jeden lub dwa woluminy są zaszyfrowane, lub gdy ten wolumin jest w trakcje szyfrowania).
- Polityka Urządzenia (**Szyfruj** lub **Odszyfruj**).
- Kliknij liczby w kolumnie Podsumowanie Woluminów aby zobaczyć informacje o każdym woluminie punktu końcowego: ID, nazwa, status szyfrowania (**Zaszyfrowany** lub **Niezaszyfrowany**), problemy, typ (**Rozruchowy** lub **Nie-rozruchowy**), rozmiar, ID klucza odzyskiwania.

Status modułów punktu końcowego

Zawiera omówienie zakresu modułów ochrony nad wybranymi celami. W szczegółach raportu, dla każdego punktu końcowego docelowego można zobaczyć, jakie moduły są aktywne, wyłączone lub nie zainstalowane, a także skanujący silnik. Klikając na nazwę punktu końcowego pokaże się **Informacja** z oknem ze szczegółowymi informacjami o punkcie końcowym i zainstalowanych warstwach ochronnych.

Klikając **Rekonfiguruj Klienta** możesz zacząć zadanie zmieniania początkowych ustawień jednego lub kilku zaznaczonych punktów końcowych. Po więcej informacja odnieś się do Rekonfiguracja Klienta.

Status ochrony punktów końcowych

Zapewnia zróżnicowane informacje o stanie dotyczące wybranych z sieci punktów końcowych.

- Stan ochrony antymalware
- status aktualizacji Bitdefender Endpoint Security Tools
- Status aktywności sieci (online/offline)
- Stan zarządzania

Możesz zastosować filtry w aspekcie bezpieczeństwa i stanu, aby znaleźć informacje, których szukasz.

Aktywność Zapory Sieciowej

Informuje Ciebie o aktywności modułu Firewall Bitdefender Endpoint Security Tools. Możesz zobaczyć liczbę zablokowanych prób ruchu i zablokowanych skanowań portów na wybranych punktach końcowych, a także użytkownika, który był zalogowany w czasie ostatniego wykrycia.

Aktywność HyperDetect

Informuje Cię o aktywności modułu HyperDetect Bitdefender Endpoint Security Tools.

Wykres w górnej części strony raportu pokazuje dynamikę prób ataku w określonym przedziale czasowym i ich rozkład według typu ataku. Przesunięcie kursora myszy nad pozycje legendy zaznaczy powiązane rodzaje ataków na wykresie. Kliknięcie w pozycje pokaże lub ukryje odpowiednią linię na wykresie. Kliknięcie dowolnego punktu na linii filtruje dane tabeli zgodnie z wybranym typem. Jeśli, na przykład, klikniesz w dowolnym punkcie pomarańczowej linii, wyświetlone zostaną jedynie exploity.

Szczegółowe informacje w dolnej części raportu pomogą Ci zidentyfikować naruszenia w Twojej sieci oraz to czy im zaradzono. Odnoszą się do:

- Ścieżka do złośliwego pliku lub wykrytego adresu URL, w przypadku zainfekowanych plików. W przypadku ataków typu file-less podana jest nazwa pliku wykonywalnego użytego w ataku, wraz z linkiem do okna szczegółów zawierającego przyczynę wykrycia i złośliwy wiersza polecenia.
- Punkt końcowy, na którym dokonano wykrycie
- Moduł zabezpieczający, który wykrył zagrożenie. Jako że HyperDetect jest dodatkowym poziomem modułów Antymalware i Kontroli Zawartości, w raporcie pojawi się informacja o jednym z nich, w zależności od rodzaju wykrywania.
- Rodzaj zamierzonego ataku (atak docelowy, grayware, exploity, ransomware, podejrzane pliki i ruch sieciowy)
- Status zagrożenia
- Poziom ochrony modułu, na którym wykryto zagrożenie (Dopuszczalny, Normalny, Agresywny)
- Ile razy zostało wykryte zagrożenie
- Najnowsze wykrycia

- Identyfikacja ataku file-less (tak lub nie), aby szybko filtrować wykrywanie ataków typu file-less

> **Notatka**
> Plik może zostać użyty w innych atakach GravityZone zgłasza każdy rodzaj ataku, w który był zaangażowany.

Z pomocą tego raportu możesz szybko rozwiązać fałszywe alarmy, dodając wyjątki do przypisanych polityk bezpieczeństwa. Aby to zrobić:

1. Wybierz z tabeli pozycje, których potrzebujesz.

   > **Notatka**
   > Do listy wyjątków nie można dodawać wykrytych ataków typu file-less, ponieważ wykryty plik wykonywalny nie jest sam w sobie złośliwym oprogramowaniem, ale może stanowić zagrożenie, gdy zostanie użyty złośliwy zakodowany wiersz poleceń.

2. Kliknij przycisk **Dodaj wyjątek** w górnej części tabeli.
3. W oknie konfiguracji wybierz polityki, do których ma zostać dodany wyjątek, a następnie kliknij przycisk **Dodaj**.

   Domyślnie powiązane informacje dla każdego dodanego wyjątku są przesyłane do Bitdefender Labs, aby poprawić możliwości wykrywania produktów Bitdefender. Działanie można kontrolować za pomocą pola wyboru **Prześlij tę opinię do Bitdefender w celu dokładniejszej analizy**.

Jeśli przez moduł Antymalware zostało wykryte zagrożenie, wyjątek będzie dotyczył zarówno trybów skanowania dostępowego, jak i skanowania na żądanie.

> **Notatka**
> Te wyjątki możesz znaleźć w następujących sekcjach wybranych polityk: **Antymalware > Ustawienia** dla plików, i **Kontroli Zawartości > Ruch** dla URL.

Status szkodliwego oprogramowania

Pomoże Ci znaleźć ile z wybranych punktów końcowych zostało zarażonych malware w określonym przedziale czasowym i jak poradzono sobie z zagrożeniami. Możesz także zobaczyć użytkownika, który był zalogowany w czasie ostatniego wykrycia.

Punkty końcowe są pogrupowane w oparciu o te kryteria:

- Punkty końcowe bez wykrycia (nie wykryto zagrożenia malware przez określony okres czasu)
- Punkty końcowe wyleczone z malware (wszystkie wykryte pliki zostały pomyślnie wyleczony lub przeniesiony do kwarantanny)
- Punkty końcowe z nierozwiązanym złośliwym oprogramowaniem (niektórym z wykrytych plików odmówiono dostępu)

Dla każdego punktu końcowego, naciśnij na dostępny odnośnik w kolumnach szczegółów dezynfekcji, możesz zobaczyć listę zarażeń i ścieżek do zarażonych plików.

W tym raporcie można szybko uruchomić zadanie pełnego skanowania na nierozwiązanych obiektach docelowych, klikając przycisk **Skanuj zainfekowane cele** z paska narzędzi akcji nad tabelą danych.

Incydenty Sieciowe

Informuje o aktywności modułu Network Attack Defense. Wykres pokazuje liczbę prób ataku wykrytych w określonym przedziale czasu. Szczegóły raportu zawierają:

- Nazwa punktu końcowego, adres IP i nazwa FQDN
- Nazwa użytkownika
- Nazwa wykrycia
- Technika ataku
- Liczba prób
- Adres IP atakującego
- Docelowy adres IP i port
- Kiedy atak został zablokowany ostatnio

Kliknięcie **Dodaj wykluczenia** dla wybranej detekcji automatycznie utworzy wpis w **Globalne Wykluczenia** w sekcji **Ochrona Sieci**.

Status Łatki Sieciowej

Sprawdź status aktualizacji oprogramowania zainstalowanego w sieci. Raport pokazuje następujące szczegóły:

- Komputer docelowy (nazwa punktu końcowego, adres IP i system operacyjny).
- Aktualizacje bezpieczeństwa (zainstalowane aktualizacje, aktualizacje zakończone niepowodzeniem, brakujące aktualizacje bezpieczeństwa i niezwiązane z bezpieczeństwem).
- Status i czas ostatniej modyfikacji dla sprawdzonych punktów końcowych.

Stan ochrony sieci

Zawiera szczegółowe informacje na temat ogólnego stanu bezpieczeństwa docelowych punktów końcowych. Na przykład możesz wyświetlić informacje o:

- Nazwa, IP i FQDN
- Stan:
  - **Ma problemy** punkt końcowy ma luki w ochronie (nieaktualny agent bezpieczeństwa, wykryte zagrożenia bezpieczeństwa, itp.)
  - **Brak problemów** - punkt końcowy jest chroniony i nie ma powodów do zmartwień.
  - **Nieznany** - punkt końcowy był offline podczas generowania raportu.
  - **Niezarządzany** - agent bezpieczeństwa nie został jeszcze zainstalowany na punkcie końcowym
- Dostępne warstwy ochrony
- Zarządzanie i niezarządzanie punkty końcowe (agent bezpieczeństwa jest zainstalowany lub nie)
- Typ i status licencji (dodatkowe kolumny związane z licencją są domyślnie ukryte)
- Stan infekcji (punkt końcowy jest „czysty" lub nie)
- Zaktualizuj stan produktu i zawartości zabezpieczeń
- Status poprawki zabezpieczeń oprogramowania (brak poprawek zabezpieczeń lub poprawek niezwiązanych z zabezpieczeniami)

W przypadku niezarządzanych punktów końcowych zobaczysz status **Niezarządzany** w innych kolumnach.

Skanowanie na żądanie

Zawiera informacje dotyczące wykonanych skanowań na żądanie na wybranych celach. Wykres kołowy wyświetla statystyki udanych i nieudanych skanowań. Tabela poniżej wykresu pokazuje szczegóły dotyczące typu skanowania, wystąpienia i ostatnie udane skanowaniae dla każdego punktu końcowego.

Zgodność Polityki

Zawiera informacje dotyczące zastosowanych polityk bezpieczeństwa na wybranych celach. Wykres kołowy wyświetla status polityki. W tabeli poniższej

wykresu, możesz zobaczyć przypisaną politykę każdego punktu końcowego i typ polityki, a także datę i użytkownika, który ją przypisał.

Nieudane zgłoszenia Sandbox Analyzer

Wyświetla wszystkie nieudane zgłoszenia obiektów wysyłanych z punktów końcowych do Sandbox Analyzer w określonym przedziale czasowym. Zgłoszenie jest uważane za nieudane po kilku ponownych próbach.

Na wykresie pokazano zróżnicowanie nieudanych zgłoszeń w wybranym okresie. W tabeli szczegółów raportu można sprawdzić, które pliki nie mogły zostać przesłane do Sandbox Analyzer, maszyny, z której został wysłany obiekt, datę i czas każdej ponownej próby, zwrócony kod błędu, opis każdej nieudanej próby i nazwę firmy.

Wyniki Sandbox Analyzer (Nieaktualne)

Dostarcza szczegółowe informacje dotyczące plików docelowych punktów końcowych, które zostały przeanalizowane w sandbox w określonym czasie. Na wykresie liniowym wyświetlana jest liczba czystych lub niebezpiecznych analizowanych plików, a tabela przedstawia szczegółowe informacje dotyczące każdego przypadku.

Możesz wygenerować raport Wyników Sandbox Analyzer dla wszystkich analizowanych plików lub tylko tych wykrytych jako złośliwe.

Możesz zobaczyć:

- Werdykt analizy, mówiący czy plik jest czysty, niebezpieczny lub nieznany (**Wykryto zagrożenie** / **Nie wykryto zagrożenia** / **Niepotwierdzone**). Kolumna pokazuje się tylko wtedy, gdy wybierzesz raport, aby wyświetlić wszystkie analizowane obiekty.

  Aby zobaczyć pełną listę plików i rozszerzeń obsługiwanych przez , Sandbox Analyzer przejdź do „Obsługiwane Typy Plików i Rozszerzenia do Wysyłania Ręcznego” (p. 520).
- Rodzaj zagrożenia, taki jak adware, rootkit, downloader, exploit, host-modifier, malicious tools, password stealer, ransomware, spam lub trojan.
- Data i godzina wykrycia - możesz je filtrować zależnie od okresu raportowania.
- Nazwa hosta lub IP punktu końcowego, na którym wykryto pliki.
- Nazwa pliku, jeśli zostały wysłane osobno, lub liczbę analizowanych plików w przypadku pakietu. Kliknij link nazwy pliku lub pakietu, aby zobaczyć szczegóły i podjęte działania.

- Status działania naprawczego dla wysłanych plików (**Częściowe**, **Nieudane**, **Tylko Zgłoszone**, **Udane**).
- Nazwa firmy.
- Więcej informacji na temat właściwości analizowanego pliku można uzyskać klikając **Więcej informacji** w kolumnie **Wynik analizy**. Tutaj można przeglądać informacje o zabezpieczeniach i szczegółowych raportach dotyczących zachowania próbek.

Sandbox Analyzer wychwytuje następujące wydarzenia behawioralne:

- Pisanie / usuwanie / przenoszenie / duplikowanie / zamienianie plików w systemie i na dysku przenośnym.
- Wykonanie nowo utworzonych plików.
- Zmiany w systemie plików.
- Zmiany w aplikacjach uruchomionych na maszynie wirtualnej.
- Zmiany w w pasku zadań i menu startowym Windows.
- Procesy tworzenia / zakończania / wstrzykiwania.
- Pisanie / usuwanie kluczy rejestracji.
- Tworzenie obiektów mutex.
- Tworzenie / uruchamianie / wstrzymywanie / modyfikowanie / wyszukiwanie / usuwanie usług.
- Zmiana ustawień bezpieczeństwa przeglądarki.
- Zmiana ustawień wyświetlania Windows Explorer.
- Dodawanie plików do listy wyjątków zapory sieciowej.
- Zmiana ustawień sieci.
- Włączanie wykonywania przy uruchamianiu systemu.
- Łączenie z hostem zdalnym.
- Uzyskiwanie dostępu do określonych domen.
- Transfer danych do i z określonych domen.
- Uzyskiwanie dostępu do URL, IP i portów, poprzez różne protokoły komunikacyjne.
- Sprawdzanie wskaźników środowiska wirtualnego.
- Sprawdzanie wskaźników narzędzi monitorujących.
- Tworzenie snapshotów.
- SSDT, IDT, IRP hooks.
- Zrzuty pamięci dla podejrzanych procesów.
- Funkcje połączeń z Windows API.
- Pozostawanie nieaktywnym przez określony czas, aby opóźnić wykonanie.
- Tworzenie plików z zadaniami, które mają być wykonywane w określonych przedziałach czasowych.

W oknie **Wyniki Analizy** kliknij przycisk **Pobierz**, aby zapisać na swoim komputerze zawartość Podsumowania Zachowań w formatach: XML, HTML, JSON, PDF.

Ten raport będzie nadal obsługiwany przez ograniczony czas. Zaleca się, aby zamiast kart przesyłania zebrać niezbędne informacje na temat analizowanych próbek. Karty przesyłania są dostępne w sekcji **Sandbox Analyzer**, w menu głównym Control Center.

Audyt Bezpieczeństwa

Zawiera informacje na temat zdarzeń związanych z bezpieczeństwem, które miały miejsce na wybranym celu. Informacja odnosi się do następujących zdarzeń:

- Wykrywanie Malware
- Zablokowana aplikacja
- Zablokowany Port Skanowania
- Zablokowany Ruch
- Zablokowana strona www
- Blokuj urządzenie
- Zablokowany e-mail
- Zablokowany Proces
- Zdarzenia HVI
- Zdarzenia Zaawansowanego Anty-Exploit
- Zdarzenia Network Attack Defense
- Detekcja Ransomware

Security Server Status

Pomaga ocenić stan docelowych Security Server. Możesz zidentyfikować problem dla każdego Security Server z pomocą różnych wskaźników stanu, takich jak:

- **Status**: pokazuje ogólny Security Server status.
- **Status Maszyny**: informuje które urządzenia Security Server zakończyły swoje działanie.
- **Status AV**: wskazuje, czy moduł antymalware jest włączony lub wyłączony.
- **Stan Aktualizacji**: wyświetla czy urządzenia Security Server zostały zaktualizowane lub czy aktualizacje zostały zablokowane.
- **Status obciążenie**: wskazuje poziom obciążenia skanowania Security Server jak opisano tutaj:

- **Nieobciążony**, gdy stosuje się mniej niż 5% jego pojemności skanowania.
- **Normalny**, gdy obciążenie skanowania jest zrównoważone.
- **Przeciążony**, gdy obciążenie skanowania przekracza 90% jego pojemności. W tym przypadku, sprawdź polityki bezpieczeństwa. Jeśli wszystkie Security Server przydzielone w ramach polityki są przeciążone, musisz dodać kolejny Security Server do listy. W przeciwnym razie, należy sprawdzić połączenia sieciowe między klientami a Security Server bez problemów obciążenia.

- **HVI chronione VMs**: informuje o maszynach wirtualnych, które są monitorowane i chronione przez moduł HVI.
- **status HVI**: wskazuje czy moduł HVI jest włączony lub nie. HVI jest włączony jeśli jednocześnie Security Server oraz Pakiet Uzupełniający są zainstalowane na hoście.
- **Podłączone Urządzenia Pamięci**: informuje, ile urządzeń pamięci zgodnych z ICAP jest podłączonych do Security Server. Kliknięcie numeru wyświetli listę urządzeń pamięci masowej wraz ze szczegółami dla każdego: nazwa, adres IP, typ, data i godzina ostatniego połączenia.
- **Status Skanowania Pamięci**: wskazuje, czy usługa Security for Storage jest włączona czy wyłączona.

Ponadto można zobaczyć, ilu agentów jest podłączonych do Security Server. Kliknięcie w liczbę podłączonych klientów, wyświetli listę punktów końcowych. Te punkty końcowe mogą być zagrożone, jeśli Security Server ma problemy.

Top 10 wykrytych malware

Pokazuje top 10 wykrytych malware w określonym czasie na wybranych końcówkach.

> **Notatka**
> Szczegółowa tabela wyświetla wszystkie końcówki, które są zainfekowane przez wykryte malware należące do top 10.

Top 10 Zainfekowanych Punktów Końcowych

Pokazuje Ci top 10 najbardziej zainfekowanych końcówek według ilości wykrytych infekcji w określonym czasie bez wybranych końcówkach.

Notatka
Szczegółowa tabela wyświetla wszystkie wykryte malware w top 10 zainfekowanych końcówek.

Stan aktualizacji
Pokazuje status aktualizacji dla agenta ochrony lub Security Server zainstalowanego na wybranych celach. Status aktualizacji odnosi się do produktu i wersji zawartości zabezpieczeń.

Używając dostępnych filtrów, możesz łatwo znaleźć, którzy klienci dokonali aktualizacji i którzy nie, w ciągu ostatnich 24 godzin.

W tym raporcie można szybko przenieść agentów do najnowszej wersji. Aby to wykonać, kliknij przycisk **Aktualizacja** z paska narzędzi nad tabelą danych.

Stan aktualizacji
Pokazuje listę agentów bezpieczeństwa zainstalowanych na wybranych obiektach oraz czy nowsze rozwiązania są dostępne.

Dla punktów końcowych z zainstalowanymi starszymi wersjami agentów, możesz szybko zainstalować najnowsze wspierane wersje agentów ochrony poprzez kliknięcie przycisku **Aktualizacja**.

Notatka
Ten raport jest dostępny tylko gdy rozwiązanie GravityZone zostało zaktualizowane.

Status ochrony sieci maszyn wirtualnych
Informuje o ochronie Bitdefender w zasięgu Twojej sieci. Dla każdego z wybranych maszyn można zobaczyć, który komponent rozwiązuje problemy z bezpieczeństwem:

- Security Server, dla bezagentowego wdrożenia w VMware NSX lub środowisku vShied, i dla HVI
- Agent ochrony, w każdej innej sytuacji

Aktywność HVI
Informuje Ciebie o wszystkich atakach, które moduł HVI wykrył na wybranych maszynach w określonym okresie czasu.

Raport zawiera również informacje o dacie i godzinie ostatniego wykrytego incydentu, który zaangażował monitorowany proces, o ostatecznym statusie działań podjętych przed atakiem, użytkowniku, na którym proces się rozpoczął i komputerze docelowym.

W zależności od podjętych działań, ten sam proces może być zgłaszany wielokrotnie. Na przykład, jeśli proces po raz kolejny został zabity, a kolejnym razem odmówiono dostępu, będziesz widział dwie pozycje w tabeli raportu.

Dla każdego procesu, po kliknięciu daty ostatniej detekcji, wyświetlony zostanie odrębny rejestr wszystkich przypadków wykrytych od rozpoczęcia procesu. Dziennik ujawnia ważne informacje, takie jak typ i opis incydentu, źródło i cel ataku i działania podjęte w celu rozwiązania problemu.

W tym raporcie, możesz szybko poinstruować moduł ochrony aby ignorował wybrane zdarzenia, które uważasz za bezpieczne. Aby to wykonać, kliknij przycisk **Dodaj wyjątek** z paska narzędzi nad tabelą danych.

Notatka
Moduł HVI dla Twojego rozwiązania GravityZone może być dostępny z oddzielnym kluczem licencyjnym.

Status Iniekcji Zewnętrznych Narzędzi HVI

Przedstawia szczegółowy stan każdego wstrzyknięcia w docelowych punktach końcowych. Informacja zawiera:

- Nazwa punktu końcowego.
- Nazwa wstrzykniętego narzędzia.
- Adres IP punktu końcowego.
- System operacyjny gościa.
- Wyzwalanie. To może być naruszenie pamięci, zadanie na żądanie lub zaplanowany przebieg.
- Liczba pomyślnych przebiegów. Kliknięcie liczby spowoduje wyświetlenie okna ze ścieżką dzienników i znacznikiem czasu dla każdego uruchomienia narzędzia. Kliknięcie ikonki znajdującej się obok ścieżki skopiuje ją do schowka.
- Liczba nieudanych przebiegów. Kliknięcie liczby spowoduje wyświetlenie okna, w którym można zobaczyć przyczynę niepowodzenia i znacznik czasu.
- Ostatnia udana iniekcja.

Wstrzyknięcia są pogrupowane według docelowych punktów końcowych. Raport można filtrować w celu wyświetlenia danych związanych tylko z określonym narzędziem, korzystając z opcji filtrowania w nagłówku tabeli.

Aktywność ransomware

Informuje Cię o atakach ransomware, które GravityZone wykrył na zarządzanych przez Ciebie punktach końcowych i dostarcza niezbędnych narzędzi do odzyskania zaszyfrowanych podczas ataku plików.

Raport jest dostępny jako strona w Control Center, odrębna od innych raport, można do niej uzyskać dostęp bezpośrednio z głównego menu GravityZone.

Strona **Aktywność Ransomware** zawiera siatkę, która dla każdego z ataków ransomware pokazuje następująco:

- Nazwa, adres IP i FQDN punktu końcowych na którym miał miejsce atak
- Firma, w której znajduje się punkt końcowy.
- Nazwa użytkownika zalogowanego podczas ataku
- Rodzaj ataku, lokalny czy zdalny
- Proces jaki ransomware uruchomiło w przypadku lokalnego ataku lub adres IP z którego odbył się atak dla zdalnego ataku
- Data i czas wykrycia
- Liczba zaszyfrowanych plików przed zablokowaniem ataku
- Status akcji przywracania dla wszystkich plików na wybranym punkcie końcowym

Niektóre dane są domyślnie ukryte. Kliknij **Pokaż/Ukryj Kolumny** w prawym górnym rogu, aby skonfigurować dane które chcesz zobaczyć w siatce. Jeżeli masz wiele wpisów w siatce, możesz ukryć filtry używając **Pokaż/Ukryj filtry** w prawym górnym rogu strony.

Dodatkowe informacje są dostępne po kliknięciu w liczbę plików. Możesz zobaczyć listę z pełną ścieżką do oryginalnych i przywróconych plików i status przywrócenia dla wszystkich plików związanych z wybranym atakiem ransomware.

WAŻNE
Kopie zapasowe są dostępne maksymalnie przez 30 dni. Pamiętaj proszę o dacie do której pliki wciąż mogą być odzyskane.

Aby odzyskać pliki z ransomware:

1. Wybierz ataki w siatce.

2. Kliknij **Przywróć pliki**. Pojawi się okno z potwierdzeniem.

   Utworzone zostanie zadanie przywracania. Możesz sprawdzić jego status na stronie **Zadania**, zupełnie jak inne zadania w GravityZone.

Jeżeli detekcje są wynikiem nieszkodliwych procesów, wykonaj następujące kroki:

1. Wybierz rekordy w siatce.
2. Kliknij **Dodaj wykluczenie**.
3. W nowym oknie, wybierz polityki dla których ma obowiązywać wykluczenie.
4. Kliknij **Dodaj**.

   zaaplikuje wszystkie możliwe wykluczenia: na folder, na proces i na adres IP.

   Możesz je sprawdzić lub zmodyfikować w sekcji polityki **Antymalware > Ustawienia > Niestandardowe Wykluczenia**.

Notatka
Aktywność Ransomware przechowuje dane o zdarzeniach przez dwa lata.

9.1.2. Raporty Serwera Exchange

To są dostępne typy raportów dla Serwerów Exchange:

Exchange - Zablokowana Zawartość i Załączniki
Dostarcza informacje na temat e-maili lub załączników usuniętych przez Kontrolę Zawartości z wybranych serwerów w określonym przedziale czasowym. Informacja zawiera:

- Adres e-mail nadawcy i odbiorcy.

  Gdy wiadomość posiada więcej odbiorców, zamiast adresu e-mail, raport wyświetla liczbę odbiorców z linkiem do okna zawierającego listę adresów e-mail.
- Temat e-maila.
- Typ wykrycia, określający filtr Kontroli Zawartości wykrył zagrożenie.
- Akcja podjęta podczas wykrycia.
- Serwer na których zostało wykryte zagrożenie.

Exchange - zablokowane nieskanowalne załączniki

Zawiera informacje na temat wiadomości e-mail zawierających nieskanowalne załączniki (nadmiernie skompresowane, chronione hasłem, itp.), zablokowane na wybranych serwerach pocztowych Exchange w określonym okresie czasu. Informacja odnosi się do:

- Adres e-mail nadawcy i odbiorcy.

  Gdy wiadomość jest wysyłana do większej ilości odbiorców, zamiast adresu e-mail, raport wyświetla liczbę odbiorców z linkiem do okna zawierającego listę adresów e-mail.

- Temat e-maila.
- Działania podjęte w celu usunięcia nieskanowalnych załączników:
  - **Usunięty E-mail** wskazuje, że cały e-mail został usunięty.
  - **Usunięte Załączniki**, ogólna nazwa dla wszystkich działań, które usuwają załączniki z wiadomości e-mail, takie jak usuwanie załącznika, przenoszenie do kwarantanny lub zastąpienie go z powiadomieniem.

  Klikając link w kolumnie **Akcja**, można wyświetlić szczegółowe informacje na temat każdego zablokowanego załącznika i odpowiedniego podjętego działania.
- Data i czas wykrycia.
- Serwer, na którym wykryto e-mail.

Exchange - skanowanie wiadomości e-mail

Wyświetla statystyki podjętych przez moduł Ochrony Exchange działań w określony przedziale czasowym.

Akcje są grupowane pod kątem typu wykrycia (malware, spam, zabronione załączniki i zabroniona zawartość) i serwera.

Statystki odnoszą się do następujących statusów wiadomości e-mail:

- **Poddane Kwarantannie.** Te adresy e-mail zostały przeniesione do folderu Kwarantanny.
- **Usunięte/Odrzucone.** Te e-maile zostały usunięte lub odrzucone przez serwer.
- **Przekierowany.** Te e-maile przekierowane są do adresów e-mail dostarczonych w politykach.

- **Wyczyszczone i dostarczone.** Te e-maile posiadają usunięte zagrożenia i przeszły przez filtry.

  E-mail uznawany jest za wyczyszczony w momencie gdzie wszystkie wykryte załączniki zostały zdezynfekowane, przesłane do kwarantanny, skasowane lub zastąpione tekstem.

- **Zmodyfikowane i dostarczone.** Informacje skanowania zostały dodane do nagłówków wiadomości e-mail, które zostały przepuszczone przez filtry.

- **Dostarczone bez żadnych innych akcji.** Te wiadomości e-mail zostały zignorowane przez Ochronę Exchange i przeszły przez filtry.

Exchange - aktywność malware'u

Dostarcza Ci informacji na temat e-maili i zagrożeń malware, wykrytych na wybrany serwerze mailowym Exchange na określony okres czasu. Informacja odnosi się do:

- Adres e-mail nadawcy i odbiorcy.

  Gdy wiadomość jest wysyłana do większej ilości odbiorców, zamiast adresu e-mail, raport wyświetla liczbę odbiorców z linkiem do okna zawierającego listę adresów e-mail.

- Temat e-maila.

- Status e-maila po skanowaniu antymalware.

  Po kliknięciu statusu linku, możesz zobaczyć szczegóły dotyczące wykrytego malware i podjętych działań.

- Data i czas wykrycia.

- Serwer na których zostało wykryte zagrożenie.

Zamiana - Top 10 wykrytych malware

Informuje Ciebie o 10 najczęściej wykrywanych zagrożeniach malware wykrywanych w załącznikach e-maili. Możesz wygenerować dwa widoki zawierające różne statystyki. Jeden widok pokazuje liczbę wykryć przez poszkodowanych odbiorców, a drugi przez nadawców.

Dla przykładu, GravityZone wykrył jeden e-mail z zainfekowanym załącznikiem, wysłanym do pięciu odbiorców.

- W widoku odbiorców:
  - Raport pokazuje 5 wykryć.

- Szczegóły raportu pokazują tylko odbiorców, nie nadawców.

- W widoku nadawców:
  - Raport pokazuje jedno wykrycie.
  - Szczegóły raportu pokazują tylko nadawcę, nie odbiorcę.

Po za nadawcą/odbiorcą i nazwą malware, raport dostarcza następujące informacje:

- Typy malware (wirusy, spyware, PUA, itp.)
- Serwer na których zostało wykryte zagrożenie.
- Miary które podjął moduł antimalware.
- Data i czas ostatniego wykrycia.

Zamiana - Top 10 Odbiorców Malware
Pokazuje 10 najczęściej atakowanych przy pomocy malware odbiorców e-maili w określonym przedziale czasowym.

Szczegóły raportu dostarczają kompletną listę malware, które miało wpływ na odbiorców wraz z podjętymi działaniami.

Exchange - Top 10 Odbiorców Spam
Pokazuje 10 odbiorców wiadomości email, którzy otrzymali największą liczbę spamu oraz wiadomości zawierających phishingowych wykrytych w określonym przedziale czasowym. Raport zawiera również informacje z działań stosowanych do poszczególnych e-maili.

9.1.3. Raporty Urządzenia Przenośnego

Notatka
Ochrona malware i powiązane raporty dostępne tylko dla urządzeń Android.

To jest lista dostępnych rodzajów raportów dla urządzeń przenośnych:

Status szkodliwego oprogramowania
Pomoże Ci znaleźć ile z docelowych urządzeń przenośnych zostało zarażonych malware w określonym przedziale czasowym i jak poradzono sobie z zagrożeniami. Urządzenia przenośne są pogrupowane w oparciu o te kryteria:

- Urządzenia przenośne bez wykrycia (nie ma zagrożenia malware został wykryty przez określony okres czasu)

- Urządzenia Przenośne na których wszystkie wykryte pliki malware zostały usunięte.
- Urządzenia Przenośne z istniejącymi malware (niektóre wykryte pliki nie zostały usunięte)

Top 10 zainfekowanych urządzeń
Pokazuje 10 najbardziej zainfekowanych urządzeń przenośnych w określonym czasie na docelowych urządzeniach przenośnych.

> **Notatka**
> Szczegółowa tabela wyświetla wszystkie wykryte malware w top 10 zainfekowanych urządzeń przenośnych.

Top 10 wykrytych malware
Pokazuje top 10 wykrytych malware w określonym czasie na docelowych urządzeniach przenośnych.

> **Notatka**
> Szczegółowa tabela wyświetla wszystkie urządzenia przenośne, które są zainfekowane przez wykryte malware należące do top 10.

Zgodność urządzenia
Informuje o statusie zgodności z docelowymi urządzeniami przenośnymi. Możesz zobaczyć nazwę urządzenia, stan, system operacyjny i powód niezgodności.

Aby uzyskać więcej informacji na temat wymagań zgodności, proszę sprawdzić „Niezgodne kryteria” (p. 396).

Synchronizacja urządzenia
Informuje o statusie synchronizacji z docelowymi urządzeniami przenośnymi. Możesz zobaczyć nazwę urządzenia, przypisanego użytkownika, stan synchronizacji, system operacyjny i czas ostatniej dostępności online.

Aby uzyskać więcej informacji, odwołaj się do „Sprawdzanie Statusu Urządzeń Mobilnych” (p. 172).

Zablokowane strony
Informuje o ilości prób jakie docelowe urządzenie ma na połączenie się ze stroną, która jest zablokowana przez zasady **Dostęp do Sieci**, w określonym przedziale czasu.

Dla każdego urządzenia z wykryciami zagrożeń, naciśnij liczbę zapewnionych kolumn **Zablokowane strony internetowe** aby zobaczyć szczegółowe informacje dla każdej zablokowanej strony sieciowej, takie jak:

- Adres URL
- Elementy polityki, która przeprowadza działania
- Liczba zablokowanych prób
- Ostatni raz kiedy strona była zablokowana

Aby uzyskać więcej informacji ustawieniach dostępu przez sieć polityki, odwołaj się do „Tryby" (p. 402).

Aktywność bezpieczeństwa sieci Web

informuje o liczbie prób jakie podjęły docelowe urządzenia przenośne aby uzyskać dostęp do zarażonych stron internetowych (phishing, fraud, malware or niezaufane strony) w określonym przedziale cenowym. Dla każdego urządzenia z wykryciami zagrożeń, naciśnij liczbę zapewnionych kolumn Zablokowane strony internetowe aby zobaczyć szczegółowe informacje dla każdej zablokowanej strony sieciowej, takie jak:

- Adres URL
- Rodzaj zagrożenia (phishing, malware, fraud, untrusted)
- Liczba zablokowanych prób
- Ostatni raz kiedy strona była zablokowana

Bezpieczeństwo Sieci jest elementem polityki, który wykrywa i blokuje strony z problemami bezpieczeństwa. Aby uzyskać więcej informacji o ustawieniach bezpieczeństwa sieciowych polityki, odwołaj się do „Bezpieczeństwo" (p. 391).

9.2. Tworzenie raportów

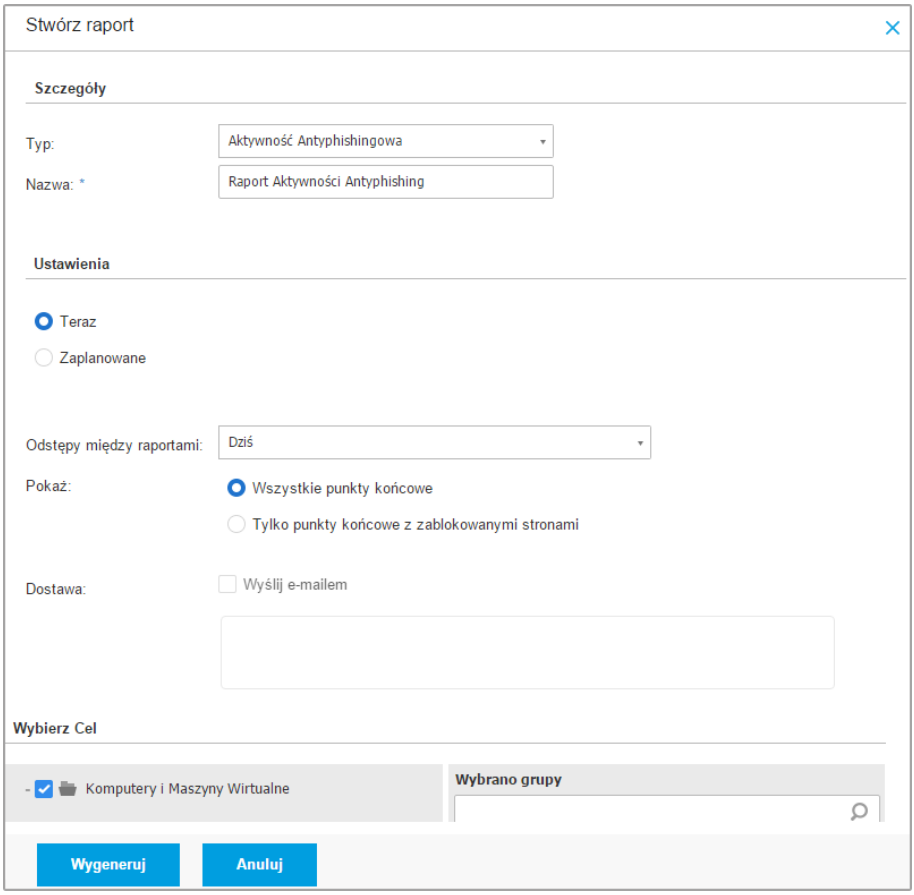
Możesz utworzyć dwie kategorie raportów:

- **Raporty natychmiastowe.** Natychmiastowe raporty sa automatycznie wyświetlane po wygenerowaniu.
- **Zaplanowane raporty.** Zaplanowane raporty mogą być skonfigurowane do okresowego uruchamiania w określonym czasie i terminie. Lista wszystkich zaplanowanych raportów jest wyświetlana na stronie **Raporty**.

WAŻNE
Raporty natychmiastowe są automatycznie usuwane kiedy zamykasz stronę raportów. raporty zaplanowane są zapisane i wyświetlone na stronie **Raporty**.

aby stworzyć raport:

1. Przejdź do strony **Raporty**.
2. Wybierz typ obiektu sieciowego z selektora widoku.
3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlono okno konfiguracji.



Opcje Raportowania Komputerów i Maszyn Wirtualnych

4. Wybierz interesujący cię rodzaj raportu z menu. Aby uzyskać więcej informacji, odwołaj się do „Typy Raportu” (p. 415)
5. Podaj sugestywną nazwę dla raportu. Kiedy wybierasz nazwę, weź pod uwagę rodzaj raportu, cel i ewentualne opcje raportu.
6. Skonfiguruj powtórzenia raportu:
   - wybierz **Teraz** aby stworzyć natychmiastowy raport.

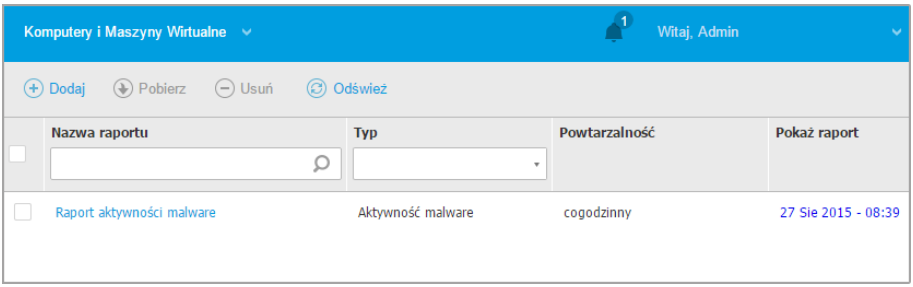
- Wybierz **Planowane** aby skonfigurować raport, który zostanie automatycznie wygenerowany w określonym czasie:
  - Po godzinach, w określonym przedziale pomiędzy godzinami.
  - Codziennie. W tym przypadku, można także ustawić czas rozpoczęcia (godzinę i minuty).
  - Raz w tygodniu, w określonych dniach tygodnia i o określonym czasie rozpoczęcia (godzinę i minuty).
  - Raz w miesiącu, w określonych dniach miesiąca i o określonym czasie rozpoczęcia (godzinę i minuty).

7. dla większości rodzajów musisz określić przedział czasu, których zawarte dane się odnoszą. Raport wyświetli tylko dane z wybranego przedziału czasu.
8. Kilka rodzajów raportów zapewniają opcje filtrowania, aby pomóc Ci łatwo znaleźć informacje, które Cię interesują. Użyj opcji filtrowania opcji w sekcji **Pokaż** w celu uzyskania jedynie potrzebnych informacji.

   Na przykład dla raportu **Status Aktualizacji** możemy ustalić wyświetlanie jedynie listy obiektów sieci, które nie były zaktualizowane lub tych, które potrzebują być uruchomione ponownie, by dokończyć aktualizację.
9. **Dostawa**. Aby otrzymać zaplanowany raport za pośrednictwem poczty elektronicznej, zaznacz odpowiednie pole wyboru. Podaj adres e-mail, który chcesz w polu poniżej. Domyślnie wiadomość zawiera archiwum z obu raportów plików (PDF i CSV). Użyj pól wyboru w sekcji **Dołącz pliki** aby dostosować, które pliki i jak mają być wysłane przez email.
10. **Wybierz cel**. Przewiń w dół, aby skonfigurować cel raportu. Wybierz jedną lub więcej grup punktów końcowych, które chcesz zawrzeć w raporcie.
11. W zależności od wybranej rekurencji, kliknij **Generuj** w celu utworzenia błyskawicznego raportu lub **Zapisz** by utworzyć zaplanowany raport.
    - Błyskawiczny raport zostanie wyświetlony natychmiast po kliknięciu przycisku **Generuj**. Czas wymagany do utworzenia raportów uzależniony jest od liczby zarządzanych obiektów sieciowych. Zaczekaj na stworzenie raportu.
    - Zaplanowane raporty będą wyświetlały się jako lista na stronie **Raporty**. Gdy raport instancji zostanie utworzony, możemy uzyskać raport klikając na odpowiednie łącze w kolumnie **Zobacz raport** na stronie **Raporty**.

9.3. Przeglądania i zarządzanie zaplanowanych raportów

Aby zobaczyć i zarządzać zaplanowanymi raportami przejdź do strony **Raporty**.



Strona Raportów

Wszystkie zaplanowane raporty wyświetlane są w tabeli wraz z użytecznymi informacjami na ich temat:

- Nazwa i rodzaj raportu
- Rekurencja raportów
- Ostatnio wygenerowana instancja.

Notatka
Zaplanowane raporty są dostępne tylko dla użytkownika, który je stworzył.

Aby posortować raporty według określonej kolumny, naciśnij na nagłówek kolumny. Kliknij nagłówek ponownie, aby zmienić kolejność porządkowania.

Aby łatwo znaleźć to, czego szukasz, skorzystaj z pola wyszukiwania lub poniżej opcje filtrowania w nagłówkach kolumn.

Aby wyczyścić pole wyszukiwania, umieść nad nim kursor i kliknij w ikonę × **Usuń**.

Aby upewnić się, że zostają wyświetlane najnowsze informacje, kliknij przycisk **Odśwież** z górnej części tabeli.

9.3.1. Przeglądanie raportów

Aby zobaczyć raport:

1. Przejdź do strony **Raporty**.

2. Sortowanie raportów po nazwie, rodzaju lub powtarzalność, aby łatwo znaleźć raport, którego szukasz.
3. Naciśnij odpowiedni link w kolumnie **Zobacz raport** aby wyświetlić raport. Najnowszy raport instancji zostanie wyświetlony.

   By zobaczyć wszystkie instancje raportów, odnieś się do„Zapisywanie raportów” (p. 443)

Wszystkie raporty składają się z sekcji podsumowania (górna część raportu) i sekcji szczegółów (dolna część raportu).

- Sekcja podsumowania umożliwia dostęp do danych statystycznych (wykresy kołowe i grafy) wszystkich wybranych obiektów sieciowych, jak również ogólnych informacji o raportach, takich jak okresy raportowania (jeśli stosowane), cele raportowania itp.
- Sekcja szczegóły dostarcza informacji o wybranym obiekcie sieciowym.

Notatka

- Aby skonfigurować informacje wyświetlone na wkresie, nacisnij legendę wpisów, aby pokazać lub ukryć wybrane dane.
- Kliknij w tabeli graficzną część (wykresu kołowego, słupkowego), którego szczegóły ciebie interesują.

9.3.2. Edytowanie zaplanowanego raportu.

Notatka
kiedy edytujesz zaplanowany raport, aktualizacja zostanie zastosowana od następnego uruchomienia raportu. Wcześniej generowane raporty nie zostanie zmieniona przez edycję.

Aby zmienić ustawienia zaplanowanego raportu:

1. Przejdź do strony **Raporty**.
2. Naciśnij nazwę raportu.
3. Zmień ustawienia raportu jeżeli potrzebujesz. Możesz zmienić jedną z następujących:
   - **Nazwa raportu.** Wybierz sugestywna nazwę dla raportu, aby w łatwy sposób móc zidentyfikować co zawiera. Kiedy wybierasz nazwę, weź pod uwagę

rodzaj raportu, cel i ewentualne opcje raportu. Raporty wygenerowane przez zaplanowany raport jest nazwany po nim.

- **Wznowienie raportu (harmonogram).** Możesz zaplanować automatyczne generowanie raportu godzinne(w odstępie godzinowym), dzienne (w odstępie dziennym), tygodniowe (w konkretnym dniu tygodnia o danej godzinie) lub miesięcznie (konkretnego dnia miesiąca o danej godzinie). W zależności od wybranego planu, raport będzie zawierał tylko dane z ostatniego dnia, tygodnia lub miesiąca, odpowiednio.
- **Ustawienia**
  - Możesz zaplanować automatyczne generowanie raportu godzinne(w odstępie godzinowym), dzienne (w odstępie dziennym), tygodniowe (w konkretnym dniu tygodnia o danej godzinie) lub miesięcznie (konkretnego dnia miesiąca o danej godzinie). W zależności od wybranego planu, raport będzie zawierał tylko dane z ostatniego dnia, tygodnia lub miesiąca, odpowiednio.
  - Raport będzie zawierał dane z wybranego przedziału czasu. Możesz zmienić przedział czasu przy następnym uruchomieniu.
  - Większość raportów zapewnia opcje filtrowania, które pomogą ci łatwo znaleźć informacje które Cie interesują. Kiedy przeglądasz raport na konsoli, wsyztskie informacje będą dostepne, niezależnie od wybranych opcji. Jeżeli pobierasz lub wysyłasz raport e-mailem, tylko podsumowanie raportu i wybrane informacje zostaną załączone do pliku PDF. Szczegóły raportu będą dostępne tylko w formacie CSV.
  - Możesz wybrać aby dostać raport mailem.
- **Wybierz cel.** Wybrana opcja wskazuje rodzaj aktualnego raportu docelowego (zarówno grupy jak i indywidualne obiekty sieciowe). Naciśnij odpowiadający link aby wyświetlić aktualny raport docelowy. aby zmienić, wybierz grupy i obiekty sieciowe, które mają byc zawarte w raporcie.

4. Naciśnij **Zapisz** aby zastosować zmiany.

9.3.3. Usuwanie zaplanowanych raportów

Kiedy zaplanowany raport nie jest dłużej potrzebny, najlepiej go usunąć. Kasowanie zaplanowanych raportów usunie wszystkie instancje które wygenerowały raporty aż do tego momentu.

Aby usunąć zaplanowany raport:

1. Przejdź do strony **Raporty**.
2. Wybierz raport, który chcesz usunąć.
3. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli.

9.4. Podejmowanie działań związanych z raportami

Podczas gdy większość raportów tylko wyszczególnia zdarzenia w sieci, niektóre z nich również oferują kilka możliwości naprawienia za pomocą jednego kliknięcia problemów, na które napotkają.

By naprawić problem występujący w raporcie, kliknij odpowiedni przycisk z paska narzędzi akcji ponad tabelą.

Notatka
Musisz posiadać prawa **Zarządzania Siecią** by wykonać tą akcję.

Oto dostępne dla każdego raportu opcje:

Zablokowane aplikacje

- **Dodaj Wyjątek**. Dodaje wykluczenie w polityce, aby zapobiec ponownemu blokowaniu tej aplikacji przez moduły ochrony.
- **Dodaj regułę**. Zdefiniuj regułę dla aplikacji lub procesu w Kontroli Aplikacji.

Aktywność HVI

- **Dodaj wyjątek**. Dodaje wykluczenie w polityce, aby zapobiec ponownym zgłoszeniom tego incydentu przez moduł ochrony.

Status szkodliwego oprogramowania

- **Skanuj zainfekowane cele**. Uruchamia zadanie wstępnego Pełnego Skanowania na celu wykazującym się jako nadal zainfekowany.

Stan aktualizacji

- **Aktualizacja**. Aktualizuje klientów docelowych do najnowszej dostępnej wersji.

Stan aktualizacji

- **Upgrade**. Zamień stare klienty końcówek na najnowszą generację dostępnych produktów.

9.5. Zapisywanie raportów

Domyślnie, zaplanowane raporty są automatycznie zapisywane w Control Center.

Jeżeli potrzebujesz żeby raporty były dostępne przez dłuższy okres czasu, możesz zapisać je na komputerze. Podsumowanie raportu będzie dostępne w formacie PDF, gdzie szczegóły raportu będą dostępne tylko w formacie CSV.

Masz dwie możliwości zapisywania raportów:

- Eksport
- Pobierz

9.5.1. Eksportowanie raportów

Aby wyeksportować raport do twojego komputera:

1. Wybierz format i kliknij **Eksportuj CSV** lub **Eksportuj PDF**.
2. W zależności od ustawień przeglądarki, plik można pobrać automatycznie do domyślnej lokalizacji pobierania, lub określić folder docelowy w oknie pobierania, które się pojawi.

9.5.2. Raporty pobierania

Archiwum Raport zawiera zarówno podsumowanie raportów i szczegółowych raportów.

Aby pobrać archiwum raportu:

1. Przejdź do strony **Raporty**.
2. wybierz raport jaki chcesz zapisać.
3. Naciśnij przycisk **Pobierz** i wybierz **Ostatnia Instancja**, aby pobrać ostatni wygenerowany raport lub **Pełne Archiwum** aby pobrać archiwum zawierające wszystkie instancje.

   W zależności od ustawień przeglądarki, plik można pobrać automatycznie do domyślnej lokalizacji pobierania, lub określić folder docelowy w oknie pobierania, które się pojawi.

9.6. Raporty E-mailów

Możesz wysłać raporty na e-mail używając poniższych opcji:

1. Aby wysłać emailem raport który przeglądasz, kliknij **Email**. Raport zostanie wysłany na adres E-mail połączony z Twoim kontem.
2. Aby skonfigurować zaplanowane raporty dostawy e-mail:
   a. Przejdź do strony **Raporty**.
   b. Naciśnij wybraną nazwę raportu.
   c. W **Ustawienia > Dostawa**, wybierz **Wyślij mailem o**.
   d. Podaj odpowiedni adres e-mail w polu poniżej. Możesz dodać dowolną liczbę adresów poczty elektronicznej.
   e. Kliknij **Zapisz**.

> **Notatka**
> Tylko podsumowanie raportu i wykres zostaną uwzględnione w pliku PDF wysłanym przez e-mail. Szczegóły raportu będą dostępne w pliku CSV.

Raporty są teraz wysyłane mailem jako archiwa .zip.

9.7. Drukowanie raportów

Control Center nie obsługuje obecnie funkcji przycisku drukowania. aby wydrukować raport, musisz najpierw zapisać go na swoim komputerze.

9.8. Kreator Raportu

W Control Center, możesz utworzyć i zarządzać zapytaniami, aby uzyskać szczegółowe raporty, które pozwalają zrozumieć każde zdarzenie lub zmianę, które miały miejsce w sieci, w dowolnym momencie.

Zapytania dostarczają ci możliwość zbadania problemów z ochroną, korzystając z różnych kryteriów, w międzyczasie utrzymując informacje zwięzłe i w najlepszym porządku. Z filtrami, możesz grupować punkty końcowe według określonych kryteriów, a następnie wybierać odpowiednie dane dla Twojego celu.

Z raportu opartego na zapytaniu można dowiedzieć się szczegółów, takich jak kiedy nastąpiło zdarzenie, ile punktów końcowych jest naruszonych, którzy użytkownicy zostali zalogowani w chwili zdarzenia, jakie zostały zastosowane polityki, status agenta bezpieczeństwa, podjęte działania, na jednym punkcie końcowym lub na grupie punktów końcowych.

Wszystkie raporty oparte na zapytaniach są dostępne w Control Center, ale możesz je zapisać na swoim komputerze lub wysłać je mailem. Dostępne formaty zawierające Przenośny format dokumentu (PDF) i wartości oddzielone przecinkami (CSV).

Z zapytaniami, możesz wykorzystać wiele korzyści jakie dają w porównaniu ze standardowymi raportami GravityZone:

- Duże ilości danych skierowane do tworzenia zniewalających raportów.
- Elastyczne raportowanie jeśli zdarzenie nie są połączone.
- Wysoki poziom dostosowania. Kiedy standardowe raporty GravityZone dawały możliwość wybrania z kilku zdefiniowanych opcji, z zapytaniami niema barier przy wybieraniu filtrów danych.
- Korelacja zdarzeń, z wszelkimi informacjami towarzyszącymi danym agenta i stanu urządzenia.
- Minimalny wysiłek rozwoju, możesz tworzyć, zapisywać i ponownie używać dowolnego typu raportu.
- Wszechstronne raporty, które w odróżnieniu od standardowych raportów, moją szczegółowe podsumowania zintegrowane razem w tym samym PDF-ie.
- Zapytania mogą pobierać informacje przez ostatnie dwa lata.

Aby użyć zapytań, musisz zainstalować rolę Kreatora Raporty wraz z GravityZone virtual appliance. Po szczegóły dotyczące instalacji Kreatora Raportów, odnieś się do Przewodnika Instalacji GravityZone.

9.8.1. Rodzaje Zapytań

GravityZone dostarczany jest z następującymi typami zapytań:

- Status Punktu Końcowego
- Zdarzenia Punktu Końcowego
- Zdarzenia Exchange

Status Punktu Końcowego

To zapytanie dostarcza Ci informacji na temat statusu bezpieczeństwa wybranych docelowych punktów końcowych, dla określonej daty. W ten sposób wiesz, czy agent bezpieczeństwa i treść zabezpieczeń są aktualizowane, nieaktualne lub wyłączone. Ponadto możesz zobaczyć, czy punkty końcowe są zakażone lub czyste,

która infrastruktura jest wykorzystywana i jakie moduły są włączone/wyłączone lub nie są zainstalowane.

To zapytanie zawiera szczegółowe informacje związane z docelowymi punktami końcowymi, takimi jak:

- Typ maszyny (fizyczna, wirtualna lub Security Server)
- Infrastruktura sieci, do której należy punkt końcowy (Active Directory, Nutanix Prism, VMWare lub Citrix Xen)
- Dane agenta bezpieczeństwa (typ, status, konfiguracja silników skanujących, status bezpieczeństwa)
- Status modułów ochrony
- Role punktu końcowego (Relay, Ochrona Exchange)

Zdarzenia Punktu Końcowego

To zapytanie pozwala przeglądać szczegóły o zdarzeniach bezpieczeństwa, które wystąpiły na docelowych punktów końcowych, w określonym dniu lub okresie. Obejmuje on informacje odnoszące się do:

- Maszyna docelowa, na której zdarzenie miało miejsce (nazwa, typ, IP, OS, infrastruktura sieci)
- Typ, status i konfiguracja zainstalowanego agenta bezpieczeństwa.
- Status modułów ochrony i zainstalowanych ról na agencie bezpieczeństwa
- Nazwa polityki i przyporządkowanie
- Zalogowany użytkownik podczas zdarzenia
- Zdarzenia, które mogą odnosić się do zablokowanych stron internetowych, zablokowanych aplikacji, wykrytego złośliwego oprogramowania lub aktywności urządzenia.

Zdarzenia Exchange

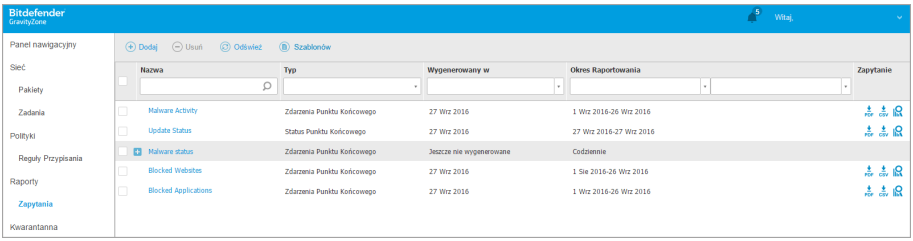
Pomaga Ci znaleźć incydenty powstałe na wybranych serwerach Microsoft Exchange, ze specyficzną datą lub w danym okresie czasu. Uwzględnia dane o:

- Kierunek ruchu e-mail
- Zdarzenia bezpieczeństwa (takie jak kierunek malware lub załącznika)

- Akcje podjęte w każdej sytuacji(dezynfekcji, usuwaniu, wymianie lub daniu pliku do kwarantanny, usunięcie, odrzuceniu maila)

9.8.2. Zarządzanie Zapytaniami

Możesz tworzyć i zarządzać zapytaniami i raportami opartymi na zapytaniach na stronie **Raport > Zapytania**.

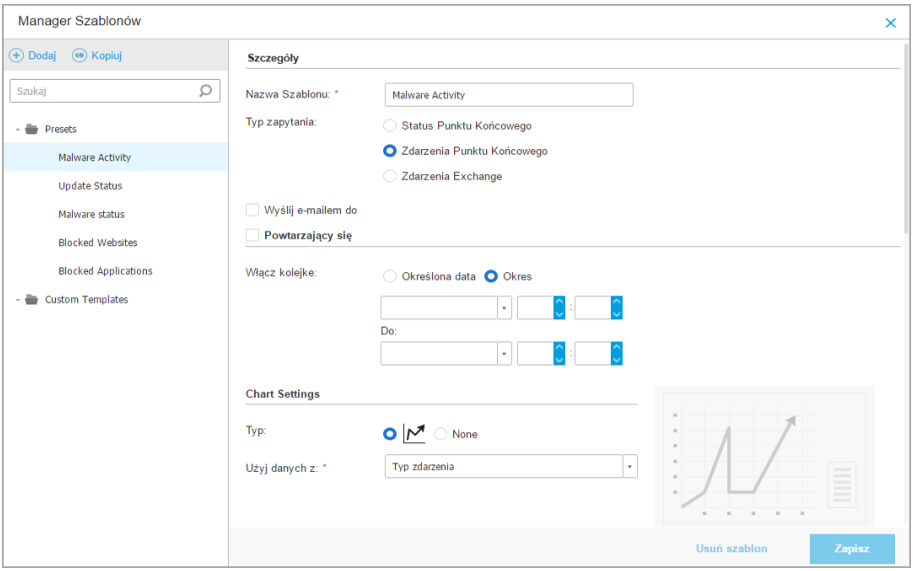


Strona Zapytania

Zapytania są kompleksowym badaniem bazy danych, używając dużej ilości filtrów, które mogą zająć kilka minut przy konfiguracji i tworzeniu. Potrzeba zapełniania formularza zapytania za każdym razem jak tworzysz nowy raport, podobny do istniejących raportów, może być frustrujące. GravityZone pozwala na łatwe tworzenie zapytań z wykorzystaniem szablonów, które automatycznie wypełniają formularz zapytania, pozostawiając Ci mniej do zrobienia przy dostosowywaniu.

Korzystanie z Szablonów

Możesz dodawać, klonować i szybko przeszukiwać pod kątem specyficznych szablonów w oknie **Manager Szablonów**.



Aby wyświetlić listę dostępnych szablonów zapytań:

1. Przejdź do strony **Raporty > Zapytania**.
2. Kliknij przycisk **Szablony** w górnej części tabeli. Okno **Manager Szablonów** zostanie wyświetlone. Wszystkie szablony są wyświetlane w lewym panelu, podczas gdy w prawym panelu możesz zobaczyć ustawienia wybranego szablonu.

Aby szybko znaleźć szablon, wprowadź nazwę w polu **Szukaj**, w górnej części lewego panelu. Można wyświetlić wyniki wyszukiwania w trakcie wpisywania. Aby wyczyścić pole **Szukaj**, kliknij ikonę × **Usuń** na końcu po prawej stronie.

Są dwie dostępne kategorie szablonów:

- Wzory Te predefiniowane szablony, które znajduja się domyślnie w GravityZone.
- Szablony użytkownika. To są szablony, które tworzysz w zależności od swoich potrzeb.

Ustawienia predefiniowane

GravityZone zawiera pięć predefiniowanych ustawień:

- **Aktywność Malware**, zapewnia informacje na temat zagrożenia złośliwym oprogramowaniem wykrytym w określonym przedziale czasowym na wybranych punktach końcowych.

  Raport zawiera nazwę maszyny docelowej, IP, status zakażenia (zainfekowany lub czysty), nazwę malware, akcja podjęta przeciwko zagrożeniu (zignorowany, obecny, usunięty, zablokowany, poddany kwarantannie, wyczyszczony lub przywrócony), typ pliku, ścieżka pliku i użytkownik zalogowany w danym momencie.

- **Status Aktualizacji**, pokazuje status aktualizacji agentów ochrony zainstalowanych na wybranych celach. Raport z wybranej maszyny zawiera: nazwę, IP, status aktualizacji produktu(aktualna, przestarzała, wyłączona), status aktualizacji sygnatur(aktualna, przestarzała, wyłączona), typ agenta ochrony, wersja produktu i wersja sygnatur.

- **Status Malware**, który pomoże Ci, aby dowiedzieć się ile z wybranych punktów końcowych zostało zarażonych malware w określonym przedziale czasowym i jak poradzono sobie z zagrożeniami.

  Raport zawiera nazwę maszyny docelowej, IP, status infekcji (zainfekowany lub czysty), nazwa malware, akcja zagrożenia (zignorowany, obecny, usunięty, zablokowany, poddany kwarantannie, wyczyszczony lub przywrócony).

- **Zablokowane Strony**, informuje Ciebie o aktywności modułu Kontroli Webowej agenta bezpieczeństwa.

  Raport zawiera nazwę maszyny docelowej, IP, typ zagrożenia (phishing, oszustwo lub niezaufane), nazwa reguły, kategoria strony i zablokowane URL.

- **Zablokowane Aplikacje**, który pomaga Ci znaleźć jakie aplikacje były zablokowane w określonym czasie.

  Raport oferuje informacje na temat nazwy maszyny docelowej, IP, nazwy zablokowanej aplikacji, jej ścieżki pliku i jak zagrożenie zostało zawarte: z ATC, IDS lub Kontroli Aplikacji.

Niestandardowe Szablony

Jeśli potrzebujesz innego szablonu niż dostarczone presety GravityZone, możesz utworzyć niestandardowe szablony zapytań. Możesz zapisać tyle szablonów ile chcesz.

Aby utworzyć niestandardowy szablon:

1. Przejdź do strony **Raporty > Zapytania**.

2. Kliknij przycisk **Szablony** w górnej części tabeli. Pojawi się okno konfiguracji **Manager Szablonów**.
3. Kliknij przycisk **Dodaj** w lewym górnym rogu okna. Formularz zapytania będzie wyświetlany po prawej stronie panelu.
4. Wypełnij formularz zapytania o wymagane informacje. Aby uzyskać szczegółowe informacje, na temat wypełniania formularza zapytania, patrz „Tworzenie Zapytań" (p. 451).
5. Kliknij **Zapisz**. Nowoutworzony szablon zostanie wyświetlony w lewym panelu, w **Szablonach Użytkownika**.

Alternatywnie, możesz utworzyć szablon użytkownika korzystając z predefiniowanych ustawień.

1. Przejdź do strony **Raporty > Zapytania**.
2. Kliknij przycisk **Szablony** w górnej części tabeli. Pojawi się okno konfiguracji **Manager Szablonów**.
3. Wybierz predefiniowane ustawienia w lewym panelu. Odpowiednie ustawienia zostaną wyświetlone w prawym panelu.
4. Kliknij **Klonuj** w lewym górnym rogu, aby utworzyć kopię predefiniowanego ustawienia.
5. Edytuj wszystkie ustawienia, które chcesz w formularzu zapytania. Aby uzyskać szczegółowe informacje, na temat wypełniania formularza zapytania, patrz „Tworzenie Zapytań" (p. 451).
6. Kliknij **Zapisz**. Nowoutworzony szablon zostanie wyświetlony w lewym panelu, w **Szablonach Użytkownika**.

Dodatkowo, podczas tworzenia nowego zapytania, możesz je zapisać jako szablon. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie Zapytań" (p. 451).

Aby usunąć jakikolwiek szablon niestandardowy:

1. Przejdź do strony **Raporty > Zapytania**.
2. Kliknij przycisk **Szablony** w górnej części tabeli. Pojawi się okno konfiguracji **Manager Szablonów**.
3. W sekcji **Szablony Niestandardowe**, kliknij szablon, który chcesz usunąć. Ustawienia szablonu zostaną wyświetlone w prawym panelu.

4. Kliknij **Usuń szablon** w dolnej części okna, a następnie potwierdź swoją akcję klikając **Tak**.

Tworzenie Zapytań

Aby utworzyć nowe zapytanie:

1. Przejdź do strony **Raporty > Zapytania**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlono okno konfiguracji.
3. Wybierz pole wyboru **Użyj szablonu** jeśli chcesz użyć domyślnego lub poprzednio utworzonego szablonu.
4. W sekcji **Szczegóły**, wprowadź sugestywną nazwę zapytania. Wybierając nazwę, rozważ typ zapytania, cele i inne ustawienia.
5. Wybierz typ zapytania. Aby uzyskać więcej informacji, odwołaj się do „Rodzaje Zapytań” (p. 445)
6. Zaznacz pole wyboru **Wyślij mailem na**, aby wysłać wyniki zapytania do określonych odbiorców. W odpowiednim polu, dodaj tak wiele adresów e-mail ile chcesz.
7. W sekcji **Powtarzalność**, zaznacz:
   a. **Określona data** dla pewnego dnia.
   b. **Okres**, dla rozszerzonego przedziału czasowego.
   c. Kliknij pole wyboru **Powtarzalny** jeśli chcesz aby zapytanie generowało się w określonych odstępach, które możesz ustawić w obszarze **Okres raportowania**.
8. Konfiguruj ustawienia wykresu.
   a. Z menu **Typ** wybierz wykres, którym chcesz zilustrować zapytanie, lub wybierz **Żaden**, aby to pominąć. Zależnie od typu zapytania oraz okresu raportowania, możesz użyć wykresu kołowego, liniowego lub słupkowego.
   b. W polu **Weź wartość z** zaznacz rodzaje danych, które chcesz wykorzystać w swoim zapytaniu. Każdy typ zapytania dostarcza określonych informacji związanych z punktami końcowymi, agentami bezpieczeństwa i zdarzeniami bezpieczeństwa. Aby uzyskać informacje na temat typu danych, odwołaj się do „Rodzaje Zapytań” (p. 445).

9. W sekcji **Ustawienia Tabeli**, zaznacz kolumny, które chcesz by zawierał raport. Dane, które możesz wybrać opierają się na typie zapytania, i mogą odnosić się do typów końcówek, systemu operacyjnego, statusu agenta bezpieczeństwa i zdarzeń, modułów, polityki i zdarzeń ochrony. Wszystkie wybrane kolumny są wyświetlane w tabeli **Kolumny**. Użyj opcji przeciągnij i upuść, aby zmienić ich kolejność.

   Notatka
   Pamiętaj o wolnej przestrzeni, tworząc układ tabeli. Użyj maksymalnie 10 kolumn, aby dobrze zwizualizować tabelę w PDFie.

10. W sekcji **Filtry**, zaznacz zbiór danych, który chcesz umieścić w raporcie korzystając z dostępnych kryteriów filtrowania:
    a. Z menu **Typ Filtra**, wybierz filtr i następnie kliknij ⊕ **Dodaj filtr**.
    b. W poniższej tabeli kliknij **Wartość**, aby określić jedną lub więcej opcji filtrowania.

       Na przykład, filtr **System operacyjny Hosta** wymaga specyficznej nazwy OS, tak jak Windows lub Linux, kiedy filtr **Moduł kontroli urządzeń** pozwala ci zaznaczyć z listy rozwijalnej końcówki gdzie moduł był wyłączony.
    c. Kliknij przycisk ⊖ **Usuń**, aby wyeliminować filtr.
11. **Wybierz Cele**. Przewiń w dół, aby skonfigurować cele raportu. Wybierz jedną lub więcej grup punktów końcowych, które chcesz zawrzeć w raporcie. Korzystając z Selektora widoku, upewnij się, że wybrałeś prawidłowe cele w widoku całej Sieci.
12. Wybierz pole wyboru **Zapisz jako szablon**, aby korzystać z tych ustawień w kolejnych zapytaniach. W tym przypadku, wprowadź sugestywną nazwę dla szablonu.
13. Kliknij **Generuj**, aby utworzyć zapytanie. Gdy zapytanie jest zapisane, otrzymasz wiadomość obszarze **Powiadomienia**.

Usuwanie Zapytań

Aby usunąć zapytanie:

1. Przejdź do strony **Raporty > Zapytania**.
2. Wybierz raport, który chcesz usunąć.
3. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli.

Notatka
Usuwanie rekordów usunie również wszystkie wygenerowane raporty.

9.8.3. Przeglądanie i Zarządzanie Raportami

Wszystkie raporty oparte na zapytaniach są wyświetlane na stronie **Raporty > Zapytania**.

Notatka
Raporty są dostępne tylko dla użytkownika, który je stworzył.

Przeglądanie raportów

Aby zobaczyć raport oparty na zapytaniu:

1. Przejdź do strony **Raporty > Zapytania**.
2. Sortuj raporty przez nazwę, typ, datę wygenerowania lub okres raportowania, aby łatwo znaleźć to, czego szukasz. Domyślnie, raporty są sortowane według daty ostatniej wygenerowanej instancji.
3. Kliknij jakąkolwiek nazwę, aby zobaczyć informacje o zapytaniu w nowym oknie. Szczegóły nie mogą być edytowane.
4. Kliknij przycisk plusa naprzeciwko nazwy zapytania aby rozwinąć listę instancji raportów lub przycisk minus aby zwinąć.
5. Kliknij ikonę **Pokaż raport**, aby wyświetlić najnowszą instancję raportu. Starsze instancje są tylko dostępne w formacie PDF i CSV.

Wszystkie raporty składają się z sekcji podsumowania w górnej części raportu i z sekcji szczegółów w dolnej części raportu.

Sekcja podsumowania dostarcza ci dane statystyczne(wykres kołowy, słupkowy, liniowy) dla wszystkich wybranych końcówek. Główne informacje na temat zapytania, jak powtarzalność, okres raportowania, typ zapytania, oraz użyte filtry.

Aby skonfigurować informacje wyświetlone na wykresie, nacisnij legendę wpisów, aby pokazać lub ukryć wybrane dane. Jeszcze, kliknij obszar, którym jesteś zainteresowany w grafice aby zobaczyć związane z nim dane w tabeli.

Sekcja szczegóły dostarcza informacji o każdym punkcie końcowym. Aby szybko znaleźć dane, które chcesz, kliknij pole wyszukiwania lub poniższe opcje filtrowania w nagłówkach kolumn.

Kliknij przycisk **Kolumny**, aby dostosować, które kolumny będą wyświetlane w tabeli.

Zapisywanie raportów

Domyślnie, wszystkie raporty są automatycznie zapisywane w Control Center. Możesz je także wyeksportować na swój komputer, zarówno w formacie PDF jak i CSV.

Możesz zapisać raporty na swoim komputerze:

- Ze strony raportu.
- Z tabeli **Zapytania**.

Aby zapisać raport gdy jesteś na jego stronie:

1. Kliknij przycisk **Eksport** w lewym dolnym rogu.
2. Wybierz odpowiedni format raportu:
   a. Przenośny Format Dokumentu (PDF) lub
   b. Wartości oddzielone przecinkami (CSV)
3. W zależności od ustawień przeglądarki, plik można pobrać automatycznie do domyślnej lokalizacji pobierania, lub określić folder docelowy w oknie pobierania, które się pojawi.

Aby eksportować raport, gdy jesteś na stronie **Raporty > Zapytania**:

1. Przejdź do strony **Raporty > Zapytania**.
2. Kliknij przycisk **PDF** lub **CSV** odpowiedni dla każdego raportu.
3. W zależności od ustawień przeglądarki, plik można pobrać automatycznie do domyślnej lokalizacji pobierania, lub określić folder docelowy w oknie pobierania, które się pojawi.

Wszystkie raporty eksportowane w formacie PDF mają podsumowanie i szczegóły w tym samym dokumencie, na oddzielnych stronach A4 zorientowanych pionowo lub poziomo. Szczegóły są ograniczone do 100 wierszy na dokument PDF.

Raporty E-mailów

Masz dwie opcje, aby wysyłać raporty mailem:

1. Na stronie raportu, który przeglądasz, kliknij klawisz **Email** w lewym dolnym rogu strony. Raport zostanie wysłany na adres e-mail powiązany z Twoim kontem.

2. Podczas tworzenia nowego zapytania, zaznacz pole wyboru **Wyślij mailem o** i wprowadź adres e-mail, który chcesz, w odpowiednim polu.

Drukowanie raportów

Control Center nie obsługuje obecnie funkcji przycisku drukowania. Aby wydrukować oparty na zapytaniu raport, najpierw musisz zapisać go na komputer.

10. KWARANTANNA

Kwarantanna jest szyfrowanym folderem który zawiera potencjalnie złośliwe pliki, takie jak podejrzane, zainfekowane lub inne niechciane pliki zawierające złośliwy kod. Gdy wirus lub inna forma złośliwego oprogramowania znajduje się w kwarantannie, nie może spowodować żadnych strat, ponieważ pliki nie mogą być zostać wykonane lub odczytane.

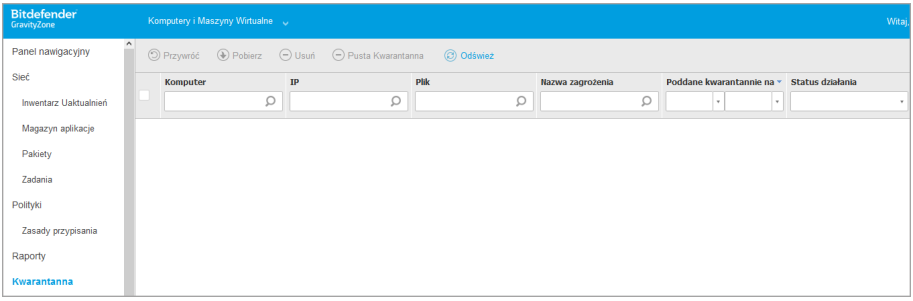
GravityZone przenosi pliki do kwarantanny zgodnie z politykami przypisanymi do punktów roboczych. Domyślnie, pliki które nie mogą zostać zdezynfekowane są przenoszone do kwarantanny.

Kwarantanna jest zapisywana lokalnie na każdym z punktów końcowych, z wyjątkiem Serwera VMware vCenter zintegrowanego z vShield Endpoint oraz z NSX, która jest zapisywana na Security Server.

WAŻNE
Kwarantanna jest niedostępna dla urządzeń mobilnych.

10.1. Poznawanie Kwarantanny

Strona **Kwarantanna** dostarcza szczegółowych informacji odnośnie plików kwarantanny ze wszystkich zarządzanych punktów końcowych.



Strona Kwarantanny

Strona Kwarantanny składa się z dwóch widoków:

- Komputery i Maszyny Wirtualne, w celu wykrywania plików bezpośrednio w systemie plików punktu końcowego.

- Serwery Exchange, dla e-maili i plików załączonych do wiadomości e-mail, wykrywane na serwerach poczty Exchange.

Selektory widoku z górnej strony strony pozwalają przełączać się pomiędzy tymi widokami.

Informacje o plikach kwarantanny są wyświetlane w tabeli. W zależności od ilości zarządzanych punktów końcowych i stopnia infekcji, tabela Kwarantanny może zawierać dużą liczbę wpisów. Tabela może rozciągać się na kilka strony (domyślnie, tylko 20 wpisów jest wyświetlanych na stronie).

Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

dla lepszego wglądu w dane, które nas interesują, możemy użyć pola wyszukiwania z kolumny nagłówka w celu przefiltrowania wyświetlanych danych. Na przykład, możesz wyszukać określonego zagrożenia wykrytego w sieci dla określonego obiektu sieciowego. Możesz również kliknąć nagłówek kolumny aby posortować dane według określonej kolumny.

Aby upewnić się, że zostają wyświetlane najnowsze informacje, kliknij przycisk **Odśwież** z górnej części tabeli. Może być potrzebne abyś spędził więcej czasu na tej stronie.

10.2. Kwarantanna Komputerów i Maszyn Wirtualnych

Pliki poddane kwarantannie są domyślnie wysyłane do laboratoriów firmy Bitdefender w celu analizy szkodliwego oprogramowania dokonywanej przez analityków Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania. Ponadto pliki poddane kwarantannie są skanowane po każdej aktualizacji sygnatur wirusów. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji. Te cechy są pokrewne dla każdej polityki bezpieczeństwa zawartej na stronie **Polityki** i możesz wybrać czy chcesz je zatrzymać czy zdezaktywować. Aby uzyskać więcej informacji, zapoznaj się z „Kwarantanna” (p. 285).

10.2.1. Wyświetlanie Szczegółów Kwarantanny

Tabela Kwarantanny dostarcza następujących informacji:

- Nazwa punktu końcowego, na którym zostało wykryte zagrożenie.
- IP punktu końcowego, na którym zostało wykryte zagrożenie.

- Ścieżka do zainfekowanego lub podejrzanego pliku na punkcie końcowym na którym został wykryty.
- Nazwa nadana dla zagrożenia malware przez testerów bezpieczeństwa Bitdefender.
- Data i czas w którym plik znajduj się kwarantanna.
- Status działania wymaga podjęcia działań względem pliku znajdującego się w kwarantannie.

10.2.2. Zarządzanie Plikami Kwarantanny

Postępowanie kwarantanny jest inne dla każdego środowiska:

- **Security for Endpoints** przechowuje pliki kwarantanny na każdym zarządzanym komputerze. Używając Control Center masz opcje do usunięcia lub przywrócenia konkretnych plików kwarantanny.
- **Security for Virtualized Environments (wieloplatformowe)** przechowuje pliki kwarantanny na każdej maszynie wirtualnej. Używając Control Center masz opcje do usunięcia lub przywrócenia konkretnych plików kwarantanny.
- **Security for Virtualized Environments (zintegrowane z VMware vShield Endpoint)** przechowuje pliki kwarantanny na urządzeniu Security Server. Używając Control Center masz opcje umożliwiającą usunięcie plików kwarantanny lub pobranie ich do wybranej lokalizacji.

Przywracanie plików kwarantanny

W konkretnych przypadkach może być konieczne, aby przywrócenie pliki kwarantanny do ich oryginalnej lokalizacji lub do lokalizacji alternatywnej. Jedna sytuacja jest wtedy gdy chcesz odzyskać ważne pliki przechowywane w zainfekowanym archiwum, które jest w kwarantannie.

Notatka
Przywracanie plików jest tylko możliwe w środowiskach chronionych przez Security for Endpoints i Security for Virtualized Environments (Multi-Platform).

Aby przywrócić jeden lub więcej plików kwarantanny:

1. Przejdź do strony **Kwarantanna**.
2. Wybierz **Komputery i Maszyny Wirtualne** z selektora widoku dostępnego w górnej części strony.
3. Zaznacz pola odpowiadające plikom kwarantanny które chcesz odzyskać.
4. Kliknij przycisk **Odzyskiwanie** z górnej strony tabeli.

5. wybierz lokalizacje gdzie chcesz przywrócić pliki (oryginalna lub niestandardowa lokalizacja na docelowym komputerze).

   Jeżeli wybierzesz, żeby przywrócić do niestandardowej lokalizacji, musisz najpierw podać dokładną ścieżkę w odpowiednim polu.
6. Wybierz **Automatyczne dodawanie wyjątków w polityce** aby wykluczyć pliki, które mają być przywrócone w następnych skanowaniach. Wyjątki mają zastosowanie do wszystkich polityk mających wpływ na wybrane pliki, z wyjątkiem polityki domyślnej, która nie może być modyfikowana.
7. Naciśnij **Zapisz** aby żądać przywrócenia pliku. Możesz zobaczyć oczekujący status w kolumnie **Działanie**.
8. Żądane działanie jest przesyłane do docelowych punktów końcowych bezpośrednio lub jak tylko pojawią się online.

   Możesz zobaczyć szczegóły dotyczące stanu akcji na stronie **Zadania**. Gdy plik zostanie przywrócony, to odpowiedni wpis zniknie z tabeli kwarantanny.

Pobieranie Plików z Kwarantanny

W zwirtualizowanych środowiska VMware zintegrowanych z vShield Endpoint lub NSX, kwarantanna zapisywana jest na Security Server. Jeżeli chcesz sprawdzić lub odzyskać dane z plików kwarantanny, musisz pobrać je z Security Server używając Control Center. Pliki kwarantanny są pobrane jako zaszyfrowane, hasło ochrony archiwum ZIP zapobiega przypadkowym infekcją malware.

Aby otworzyć archiwum i wypakować jego zawartość, musisz użyć Narzędzia Kwarantanny, samodzielnej aplikacji Bitdefender, która nie wymaga instalacji.

Narzędzie Kwarantanny jest dostępne dla następujących systemów operacyjnych:

- Windows 7 lub nowszy
- Większość 32-bitowych dystrybucji Linuxa wraz z graficznym interfejsem użytkownika (GUI).

Notatka
Należy pamiętać, że Narzędzie Kwarantanny nie posiadają interfejsu wiersza poleceń.

Ostrzeżenie
Należy zachować ostrożność przy wyodrębnieniu plików poddanych kwarantannie, ponieważ mogą one zainfekować system. Zaleca się, aby wyodrębnić i przeanalizować pliki z kwarantanny podczas testów lub w izolowanym systemie, najlepiej działającym pod Linuksem. Infekcje malware łatwiej przechowywać w systemie Linux.

Aby pobrać pliki kwarantanny na twój komputer:

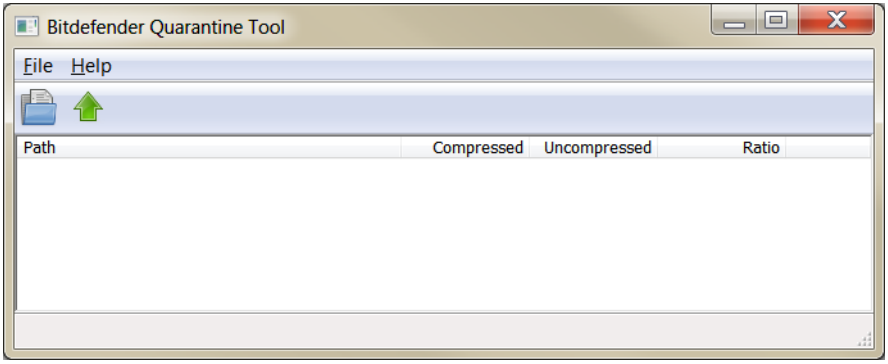
1. Przejdź do strony **Kwarantanna**.
2. Wybierz **Komputery i Maszyny Wirtualne** z selektora widoku dostępnego w górnej części strony.
3. Filtruj dane z tabeli poprzez wprowadzenie nazwy hosta Security Server lub podanie adresu IP w odpowiednim polu w nagłówku tabeli.

   Jeżeli kwarantanna jest zbyt rozległa, by znaleźć pożądane przez nas pliki, możemy zastosować dodatkowe filtry w celu zwiększenia liczby plików wymienionych na stronie.
4. Zaznacz pola wyboru odpowiednie dla plików które chcesz pobrać.
5. Kliknij przycisk **Pobierz** w górnej części tabeli. W zależności od ustawień przeglądarki, zostaniesz poproszony o zapisanie plików w wybranym przez siebie folderze lub plik zostanie automatycznie pobrany do lokalizacji pobrania.

Aby uzyskać dostęp do przywróconych plików:

1. Pobierz odpowiednie Narzędzia Kwarantanny dla swojego systemu operacyjnego ze strony **Pomoc & Wsparcie** lub poniższego adresu:
   - Narzędzie kwarantanny dla Windows
   - Narzędzie kwarantanny dla Linux

   Notatka
   Narzędzia kwarantanny dla Linux jest zarchiwizowane w pliku `tar`.
2. Uruchom wykonywalny plik Narzędzia Kwarantanny.



Narzędzie Kwarantanny

3. W menu **Plik** kliknij **Otwórz** (CTRL+0) lub kliknij przycisk **Otwórz** aby załadować archiwum do narzędzia.

   Pliki zorganizowane w archiwa przez wirtualną maszynę zostały wykryte i zachowują swoją oryginalną ścieżkę.
4. Przed rozpakowaniem plików archiwum, jeżeli skanowanie antymalware podczas dostępu jest włączone w systemie, upewnij się żeby je nie wyłączyć lub skonfiguruj wyjątek dla konkretnej lokalizacji, w której chcesz rozpakować pliki. W przeciwnym razie program antymalware wykryje i podejmie działanie aby wyodrębnić pliki.
5. Wybierz pliki które chcesz rozpakować.
6. W menu **Plik** kliknij opcję **Rozpakuj** (CTRL+E) lub kliknij przycisk **Rozpakuj**.
7. Wybierz folder docelowy. Pliki zostają wypakowane w wybranej lokalizacji, zachowując oryginalną strukturę folderów.

Automatyczne usunięcie plików kwarantanny

Domyślnie wszystkie pliki objęte kwarantanną dłużej niż 30 dni są automatycznie usuwane. Te ustawienia mogą być zmieniane poprzez edytowanie polityk przypisanych do zarządzanych punktów końcowych.

Aby zmienić przedział automatycznego usuwania plików poddanych kwarantannie:

1. Przejdź do strony **Polityki**.
2. Znajdz politykę przypisaną do punktu końcowego na którym chcesz zmienić ustawienia i kliknij jego nazwę.
3. Przejdź do strony **Antymalware > Ustawienia**.
4. W sekcji **Kwarantanna**, wybierz liczbę dni, po których pliki są kasowane.
5. Naciśnij **Zapisz** aby zastosować zmiany.

Ręczne Usuwanie Plików Kwarantanny

Jeżeli chcesz ręcznie usunąć pliki kwarantanny , musisz najpierw być pewien, że pliki, które wybrałeś nie są potrzebne.

Plik faktycznie może być złośliwym oprogramowaniem. Jeżeli prowadzisz badania doprowadzą ciebie do takich sytuacji, możesz przeszukać kwarantannę w poszukiwaniu określonych zagrożeń i usunąć je.

Aby usunąć jeden lub więcej plików kwarantanny:

1. Przejdź do strony **Kwarantanna**.

2. Wybierz **Komputery i Maszyny Wirtualne** z selektora widoku dostępnego w górnej części strony.
3. Zaznacz pola wyboru odpowiadające plikom z kwarantanny które chcesz usunąć.
4. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Musisz potwierdzić tę czynność poprzez kliknięcie **Tak**.

   Możesz zobaczyć oczekujący status w kolumnie **Działanie**.

   Żądane działanie jest przekazywane do docelowych obiektów sieciowych bezpośrednio lub jak tylko pojawią się online. Gdy plik zostanie usunięty, w odpowiedni wpis zniknie z tabeli kwarantanny.

Czyszczenie Kwarantanny

Aby usunąć wszystkie obiekty kwarantanny:

1. Przejdź do strony **Kwarantanna**.
2. Wybierz **Komputery i Wirtualne Maszyny** z selektora widoku.
3. Kliknij przycisk **Wyczyść Kwarantannę**.

   Czynności należy potwierdzić, klikając **Tak**.

Wszystkie wpisy z tabeli Kwarantanna są wyczyszczone. Żądane działanie jest przekazywane do docelowych obiektów sieciowych bezpośrednio lub jak tylko pojawią się online.

10.3. Kwarantanna Serwerów Exchange

Kwarantanna Exchange zawiera e-maile i załączniki. Moduł Antymalware poddaje kwarantannie załączniki do wiadomości e-mail, natomiast Antyspam, Filtrowanie zawartości i załączników poddają kwarantannie całą wiadomość e-mail.

Notatka
Miej na uwadze, że kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni na partycji dysku twardego gdzie zainstalowano agenta. Rozmiar kwarantanny zależy od liczby elementów przechowywanych oraz ich wielkości.

10.3.1. Wyświetlanie Szczegółów Kwarantanny

Strona **Kwarantanna** oferuje szczegółowe informacje na temat poddanych kwarantannie obiektów ze wszystkich Serwerów Exchange z całej organizacji. Informacje dostępne są w tabeli Kwarantanny oraz w oknie szczegółów dla każdego obiektu.

Tabela Kwarantanny dostarcza następujących informacji:

- **Temat.** Temat wiadomości poddanej kwarantannie.
- **Nadawca.** Adres nadawcy e-maila, który pojawia się w polu **Od**.
- **Odbiorcy.** Lista od odbiorców według ich pojawiania się w polu nagłóka **Do** i **Cc**.
- **Prawdziwi odbiorcy.** Lista indywidualnych adresów mailowych użytkowników, do których e-maile były z założenia wysyłane przed poddaniem kwarantannie.
- **Status.** Status obiektu po jego przeskanowaniu. Status pokazuje, czy e-mail jest oznaczony jako spam lub zawiera niepożądane treści, lub jeśli załącznik jest zainfekowany malware, podejrzany o zakażenie, niechciany lub nieskanowalny.
- **Nazwa Malware.** Nazwa nadana zagrożeniu malware przez analityków bezpieczeństwa Bitdefender.
- **Nazwa Serwera.** Nazwa hosta serwera, na którym zagrożenie zostało wykryte.
- **Poddane Kwarantannie.** Data i czas, w którym obiekt był poddany kwarantannie.
- **Status akcji.** Status akcji podjętej na obiektach poddanych kwarantannie. W ten sposób możesz szybko wyświetlić czy akcja jest nadal oczekująca lub nie powiodła się.

Notatka

- Kolumny **Prawdziwy odbiorca**, **Nazwa Malware** i **Nazwa Serwera** są ukryte w widoku domyślnym.
- Gdy kilka załączników z tego samego e-maila zostanie poddana kwarantannie, tabela Kwarantanny pokazuje rozdzielone wpisy dla każdego z nich.

Aby dostosować szczegóły kwarantanny w tabeli:

1. Kliknij przycisk **Kolumny** z prawej strony nagłówka tabeli.
2. Wybierz kolumny, które chcesz zobaczyć.

   Aby wrócić do widoku domyślnych kolumn, kliknij przycisk **Resetuj**.

Możesz uzyskać więcej informacji poprzez kliknięcie linku **Temat** odpowiednie dla każdego obiektu. Okno **Szczegóły Obiektu** jest wyświetlone, dostarczając następujących informacji:

- **Obiekt poddany kwarantannie.** Typ obiektu poddanego kwarantannie, którym może być albo e-mail albo załącznik.
- **Poddane Kwarantannie.** Data i czas, w którym obiekt był poddany kwarantannie.
- **Status.** Status obiektu po jego przeskanowaniu. Status pokazuje, czy e-mail jest oznaczony jako spam lub zawiera niepożądane treści, lub jeśli załącznik jest zainfekowany malware, podejrzany o zakażenie, niechciany lub nieskanowalny.
- **Załączona nazwa.** Nazwa pliku załącznika wykrytego przez Antimalware lub moduł Filtrowania Załączników.
- **Nazwa Malware.** Nazwa nadana zagrożeniu malware przez analityków bezpieczeństwa Bitdefender. Ta informacja jest dostępna, tylko jeżeli obiekt został zainfekowany.
- **Punkt wykrywania.** Obiekt jest wykryty albo na poziomie dostarczenia lub w skrzynce pocztowej lub publicznym folderze z Exchange Store.
- **Zasada dopasowana.** Zasady polityk, do których pasuje zagrożenie.
- **Serwer.** Nazwa hosta serwera, na którym wykryto zagrożenie.
- **IP nadawcy.** Adres IP nadawcy.
- **Nadawca.** Adres e-mail nadawcy taki jaki pojawia się w polu nagłówka wiadomości **Od**.
- **Odbiorcy.** Lista od odbiorców według ich pojawiania się w polu nagłóka **Do** i **Cc**.
- **Prawdziwi odbiorcy.** Lista indywidualnych adresów mailowych użytkowników, do których e-maile były z założenia wysyłane przed poddaniem kwarantannie.
- **Temat.** Temat wiadomości poddanej kwarantannie.

Notatka
Znak wielokropka na końcu tekstu oznacza, że część tekstu została pominięta. W tym przypadku, przesuń kursor myszy nad tekst by zobaczyć go w podpowiedzi.

10.3.2. Obiekty Kwarantanny

E-maile i pliki poddane kwarantannie przez moduł Ochrony Exchange są przechowywane na serwerze jako zaszyfrowane pliki. Korzystając z Control Center

masz możliwość przywrócenia maili poddanych kwarantannie, a także usunąć lub zapisać dowolne pliki lub e-maile poddane kwarantannie.

Przywracanie E-maili Poddanych Kwarantannie

Jeśli zdecydujesz, że e-mail poddany kwarantannie nie stanowi zagrożenia, możesz go zwolnić z kwarantanny. Korzystając z Usług Webowych Exchange, Ochrona Exchange wysyła e-maile poddane kwarantannie do ich docelowych odbiorców jako załączniki do wiadomości Bitdefender.

Notatka
Możesz odtworzyć jedynie wiadomości e-mailowe. Aby odzyskać załączniki poddane kwarantannie, trzeba zapisać je do lokalnego folderu na serwerze Exchange.

Aby odzyskać jeden lub więcej e-maili:

1. Przejdź do strony **Kwarantanna**.
2. Wybierz z selektora widoku **Exchange** dostępnego w górnej części strony.
3. Zaznacz pola wyboru odpowiadające e-mailom, które chcesz odzyskać.
4. Kliknij przycisk **Odzyskiwanie** z górnej strony tabeli. Pojawi się okno **Przywróć poświadczenia**.
5. Wybierz poświadczenia użytkownika programu Exchange uprawnionego do wysyłania e-maili, które mają być przywrócone. Jeśli poświadczenia, które masz zamiar używać są nowe, musisz je najpierw dodać do Menedżera Poświadczeń.

   Aby dodać wymagane poświadczenia:

   a. Wprowadź wymagane informacje w odpowiednich polach z nagłówka tabeli:
      - Nazwa użytkownika i hasło użytkownika Exchange.

        Notatka
        Nazwa użytkownika musi zawierać nazwę domeny, tak jak w `user@domain` lub `domain\user`

      - Adres e-mail użytkownika Exchange, jest konieczny tylko wtedy, gdy adres e-mail jest inny niż nazwa użytkownika.
      - URL Serwisu Webowego Exchange (EWS) jest konieczne, gdy Automatyczne Wykrywanie Exchange nie działa. Jest to zwykle sprawa z serwerami Edge Transport w DMZ.

b. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli. Nowe ustawienia poświadczeń zostały dodane do tabeli.

6. Kliknij przycisk **Przywróć**. Pojawi się nowa wiadomość potwierdzająca.

   Żądane działanie jest natychmiast wysyłane do docelowego serwera. Gdy e-mail zostanie przywrócony, to zostanie również usunięty z kwarantanny, więc odpowiedni wpis zniknie z tabeli Kwarantanna.

   Możesz sprawdzić status przywróconych akcji w każdym z tych miejsc:

   - Kolumna **Status działań** tabeli Kwarantanna.
   - Strona **Sieć > Zadania**.

Zapisywanie Plików Kwarantanny

Jeśli chcesz sprawdzić lub odzyskać dane z plików w kwarantannie, możesz zapisać pliki do folderu lokalnego na serwerze Exchange. Bitdefender Endpoint Security Tools deszyfruje pliki i zapisuje je do określonej lokalizacji.

Aby zapisać jeden lub więcej plików kwarantanny:

1. Przejdź do strony **Kwarantanna**.
2. Wybierz z selektora widoku **Exchange** dostępnego w górnej części strony.
3. Filtruj dane z tabeli, aby wyświetlić wszystkie pliki, które chcemy zapisać, poprzez wprowadzenie warunków wyszukiwania w polu nagłówka kolumny.
4. Zaznacz pola odpowiadające plikom kwarantanny które chcesz odzyskać.
5. Kliknij przycisk ⊛ **Zapisz** z górnej strony tabeli.
6. Wprowadź ścieżkę do folderu docelowego na Serwerze Exchange. Jeżeli folder nie istnieje na serwerze, zostanie utworzony.

   WAŻNE
   Musisz wykluczyć ten folder z poziomu skanowania plików systemowych, w innym wypadku pliki zostaną przeniesione do Komputerów oraz Kwarantanny Maszyn Wirtualnych. Aby uzyskać więcej informacji, odwołaj się do „Wykluczenia” (p. 287).

7. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

   Możesz zaobserwować oczekujący status w kolumnie **Status Działania**. Możesz również zobaczyć status akcji na stronie **Sieć > Zadania**.

Automatyczne usunięcie plików kwarantanny

Domyślnie, pliki poddane kwarantannie na dłużej niż 30 dni są automatycznie kasowane. Możesz zmienić ustawienia poprzez edycję polityk przypisanych do zarządzanego Serwera Exchange.

Aby zmienić przedział automatycznego usuwania plików poddanych kwarantannie:

1. Przejdź do strony **Polityki**.
2. Kliknij nazwę polityki przypisanej do pożądanego Serwera Exchange.
3. Przejdź do strony **Bezpieczeństwo Exchange > Ogólne**.
4. W sekcji **Ustawienia**, wybierz liczbę dni, po których pliki są kasowane.
5. Naciśnij **Zapisz** aby zastosować zmiany.

Ręczne Usuwanie Plików Kwarantanny

Aby skasować jeden lub więcej obiektów kwarantanny:

1. Przejdź do strony **Kwarantanna**.
2. Wybierz z pośród selektorów wyboru **Exchange**.
3. Zabierz pola wyboru odpowiednich plików, które chcesz usunąć.
4. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Musisz potwierdzić tę czynność poprzez kliknięcie **Tak**.

   Możesz zaobserwować oczekujący status w kolumnie **Status Działania**.

   Żądane działanie jest natychmiast wysyłane do docelowego serwera. Gdy plik zostanie usunięty, w odpowiedni wpis zniknie z tabeli kwarantanny.

Czyszczenie Kwarantanny

Aby usunąć wszystkie obiekty kwarantanny:

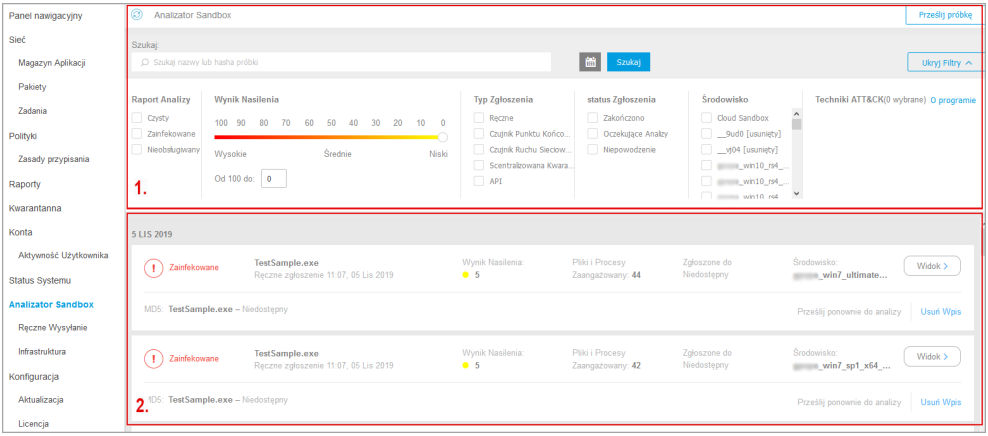
1. Przejdź do strony **Kwarantanna**.
2. Wybierz **Exchange** z selektora widoku.
3. Kliknij przycisk **Wyczyść Kwarantannę**.

   Czynności należy potwierdzić, klikając **Tak**.

Wszystkie wpisy z tabeli Kwarantanna są wyczyszczone. Żądana akcja zostanie natychmiast wysłana do docelowych obiektów sieciowych.

11. KORZYSTANIE Z SANDBOX ANALYZER

Strona **Sandbox Analyzer** udostępnia ujednolicony interfejs do przeglądania, filtrowania i wyszukiwania automatycznych i ręcznych zgłoszeń do środowiska sandbox. Strona **Sandbox Analyzer** składa się z dwóch obszarów:



Strona Sandbox Analyzer

1. **Obszar filtrowania** umożliwia wyszukiwanie i filtrowanie zgłoszeń według różnych kryteriów: nazwa, hash, data, wynik analizy, status, środowisko detonacji i techniki MITRE's ATT&CK.
2. W **Obszar kart zgłoszeń** wyświetlane są wszystkie zgłoszenia w kompaktowym formacie ze szczegółowymi informacjami o każdym z nich.

Na stronie Sandbox Analyzer możesz wykonać następujące czynności:

- Filtrowanie Kart Zgłoszeń
- Wyświetl listę zgłoszeń i szczegóły analizy
- Ponownie wyślij próbki do analizy z karty wysyłania.
- Usuwanie Kart Zgłoszeń
- Dokonuj ręcznego przesyłania

11.1. Filtrowanie Kart Zgłoszeń

Oto, co możesz zrobić w obszarze filtrów:

- Filtruj zgłoszenia według różnych kryteriów. Strona automatycznie załaduje tylko karty zdarzeń bezpieczeństwa spełniające wybrane kryteria.
- Zresetuj filtry, klikając przycisk **Wyczyść Filtry**.
- Ukryj obszar filtrów, klikając przycisk **Ukryj Filtry**. Możesz ponownie wyświetlić ukryte opcje, klikając **Pokaż Filtry**.

Możesz filtrować zgłoszenia Sandbox Analyzer według następujących kryteriów:

- **Przykładowa nazwa i hash (MD5)**. Wpisz w polu wyszukiwania część lub całą nazwę lub hash szukanej próbki, a następnie kliknij przycisk **Wyszukaj** po prawej stronie.
- **Data**. Aby filtrować według daty:
  1. Kliknij ikonę kalendarza, aby skonfigurować czas wyszukiwania.
  2. Zdefiniuj interwał. Kliknij przyciski **Od** i **Do** w górnej części kalendarza, aby wybrać daty określające przedział czasu. Możesz także wybrać z góry określony okres z listy opcji po prawej stronie, w odniesieniu do bieżącego czasu (na przykład z ostatnich 30 dni).

     Możesz także określić godzinę i minuty dla każdej daty przedziału czasu, korzystając z opcji pod kalendarzem.
  3. Kliknij **OK**, aby zastosować filtr.
- **Wyniki analizy**. Wybierz jedną lub więcej z następujących opcji:
  - **Czysta** - próbka jest bezpieczna.
  - **Zainfekowana** - próbka jest niebezpieczna.
  - **Nieobsługiwana** - próbka ma format, którego Sandbox Analyzer nie zdoła detonować. Aby zobaczyć pełną listę plików i rozszerzeń obsługiwanych przez , Sandbox Analyzer przejdź do „Obsługiwane Typy Plików i Rozszerzenia do Wysyłania Ręcznego” (p. 520).
- **wskaźnik szkodliwości**. Wartość wskazuje, jak niebezpieczna jest próbka w skali od 100 do 0 (zero). Im wyższy wynik, tym bardziej niebezpieczna jest próbka. Wynik szkodliwości dotyczy wszystkich przesłanych próbek, w tym tych z symbolem **Czyste** lub **Nieobsługiwane**.

- **Typ zgłoszenia**. Wybierz jedną lub więcej z następujących opcji:
  - **Ręczne**. Sandbox Analyzer otrzymał próbkę za pomocą opcji **Ręczne przesyłanie**.
  - **Czujnik punktu końcowego**. Bitdefender Endpoint Security Tools wysłał próbkę do Sandbox Analyzer w oparciu o ustawienia polityki.
  - **Czujnik Ruchu Sieciowego**. Czujnik sieci wysłał próbkę do instancji Sandbox Analyzer w oparciu o ustawienia polityki.
  - **Scentralizowana kwarantanna**. GravityZone wysłało próbkę do lokalnej instancji Sandbox Analyzer w oparciu o ustawienia polityk.
  - **API**. Próbka została wysłana do lokalnej instancji Sandbox Analyzer używając metody API.
  - **Czujnik ICAP**. Security Server wysłał próbkę do lokalnej instancji Sandbox Analyzer po przeskanowaniu serwera ICAP.
- **Status Zgłoszenia**. Zaznacz jedno lub więcej z następujących pól wyboru:
  - **Zakończono** - Sandbox Analyzer dostarczył wynik analizy.
  - **Oczekuje na analizę** - Sandbox Analyzer detonuje próbkę.
  - **Nie powiodło się** - Sandbox Analyzer nie mógł zdetonować próbki.
- **Środowisko**. Tutaj wypisane są wirtualne maszyny dostępne do detonacji, wliczając instancję Sandbox Analyzer hostowaną przez Bitdefender. Zaznacz jedno lub kilka okien aby zobaczyć jakie próbki zostały zdetonowana w określonych środowiskach.
- **Techniki ATT&CK**. Ta opcja filtrowania integruje bazę wiedzy MITRE's ATT&CK, jeśli dotyczy. Wartości technik ATT&CK zmieniają się dynamicznie, w zależności od zdarzeń bezpieczeństwa.

  Kliknij **Na temat**, aby otworzyć ATT&CK Matrix w nowej karcie.

11.2. Przeglądanie Szczegółów Analizy

Strona **Sandbox Analyzer** wyświetla karty zgłoszeń według dni, w odwrotnej kolejności chronologicznej. Karty zgłoszenia zawierają następujące dane:

- Wyniki analizy
- Nazwa próbki
- Typ zgłoszenia

- wskaźnik szkodliwości
- Pliki i procesy towarzyszące
- Środowisko detonacji
- Wartość skrótu (MD5)
- Techniki ATT&CK
- Status zgłoszenia, gdy wynik jest niedostępny

Każda karta zgłoszenia zawiera link do szczegółowego raportu analizy w HTML, jeśli jest dostępny. Aby otworzyć raport, kliknij przycisk **Wyświetl** po prawej stronie karty.

Raport HTML zawiera bogate informacje zorganizowane na wielu poziomach, z tekstem opisowym, grafiką i zrzutami ekranu, które ilustrują zachowanie próbki w środowisku detonacji. Tego możesz się dowiedzieć z raportu HTML Sandbox Analyzer:

- Ogólne dane o analizowanej próbce, takie jak: nazwa i klasyfikacja złośliwego oprogramowania, szczegóły przesyłania (nazwa, typ i rozmiar pliku, hash, czas przesyłania i czas trwania analizy).
- Wyniki analizy behawioralnej, które obejmują wszystkie zdarzenia bezpieczeństwa zarejestrowane podczas detonacji, zorganizowane w sekcjach. Zdarzenia bezpieczeństwa odnoszą się do:
  - Pisanie / usuwanie / przenoszenie / duplikowanie / zamienianie plików w systemie i na dysku przenośnym.
  - Wykonanie nowo utworzonych plików.
  - Zmiany w systemie plików.
  - Zmiany w aplikacjach uruchomionych na maszynie wirtualnej.
  - Zmiany w w pasku zadań i menu startowym Windows.
  - Procesy tworzenia / zakończania / wstrzykiwania.
  - Pisanie / usuwanie kluczy rejestracji.
  - Tworzenie obiektów mutex.
  - Tworzenie / uruchamianie / wstrzymywanie / modyfikowanie / wyszukiwanie / usuwanie usług.
  - Zmiana ustawień bezpieczeństwa przeglądarki.
  - Zmiana ustawień wyświetlania Windows Explorer.
  - Dodawanie plików do listy wyjątków zapory sieciowej.
  - Zmiana ustawień sieci.
  - Włączanie wykonywania przy uruchamianiu systemu.
  - Łączenie z hostem zdalnym.
  - Uzyskiwanie dostępu do określonych domen.

- Transfer danych do i z określonych domen.
- Uzyskiwanie dostępu do URL, IP i portów, poprzez różne protokoły komunikacyjne.
- Sprawdzanie wskaźników środowiska wirtualnego.
- Sprawdzanie wskaźników narzędzi monitorujących.
- Tworzenie snapshotów.
- SSDT, IDT, IRP hooks.
- Zrzuty pamięci dla podejrzanych procesów.
- Funkcje połączeń z Windows API.
- Pozostawanie nieaktywnym przez określony czas, aby opóźnić wykonanie.
- Tworzenie plików z zadaniami, które mają być wykonywane w określonych przedziałach czasowych.

WAŻNE
Raporty HTML są dostępne tylko w j. angielskim, niezależnie od języka, którego używasz w GravityZone Control Center.

11.3. Ponowne przesłanie próbki

Z obszaru wysyłania, możesz ponownie przesłać zdetonowane już próbki do lokalnej instancji Sandbox Analyzer bez konieczności ponownego ich wysyłania. Możesz to zrobić dla próbek poprzednio przesłanych do lokalnej instancji Sandbox Analyzer przez sensor, metodę, automatycznie, ręcznie lub przez API.

Aby ponownie przesłać próbkę:

1. Kliknij **Ponownie prześlij do analizy** w karcie wysyłania.
2. W oknie konfiguracji zachowaj ustawienia z poprzedniego razu lub zmień je jak następuje:
   a. Pod **Zarządzanie obrazem**, wybierz wirtualną maszynę, którą chcesz wykorzystać do detonacji.
   b. W menu **Konfiguracja detonacji**, skonfiguruj następujące ustawienia:
      i. **Limit czasu dla detonacji próbki (minuty)**. Przydziel określona ilość czasu na ukończenie analizy próbki. Wartość domyślna to 4 minuty, ale czasami analiza może zająć więcej czasu. Pod koniec skonfigurowanego odstępu czasowego Sandbox Analyzer przerywa analizę i generuje raport na podstawie danych zebranych do tego momentu. Jeśli zostanie przerwana przed zakończeniem, analiza może zawierać niedokładne wyniki.

ii. **Liczba dozwolonych powtórzeń**. W przypadku nieoczekiwanych błędów Sandbox Analyzer próbuje zdetonować próbkę zgodnie z konfiguracją aż do zakończenia analizy. Wartość domyślna to 2. Oznacza to, że w przypadku błędu Sandbox Analyzer spróbuje jeszcze dwa razy zdetonować próbkę.

iii. **Filtrowanie wstępne**. Wybierz tę opcję, aby wykluczyć z detonacji próbki już przeanalizowane.

iv. **Dostęp do Internetu podczas detonacji**. Podczas analizy niektóre próbki wymagają połączenia z Internetem, aby zakończyć analizę. Aby uzyskać najlepszy wynik, zaleca się włączenie tej opcji.

c. Pod **Profil detonacji**, dostosuj poziom złożoności analizy behawioralnej, jednocześnie wpływając na przepustowość Sandbox Analyzer. Na przykład, jeśli jest ustawiony na **Wysoki**, Sandbox Analyzer wykonałby dokładniejszą analizę na mniejszej liczbie próbek w tym samym przedziale czasu niż na **Średni** lub **Niski**.

3. Kliknij **Ponownie wyślij**.

Po ponownym wysłaniu strona **Sandbox Analyzer** wyświetla nową kartę i przechowywanie danych dla tej próbki jest odpowiednio przedłużone.

Notatka
Opcja **Ponownie prześlij do analizy** jest dostępna dla próbek wciąż dostępnych w magazynie danych Sandbox Analyzer. Upewnij się, że przechowywanie danych jest skonfigurowane na stronie ustawień polityki **Sandbox Analyzer > Menedżer Sandbox**

11.4. Usuwanie Kart Zgłoszeń

Aby usunąć kartę zgłoszenia, której już nie potrzebujesz:

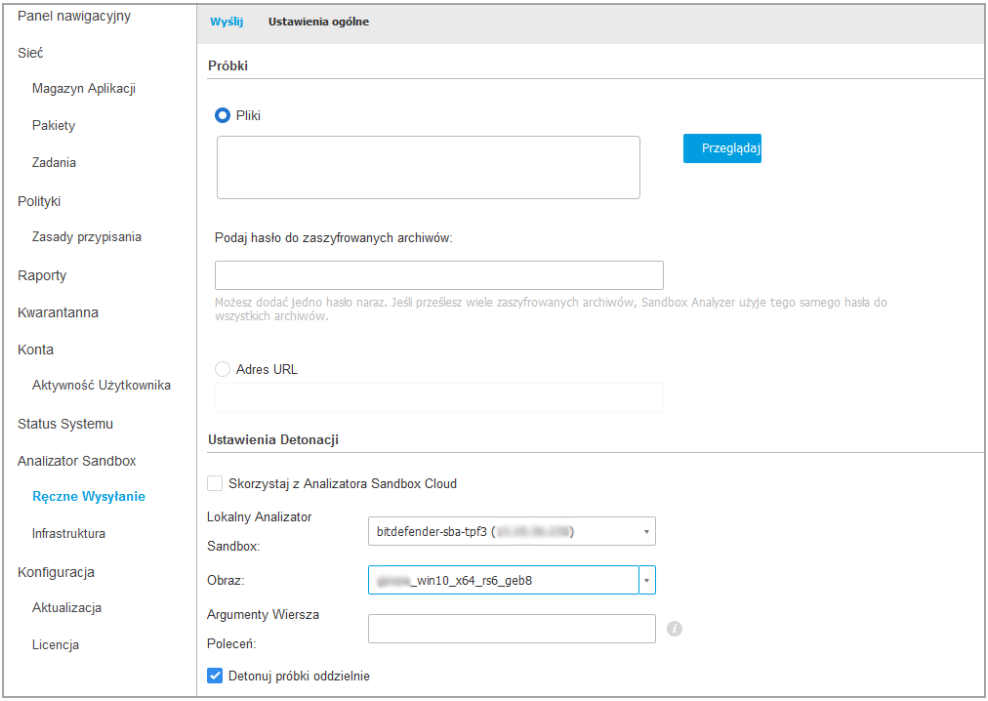
1. Przejdź do karty zgłoszenia, którą chcesz usunąć.
2. Kliknij opcję **Usuń Wpis** po lewej stronie karty.
3. Kliknij **Tak**, aby potwierdzić akcję.

Notatka
Wykonując poniższe czynności, usuwasz tylko kartę zgłoszenia. Informacje dotyczące zgłoszenia są nadal dostępne w raporcie **Wyniki Sandbox Analyzer (Nieaktualne)**. Jednak ten raport będzie nadal obsługiwany tylko przez ograniczony czas.

11.5. Ręczne Wysyłanie

Z **Sandbox Analyzer > Zgłoszenia Ręczne** możesz wysyłać próbki podejrzanych obiektów do Sandbox Analyzer, aby określić, czy są to zagrożenia, czy też nieszkodliwe pliki. Możesz również uzyskać dostęp do strony **Ręczne Wysyłanie**, klikając przycisk **Prześlij próbkę** w prawym górnym rogu obszaru filtrowania na stronie Sandbox Analyzer.

Notatka
Ręczne Wysyłanie Sandbox Analyzer jest zgodne ze wszystkimi przeglądarkami internetowymi wymaganymi przez Control Center, z wyjątkiem Internet Explorera 9. Aby wysłać obiekty do Sandbox Analyzer, zaloguj się do Control Center za pomocą jakiejkolwiek innej obsługiwanej przeglądarki internetowej wymienionej w „Łączenie z Control Center” (p. 19).



Sandbox Analyzer > Ręczne Wysyłanie

Aby przesłać próbki do Sandbox Analyzer:

1. Na stronie **Prześlij**, w obszarze **Próbki** wybierz typ obiektu:
   a. **Pliki**. kliknij przycisk **Przeglądaj**, aby wybrać obiekty, które chcesz przesłać do analizy behawioralnej. W przypadku archiwów chronionych hasłem można zdefiniować jedno hasło na jedną przesłaną sesję w dedykowanym polu. Podczas procesu analizy Sandbox Analyzer stosuje określone hasło do wszystkich przesłanych archiwów.
   b. **URL**. Wypełnij odpowiednie pole dowolnym adresem URL, który chcesz przeanalizować. Możesz przesłać tylko jeden adres URL na sesję.
2. W obszarze **Ustawienia detonacji** skonfiguruj parametry analizy dla bieżącej sesji:
   - Instancja Sandbox Analyzer którą chcesz użyć. Możesz wybrać instancję w Chmurze lub lokalnie zainstalowaną instancję Sandbox Analyzer.

     Jeżeli zdecydujesz się wykorzystać lokalną instancję Sandbox Analyzer, możesz wybrać wiele wirtualnych maszyn do których możesz wysłać próbkę.
   - **Argumenty Wiersza Poleceń**. Dodaj tyle argumentów wiersza poleceń, ile chcesz, oddzielonych spacjami, aby zmienić działanie niektórych programów, takich jak pliki wykonywalne. Argumenty wiersza polecenia odnoszą się do wszystkich przesłanych próbek podczas analizy.
   - **Detonuj próbki oddzielnie**. Zaznacz pole wyboru, aby pliki z pakietu były analizowane jeden po drugim.
3. Pod **Profil detonacji**, dostosuj poziom złożoności analizy behawioralnej, jednocześnie wpływając na przepustowość Sandbox Analyzer. Na przykład, jeśli jest ustawiony na **Wysoki**, Sandbox Analyzer wykonałby dokładniejszą analizę na mniejszej liczbie próbek w tym samym przedziale czasu niż na **Średni** lub **Niski**.
4. Na stronie **Ustawienia ogólne** możesz tworzyć konfiguracje, które dotyczą wszystkich ręcznych zgłoszeń, niezależnie od sesji:
   a. **Limit czasu dla detonacji próbki (minuty)**. Przydziel określona ilość czasu na ukończenie analizy próbki. Wartość domyślna to 4 minuty, ale czasami analiza może zająć więcej czasu. Pod koniec skonfigurowanego odstępu czasowego Sandbox Analyzer przerywa analizę i generuje raport na podstawie danych zebranych do tego momentu. Jeśli zostanie przerwana przed zakończeniem, analiza może zawierać niedokładne wyniki.

b. **Liczba dozwolonych powtórzeń**. W przypadku nieoczekiwanych błędów Sandbox Analyzer próbuje zdetonować próbkę zgodnie z konfiguracją aż do zakończenia analizy. Wartość domyślna to 2. Oznacza to, że w przypadku błędu Sandbox Analyzer spróbuje jeszcze dwa razy zdetonować próbkę.

c. **Filtrowanie wstępne**. Wybierz tę opcję, aby wykluczyć z detonacji próbki już przeanalizowane.

d. **Dostęp do Internetu podczas detonacji**. Podczas analizy niektóre próbki wymagają połączenia z Internetem, aby zakończyć analizę. Aby uzyskać najlepszy wynik, zaleca się włączenie tej opcji.

e. Kliknij **Zapisz** aby zapisać zmiany.

5. Wróć do strony **Wyślij**
6. Kliknij **Wyślij**. Pasek postępu wskazuje status przesłania.

   Po wysłaniu strona **Sandbox Analyzer** wyświetli nową kartę. Po zakończeniu analiza karta dostarczy wyrok i odpowiednie szczegóły.

Notatka
Aby ręcznie wysłać próbki do Sandbox Analyzer musisz mieć uprawnienia **Zarządzanie Sieciami**.

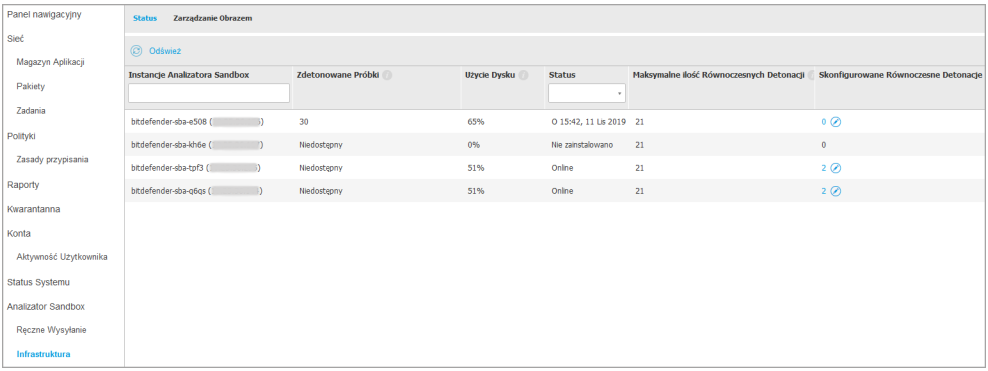
11.6. Zarządzanie infrastrukturą Sandbox Analyzer

W sekcji **Sandbox Analyzer > Infrastruktura**, możesz wykonać następujące akcje powiązane z lokalnie zainstalowaną instancją Sandbox Analyzer:

- Sprawdź status instancji Sandbox Analyzer
- Skonfiguruj równoczesne detonacje
- Sprawdź status obrazu wirtualnej maszyny
- Skonfiguruj i zarządzaj obrazami wirtualnej maszyny

11.6.1. Sprawdzanie statusu Sandbox Analyzer

Po wdrożeniu i skonfigurowaniu wirtualnego urządzenia Sandbox Analyzer na Hipernadzorcy ESXI możesz zdobyć informacje o lokalnej instancji Sandbox Analyzer ze strony **Status**.



Sandbox Analyzer > Infrastruktura > Status

Tabela dostarcza Ci następujące dane:

- **Nazwa instancji Sandbox Analyzer**. Każda nazwa odpowiada instancji Sandbox Analyzer zainstalowanej na hipernadzorcy ESXi Możesz zainstalować Analizator Sandbox na wielu hipernadzorcach ESXi
- **Zdetonowane próbki**. Wartość określa liczbę przeanalizowanych próbek od czasu licencjonowania instancji Sandbox Analyzer po raz pierwszy.
- **Użycie dysku**. Procenty wskazują ilość zajętego miejsca na dysku przez Sandbox Analyzer w magazynie danych.
- **Status**. W tej kolumnie zobaczysz czy instancja Sandbox Analyzer jest online, offline, nie zainstalowana, instalacja jest w trakcie lub czy zakończyła się niepowodzeniem.
- **Maksymalne ilość równoczesnych detonacji**. Wartość przedstawia maksymalną liczbę wirtualnych maszyn, które Sandbox Analyzer może utworzyć do zdetonowania próbek. W danym czasie jedna wirtualna maszyna może przeprowadzić jedną detonację. Liczba wirtualnych maszyn jest określana przez liczbę dostępnych zasobów sprzętowych dostępnych na ESXi.
- **Skonfigurowane równoczesne detonacje**. Jest to faktyczna liczba utworzonych wirtualnych maszyn oparta na dostępnej licencji.
- **Użyj proxy**. Kliknij przełącznik Włączone/Wyłączone aby włączyć lub wyłączyć komunikację pomiędzy GravityZone Control Center i instancjami Sandbox Analyzer przez serwer proxy. Aby ustawić proxy, przejdź do **Konfiguracja > Proxy**

w głównym menu Control Center Jeżeli nie ma ustawionego proxy, Control Center zignoruje tę opcje.

Aby uzyskać więcej informacji na temat konfiguracji proxy, zapoznaj się z rozdziałem **Instalacja Ochrony > GravityZone Instalacja > Konfiguracja Control Center Ustawienia > Proxy** w Poradniku Instalacji GravityZone.

Notatka
Control Center tylko używa tego do komunikacji z instancjami Sandbox Analyzer On-Premises. Aby konfigurować się z instancją Sandbox Analyzer w chmurze, Control Center wykorzystuje serwer proxy skonfigurowany w ustawieniach polityki Sandbox Analyzer.
Te proxy jest również inne od tego skonfigurowanego na stronie ustawień **Ogólne > Ustawienia**, które zapewnia komunikację pomiędzy punktami końcowymi i komponentami GravityZone.

Możesz wyszukiwać i filtrować kolumny po nazwie i statusie Sandbox Analyzer. Użyj przycisków w prawym górnym rogu tabeli, aby odświeżyć stronę i pokazać lub ukryć filtry i kolumny.

11.6.2. Konfigurowanie Równoczesnych Detonacji

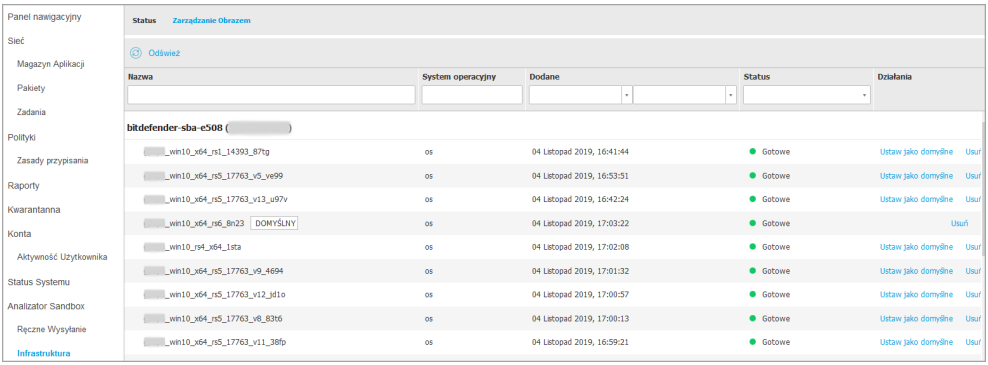
Na stronie **Status** można skonfigurować równoczesne detonacje, reprezentujące liczbę maszyn wirtualnych, które mogą jednocześnie uruchamiać i zdetonować próbki w instancji Sandbox Analyzer. Liczba równoczesnych detonacji zależy od zasobów sprzętowych i dystrybucji miejsc licencyjnych w wielu instancjach Sandbox Analyzer.

Aby skonfigurować równoczesne detonacje:

1. Kliknij w numer lub ikonę **Edytuj** w kolumnie **Skonfigurowane Jednoczesne Detonacje**
2. W nowym oknie określ w odpowiednim polu ilość jednoczesnych detonacji, które chcesz przydzielić do instancji Sandbox Analyzer.
3. Kliknij **Zapisz**.

11.6.3. Sprawdzanie Statusu Obrazów WM

Sandbox Analyzer wykorzystuje obrazy maszyn wirtualnych jako środowiska detonacyjne do przeprowadzania analizy behawioralnej na przesłanych próbkach. Możesz sprawdzić status wirtualnych maszyn na **Strona Zarządzania obrazami**.



Sandbox Analyzer > Infrastruktura > Zarządzanie Obrazem

Tabela dostarcza ci następujących detali:

- **Nazwa** dostępnych obrazów wirtualnych maszyn jak określono w konsoli urządzenia Sandbox Analyzer. Wiele obrazów wirtualnych maszyn jest zgrupowanych pod tą samą instancją Analizatora Sandbox.
- **System operacyjny**, jak określono w konsoli urządzenia Sandbox Analyzer.
- Czas dodania obrazu wirtualnej maszyny.
- **Status**. W tej kolumnie dowiesz się czy obraz wirtualnej maszyny jest nowy i może być przygotowany do detonacji, jest gotowy do detonacji lub czy proces przygotowania się nie powiódł.
- **Działania**. W tej kolumnie dowiesz się co możesz zrobić z obrazami wirtualnych maszyn w zależności od ich statusu: budowanie obrazów do detonacji, ustawienie ich jako domyślne środowisko detonacji lub usuwanie ich.

11.6.4. Konfigurowanie i Zarządzanie obrazami WM

Budowanie Maszyn Wirtualnych do detonacji

Aby detonować próbki z wykorzystanie lokalnej instancji Analizatora Sandbox, musisz zbudować dedykowane maszyny wirtualne. Strona **Zarządzanie Obrazem** pozwoli Ci na tworzenie wirtualnych maszyn do detonacji, pod warunkiem, że dodano obrazy WM w konsoli urządzenia Analizatora Sandbox.

Notatka
Aby nauczyć się jak dodawać obrazy WM w konsoli urządzenia Sandbox Analyzer odnieś się do rozdziału **Instalacja Wirtualnego Urządzenia Analizator Sandbox**. w Podręczniku Instalacji GravityZone.

Aby zbudować wirtualne maszyny do detonacji w kolumnie **Akcje**, kliknij opcję **Zbuduj obraz** dla obrazów WM ze statusem: **Nowy - wymaga zbudowania**. Budowanie wirtualnej maszyny zazwyczaj wymaga od 15 do 30 minut, w zależności od rozmiaru. Gdy budowanie zostanie zakończono, status wirtualnej maszyny zmienia się na **Gotowa**.

Konfigurowanie Domyślnej Wirtualnej Maszyny

Instancja Sandbox Analyzer może mieć zainstalowane i skonfigurowane wiele obrazów jako maszyny wirtualne do detonacji. W przypadku automatycznego wysyłania, Sandbox Analyzer użyje pierwszego zbudowanego obrazu WM do zdetonowania próbek.

Możesz zmienić to zachowanie konfigurując domyślny obraz WM. Aby to zrobić kliknij opcję **Ustaw jako domyślny** dla preferowanego obrazu WM.

Usuwanie Wirtualnych Maszyn

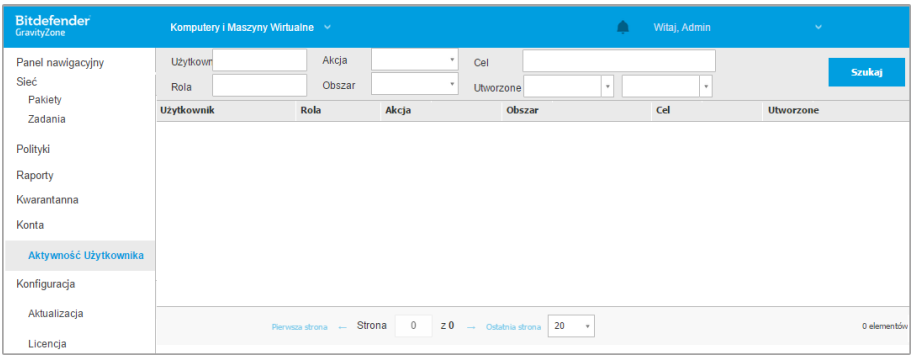
Aby usunąć obraz wirtualnej maszyny ze strony **Zarządzanie obrazem** kliknij **Usuń** w zakładce **Kolumny**. W oknie potwierdzającym kliknij **Usuń obraz**.

12. DZIENNIK AKTYWNOŚCI UŻYTKOWNIKA

Control Center rejestruje wszystkie operacje i akcje wykonane przez użytkowników. Lista aktywności użytkownika zawiera poniższe wydarzenia, zależne od twojego poziomu dostępu administracyjnego:

- Logowanie i wylogowywanie
- Tworzenie, edytowanie, zmiana nazwy i usuwanie raportów
- Dodawanie i usuwanie portletów z panelu
- Tworzenie, edytowanie i usuwanie poświadczeń
- Tworzenie, modyfikowanie, pobieranie i usuwanie pakietów internetowych
- Tworzenie zadań sieciowych
- Rozpoczynanie, kończenie, anulowania i zatrzymywanie procesów rozwiązywania problemów na zainfekowanych maszynach
- Tworzenie, edytowanie, zmiana nazwy i usuwanie kont użytkowników
- Usuwanie i przesuwanie punktów końcowych pomiędzy grupami
- Tworzenie, przesuwanie, zmiana nazwy i usuwanie grup
- Usuwanie i przywracanie plików kwarantanny
- Tworzenie, edytowanie i usuwanie kont użytkowników
- Tworzenie, edytowanie i usuwanie reguł uprawnień dostępu.
- Tworzenie, edytowanie, zmienianie nazwy, przypisywanie i usuwanie polityk
- Edytowanie ustawień uwierzytelniania dla kont GravityZone.
- Tworzenie, edytowanie, synchronizowanie i usuwanie integracji Amazon EC2
- Tworzenie, edytowanie, synchronizowanie i usuwanie integracji Microsoft Azure
- Aktualizacja urządzenia GravityZone.

Aby zbadać zapisy aktywności użytkownika, przejdź do strony **Konta > Aktywność Użytkownika** i wybierz odpowiednie widoki sieciowe z selektor widoku.



Strona aktywności użytkownika

Aby wyświetlić zapisane wydarzenia , które Cie interesują, musisz zdefiniować wyszukiwanie. Uzupełnij dostępne pola kryteriami wyszukiwania i naciśnij przyciszk **Szukaj**. Wszystkie wpisy pasujące do twoich kryteriów zostaną wyswietlone w tabeli.

Kolumny tabeli dostarczają przydatnych informacji na temat wymienionych wydarzeń:

- Nazwa użytkownika, który wykonał akcję.
- Rola użytkownika.
- Akcja, która spowodowała zdarzenie.
- Rodzaj obiektów konsoli na które miała wpływ akcja.
- Określ obiekty konsoli, na które miała wpływ akcja.
- Czas wystąpienia zdarzenia.

Aby posortować wydarzenia według określonej kolumny, naciśnij na nagłówek kolumny. Naciśnij nagłówek kolumny ponownie aby odwrócić kolejność sortowania.

Aby zobaczyć szczegółowe informacje o wydarzeniu, wybierz je i sprawdź sekcje pod tabelą.

13. UŻYWANIE NARZĘDZI

13.1. Iniekcja Narzędzi Niestandardowych z HVI

Bitdefender HVI uwalnia Cię od problemów, gromadząc dane pochodzące z analiz lub wykonując czynności związane z regularną obsługą zadań na maszynach wirtualnych w środowisku Citrix, umożliwiając wstrzykiwanie na bieżąco narzędzi zewnętrznych do systemów operacyjnych gościa. Te operacje są wykonywane za pomocą Bezpośrednich kontroli interfejsów API (bez połączenia z TCP/IP) i bez zakłócania użytkowników końcowych. W tym celu, narzędzia muszą być w stanie działać w tle.

GravityZone zapewnia 3 GB miejsca na bezpieczne przechowywanie narzędzi oraz miejsce, do którego można wstrzyknąć systemy operacyjne gościa.

Aby przesłać zestawy narzędzi do GravityZone:

1. Pobierz najnowszą wersję zestawu narzędzi dla swojego komputera.
2. Zarchiwizuj zestaw w pliku ZIP.
3. Przejdź do GravityZone Control Center i kliknij menu **Narzędzi** w lewym dolnym rogu strony. Wyświetlana jest strona **Centrum Zarządzania Narzędziami**.
4. Kliknij odpowiedni przycisk przesyłania w górnej części tabeli, w oparciu o docelowy system operacyjny: **Prześlij narzędzie Windows** lub **Prześlij narzędzie Linux**.
5. Jeśli narzędzia są przeznaczone dla systemu Windows, należy wybrać odpowiednią architekturę komputera z menu rozwijanego.
6. Zlokalizuj plik ZIP, zaznacz go, a następnie kliknij przycisk **Otwórz**.

   W przypadku dużych plików, przesyłanie może potrwać kilka minut. Po zakończeniu narzędzie jest dodawane do tabeli, a pasek postępu nad tabelą powoduje odświeżenie informacji na temat dostępnej przestrzeni dla przyszłych plików.

Oprócz nazwy narzędzia, tabela zawiera użyteczne informacje, takie jak:

- System operacyjny i platformę, na której uruchomione są narzędzia.
- Krótki opis narzędzia. Jeśli chcesz, możesz w każdej chwili edytować to pole.
- Nazwa użytkownika, który przesłał narzędzie.

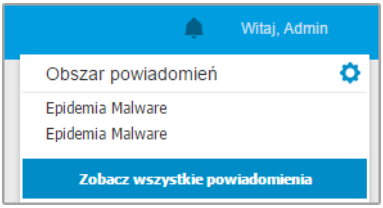
- Status przesyłania. Sprawdź to pole, aby upewnić się, że narzędzie zostało przesłane poprawnie.
- Data i czas przesyłania.

Następnie, dzięki politykom możesz zaplanować, kiedy wstrzykiwać narzędzia lub wstrzykiwać je w dowolnym momencie, uruchamiając zadania z poziomu strony **Sieci**.

Jeśli nie używasz już narzędzi, wybierz je, a następnie kliknij przycisk **Usuń** w górnej części tabeli. Należy potwierdzić, klikając **Tak**.

14. POWIADOMIENIA

W zależności od zdarzeń mogących wpłynąć na twoją sieć, Control Center wyświetli różne powiadomienia, informując o sranie bezpieczeństwa twojego środowiska. Powiadomienia zostaną wyświetlone w **Obszarze Powiadomień**, znajdującym się po prawej stronie Control Center.



Obszar powiadomień

Gdy nowe zdarzenie zostanie wykryte w sieci, ikona 11 w prawym górnym rogu Control Center wyświetli liczbę nowych wykrytych zdarzeń. Klikając ikonę wyświetla się Obszar Powiadomień zawierający listę wykrytych zdarzeń.

14.1. Rodzaje powiadomień

To jest lista aktywnych rodzajów powiadomień:

Epidemia Malware

To powiadomienie jest wysłane do użytkowników, którzy mają przynajmniej 5% z wszystkich zarządzanych obiektów sieciowych zainfekowanych przez to samo malware.

Możesz skonfigurować próg wybuchu epidemii malware według własnych potrzeb w oknie **Ustawienia Powiadomień** Aby uzyskać więcej informacji, zapoznaj się z „Konfiguracja ustawień powiadomień” (p. 494).

Zagrożenia wykryte przez HyperDetect nie wchodzą w zakres niniejszego powiadomienia.

Dostępność formatu Syslog: JSON, CEF

Licencja wygasła

Powiadomienie jest wysyłane 30, 7 i 1 dzień przed wygaśnięciem licencji.

Musisz mieć uprawnienia do **Zarządzania Firmą**, aby zobaczyć to powiadomienie.

Dostępność formatu Syslog: JSON, CEF

Limit wykorzystania licencji został osiągnięty

To powiadomienie jest wysyłane jeżeli wszystkie z aktywnych licencji zostały użyte.

Dostępność formatu Syslog: JSON, CEF

Limit wykorzystania licencji został prawie osiągnięty

To powiadomienie jest wysyłane jeżeli 90% z aktywnych licencji zostało użytych.

Musisz mieć uprawnienia do **Zarządzania Firmą**, aby zobaczyć to powiadomienie.

Dostępność formatu Syslog: JSON, CEF

Limit wykorzystania licencji Exchange został osiągnięty

Powiadomienie to jest uruchamiane za każdym razem, gdy liczba chronionych skrzynek pocztowych z serwerów Exchange osiągnie limit określony na klucz licencyjny.

Musisz mieć uprawnienia do **Zarządzania Firmą**, aby zobaczyć to powiadomienie.

Dostępność formatu Syslog: JSON, CEF

Nieważne poświadczenia użytkownika Exchange

Takie powiadomienie jest wysyłane, gdy nie można uruchomić skanowania na żądanie na docelowym serwerze Exchange z powodu nieprawidłowych poświadczeń użytkownika Exchange.

Dostępność formatu Syslog: JSON, CEF

Stan aktualizacji

To powiadomienie jest wysyłane co tydzień, jeśli w twojej sieci zostaną znalezione stare wersje produktów.

Dostępność formatu Syslog: JSON, CEF

Aktualizacja dostępna

To powiadomienie poinformuje Cię o dostępnej nowej aktualizacji GravityZone, nowej paczce lub nowej aktualizacji produktu.

Dostępność formatu Syslog: JSON, CEF

Połączenie z Internetem

To powiadomienie jest uruchamiane gdy zmiana połączenia Internetowego zostanie wykryta przez poniższe procesy:

- Ważności licencji
- Żądanie uzyskania podpisania certyfikatu Apple
- Komunikacja urządzeń przenośnych Apple i Android
- Dostęp do Konta BitDefender

Dostępność formatu Syslog: JSON, CEF

Połączenie SMTP

To powiadomienie jest wysyłane za każdym razem gdy BitdefenderGravityZone wykrywa zmiany w odniesieniu do połączeń z serwerem poczty.

Dostępność formatu Syslog: JSON, CEF

Użytkownicy urządzeń mobilnych bez adresów e-mail

To powiadomienie jest wysyłane po dodaniu urządzeń przenośnych dla wielu użytkowników i jeden lub kilku wybranych użytkowników nie posiada adresu e-mail przypisanego do jego konta. To powiadomienie ma ostrzec cie, że użytkownicy bez przypisanego adresu e-mail nie mogą zapisać się do urządzeń przenosnych przypisanych do nich, gdyż dane aktywacyjne są wysyłane w wiadomości e-mail.

Szczegóły na temat dodawania urządzeń mobilnych wielu użytkownikom, odnieś się do Przewodnika Instalacji GravityZone.

Dostępność formatu Syslog: JSON, CEF

Kopia zapasowa bazy danych

To powiadomienie informuje cie o stanie zaplanowanych kopi zapasowych bazy danych, czy są udane czy nie. Jeżeli kopia zapasowa bazy danych nie powiedzie się, powiadomienie wyświeli powód niepowodzenia.

Dla uzyskania szczegółów na temat konfiguracji bazy danych kopii zapasowych GravityZone, zapoznaj się z Podręcznikiem Instalacyjnym GravityZone.

Dostępność formatu Syslog: JSON, CEF

Wykryto złośliwe oprogramowanie Exchange

Zawiadomienie to informuje użytkownika o wykryciu malware na serwerze Exchange w Twojej sieci.

Dostępność formatu Syslog: JSON, CEF

Zaawansowany Anty-Exploit

To powiadomienie informuje Cię gdy Zaawansowany Anty-Exploit wykrył próby wykorzystania exploita w twojej sieci.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie Antymalware

To powiadomienie informuje o wykryciu malware na komputerze końcowym w twojej sieci. Te powiadomienie jest tworzone dla każdej detekcji malware, dostarcza szczegółów na temat zainfekowanego punktu końcowego (nazwa, IP, zainstalowany agent, rodzaj skanowania, wykryte malware, wersja sygnatury, czas detekcji i rodzaj silnika skanowania.

Dostępność formatu Syslog: JSON, CEF

Integracja Out of Sync

To powiadomienie jest wysyłane, gdy nie można zsynchronizować istniejącej integracji platformy wirtualnej z GravityZone. W ustawieniach powiadomień możesz wybrać integracje, dla których chcesz otrzymywać powiadomienia, gdy wystąpi błąd synchronizacji. Możesz sprawdzić więcej informacji o stanie synchronizacji w szczegółach powiadomienia.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie Antyphishing

To powiadomienie informuje cię za każdym razem jak agent punktu końcowego blokuje znana stronę phishing przed próba dostępu. To powiadomienie również podaje szczegóły o próbach dostępu przez punkty końcowe do niezaufanych stron (nazwa i IP), zainstalowanym agencie i blokowanych URL.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie Firewall

Z tym powiadomieniem jesteś informowany za każdym razem gdy moduł zapory sieciowej zainstalowanego agenta blokuje port skanowania lub aplikacje przed dostępem do internetu w zależności od zastosowanej polityki.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie ATC/IDS

To powiadomienie jest wysyłane za każdym razem jak potencjalnie niebezpieczna aplikacja jest wykryta i zablokowana na punkcie końcowym w twojej sieci. Znajdziesz szczegółowe informacje o typie aplikacji, nazwie i ścieżce, a także o identyfikatorze i ścieżce procesu nadrzędnego oraz linii poleceń, która uruchomiła proces, jeśli tak jest.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie Kontroli użytkownika

To powiadomienie jest wysyłane za każdym razem gdy aktywność użytkownika taka jak przeglądanie stron internetowych lub aplikacje są zablokowane przez klienta na punkcie końcowym, zgodnie z zastosowaną polityką.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie Ochrony Danych

To powiadomienie jest wysyłane za każdym razem gdy ruch danych jest zablokowany na punkcie końcowym zgodnie z regułami ochrony danych.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie modułów produktu

To powiadomienie jest wysyłane za każdym razem, gdy moduł bezpieczeństwa na zainstalowanym agencie zostanie włączony lub wyłączony.

Dostępność formatu Syslog: JSON, CEF

Status zdarzenia Security Server

Ten rodzaj powiadomień dostarcza informacje o zmianach określonego Security Server zainstalowanego w twojej sieci. Zmiany stanu Security Server odnoszą się do następujących zdarzeń: wyłączone/włączone, aktualizacja produktu, aktualizacja zawartości zabezpieczeń i wymagane ponowne uruchomienie.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie Przeciążenia Security Server

Takie powiadomienie jest wysłane, kiedy skanowanie ładuje się na Security Server w twojej sieci i przekroczy zdefiniowany próg.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie rejestracji produktu

To powiadomienie informuje cię o zmianach stanu rejestracji zainstalowanych agentów w twojej sieci.

Dostępność formatu Syslog: JSON, CEF

Audyt Uwierzytelniania

Powiadomienie to informuje, kiedy inne konto GravityZone, z wyjątkiem Twojego własnego, było używane do logowania się do Control Center z nierozpoznanego urządzenia.

Dostępność formatu Syslog: JSON, CEF

Logowanie z Nowego Urządzenia

Takie powiadomienie informuje, że Twoje konto GravityZone zostało użyte do logowania się do Control Center z urządzenia, którego nie używałeś do tego celu wcześniej. Zgłoszenie jest automatycznie skonfigurowane, aby było widoczne zarówno w Control Center jak i na mailu, aby można je było tylko wyświetlić.

Dostępność formatu Syslog: JSON, CEF

Certyfikat Wygasa

Zawiadomienie to informuje, że wygasa certyfikat bezpieczeństwa. To powiadomienie jest wysyłane na 30, siedem i jeden dzień przed datą wygaśnięcia.

Dostępność formatu Syslog: JSON, CEF

Aktualizacja GravityZone

Powiadomienie jest wysyłane, gdy aktualizacja GravityZone jest zakończona. Jeśli się nie powiedzie, aktualizacja uruchomi się ponownie w ciągu 24 godzin.

Dostępność formatu Syslog: JSON, CEF

Status Zadań

Zawiadomienie to informuje, albo za każdym razem, gdy status zadania się zmieni lub tylko wtedy, gdy zadanie zakończy się, zgodnie z Twoimi preferencjami.

Dostępność formatu Syslog: JSON, CEF

Nieaktualny serwer aktualizacji

To powiadomienie jest wysyłane, gdy serwer aktualizacji w sieci ma nieaktualną zawartość zabezpieczeń.

Dostępność formatu Syslog: JSON, CEF

Zdarzenie dotyczące incydentów sieciowych

To powiadomienie jest wysyłane za każdym razem, gdy moduł Network Attack Defense wykrywa próbę ataku w sieci. To powiadomienie informuje również, czy próba ataku została przeprowadzona spoza sieci lub z zagrożonego punktu końcowego w sieci. Inne szczegóły zawierają dane dotyczące punktu końcowego, techniki ataku, adresu IP osoby atakującej oraz działań podjętych przez Network Attack Defense.

Dostępność formatu Syslog: JSON, CEF

Raport Użytkownika Został Wygenerowany

To powiadomienie informuje ciebie kiedy raport oparty na zapytaniu został wygenerowany.

Dostępność formatu Syslog: n/a

Wykryto Naruszenie Pamięci

Powiadomienie to informuje o wykryciu przez HVI ataku naruszającego pamięć chronionych maszyn wirtualnych w środowisku Citrix Xen. Powiadomienie zawiera ważne szczegóły, takie jak imię i IP zainfekowanej maszyny, opis zdarzenia, źródło i cel ataku, działania podjęte w celu usunięcia zagrożenia i czas detekcji.

Powiadomienia są tworzone dla następujących przypadków:

- Próby użycia obszaru pamięci w inny sposób niż hypervisor zostały zainicjowane przez Rozszerzone Tabele Strony (EPT).
- Próby procesów wprowadzenia kodu do innych procesów.
- Próby zmiany adresów procesu w tabelach tłumaczeń.
- Próby zmiany Modelu Określonych Rejestrów (MSR).
- Próby zmiany zawartości poszczególnych Obiektów Sterownika lub Tabeli Opisów Przerwań (IDT).
- Próby załadowania konkretnych Rejestrów Kontroli (CR) z niepoprawnymi wartościami.
- Próby załadowania konkretnych Rozszerzonych Rejestrów Kontroli (XCR) z niepoprawnymi wartościami.
- Próby zmiany Tabeli Opisów Globalnych lub Przerwań.

Notatka
Funkcja HVI dla Twojego rozwiązania GravityZone może być dostępna z oddzielnym kluczem licencyjnym.

Dostępność formatu Syslog: JSON, CEF

Nowa aplikacja w Magazynie Aplikacji

To powiadomienie informuje użytkownika, gdy Kontrola Aplikacji wykrywa nową aplikację zainstalowaną na monitorowanych punktach końcowych.

Dostępność formatu Syslog: JSON, CEF

Zablokowana Aplikacja

Te powiadomienie informuje Cię kiedy moduł Kontrola Aplikacji zablokowała lub może zablokować proces nieautoryzowanej aplikacji, w zależności od konfiguracji modułu (Produkcja lub Tryb Testowy)

Dostępność formatu Syslog: JSON, CEF

Wykrywanie Sandbox Analyzer

To powiadomienie ostrzega użytkownika za każdym razem, gdy Sandbox Analyzer wykryje nowe zagrożenie wśród przesyłanych próbek. Zostaną wyświetlone szczegóły, takie jak nazwa hosta lub adres IP punktu końcowego, czas i data wykrycia, rodzaj zagrożenia, ścieżka, nazwa, rozmiar plików i podjęte na każdym znich działania naprawcze.

> **Notatka**
> Nie otrzymasz powiadomień o czystych analizowanych próbkach. Informacje o wszystkich przesłanych próbkach są dostępne w raporcie **Sandbox Analyzer Wyniki (przestarzałe)** oraz w sekcji **Sandbox Analyzer** , w menu głównym Control Center.

Dostępność formatu Syslog: JSON, CEF

Problem z brakującą aktualizacją

To powiadomienie pojawia się, gdy w punktach końcowych w sieci brakuje jednej lub więcej dostępnych aktualizacji.

GravityZone automatycznie wysyła powiadomienie zawierające wszystkie wyniki z ostatnich 24 godzin do daty powiadomienia.

Możesz sprawdzić, które punkty końcowe są w tej sytuacji, klikając przycisk **Wyświetl raport** w szczegółach powiadomienia.

Domyślnie powiadomienie dotyczy aktualizacji zabezpieczeń, ale można je skonfigurować tak, aby informowały również o aktualizacjach niezwiązanych z zabezpieczeniami.

Dostępność formatu Syslog: JSON, CEF

Wykrycie Ransomware

To powiadomienie informuje, gdy GravityZone wykryje atak ransomware w Twojej sieci. Otrzymujesz szczegółowe informacje dotyczące docelowego punktu końcowego, zalogowanego użytkownika, źródła ataku, liczby zaszyfrowanych plików oraz godziny i daty ataku.

W momencie otrzymania powiadomienia atak jest już zablokowany.

Link w powiadomieniu przekierowuje do strony **Aktywność Ransomware**, gdzie można zobaczyć listę zaszyfrowanych plików i odzyskać je, jeśli potrzeba.

Dostępność formatu Syslog: JSON, CEF

Antymalware pamięci

To powiadomienie jest wysyłane po wykryciu złośliwego oprogramowania na urządzeniu magazynującym zgodnym z ICAP. To powiadomienie jest stworzone dla każdego wykrycia malware, typ), wykryte malware i czas wykrycia.

Dostępność formatu Syslog: JSON, CEF

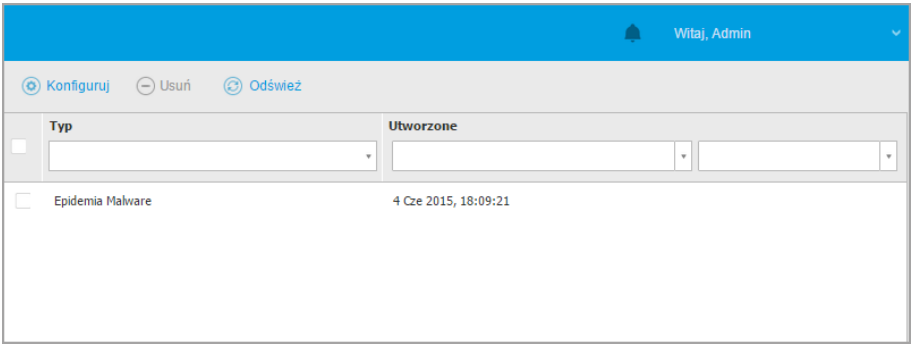
Zablokowane Urządzenia

Te powiadomienie jest wyzwalane gdy zablokowane urządzenie lub urządzenie z uprawnieniami tylko do odczytu łączy się z punktem końcowym. Jeżeli dokładnie to samo urządzanie połączy się wielokrotnie w przeciągu jednej godziny, tylko jedno powiadomienie jest wysyłane w ciągu tego okresu. Jeżeli urządzenie ponownie połączy się po godzinie, pojawi się nowe powiadomienie.

Dostępność formatu Syslog: JSON, CEF

14.2. Zobacz powiadomienia

Aby zobaczyć powiadomienia naciśnij przycisk **Powiadomienia** i naciśnij **Zobacz wszystkie powiadomienia**. Wyświetlana jest tabela zawierająca wszystkie powiadomienia.



Strona powiadomień

W zależności od liczby powiadomień, tabela może obejmować kilka stron (domyślnie tylko 20 wpisów jest wyświetlanych na jednej stronie).

Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli.

Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

Jeżeli jest za mało wpisów, możesz użyć pola wyszukiwania pod nagłówkiem kolumny w menu filtry na górze tabeli, aby odfiltrować wyniki według daty.

- Aby odfiltrować powiadomienia, wybierz rodzaj powiadomień jaki chcesz zobaczyć z menu **Rodzaj**. Jeżeli wiele powiadomień zostało wygenerowanych, możesz wybrać przedziały czasu podczas których powiadomienia zostały wygenerowane, aby zredukować ilość wpisów w tabeli.
- Aby zobaczyć szczegóły powiadomień, naciśnij nazwę powiadomienia w tabeli. Sekcja **Szczegóły** gdzie możesz zobaczyć wydarzenia, które generują powiadomienia, wyświetla sie pod tabelą.

14.3. Usuwanie powiadomień

Aby usunąć powiadomienia:

1. Kliknij przycisk **Powiadomienia** z prawej strony menu i naciśnij **Zobacz Wszystkie Powiadomienia**. Wyświetlana jest tabela zawierająca wszystkie powiadomienia.
2. Wybierz powiadomienia, które chcesz usunąć.
3. Kliknij przycisk **Kasuj** z górnej strony tabeli.

Możesz dodatkowo skonfigurować powiadomienia, które zostaną automatycznie usunięte po określonej ilości dni. Aby uzyskać więcej informacji, odwołaj się do „Konfiguracja ustawień powiadomień” (p. 494).

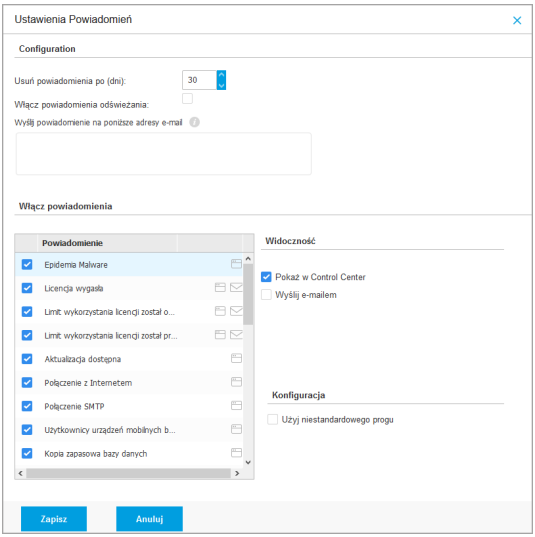
14.4. Konfiguracja ustawień powiadomień

Rodzaj powiadomień jaki ma być wysyłany na adres e-mail, może być konfigurowany dla każdego użytkownika.

Aby skonfigurować ustawienia powiadomień:

1. Kliknij przycisk **Powiadomienia** z prawej strony menu i naciśnij **Zobacz Wszystkie Powiadomienia**. Wyświetlana jest tabela zawierająca wszystkie powiadomienia.

2. Kliknij przycisk **Konfiguruj** z górnej strony tabeli. Okno **ustawienia Powiadomień** jest widoczne.



Ustawienia Powiadomień

Notatka
Masz dodatkowo dostęp do okna **Ustawienia Powiadomień** używając ikony **konfiguracja** z górnego prawego rogu okna **Obszar Powiadomień**.

3. W sekcji **Konfiguracja** możesz zdefiniować poniższe ustawienia:
   - Automatyczne usuwanie powiadomień po pewnym okresie czasu. Ustaw jakąkolwiek liczbę, którą chcesz, pomiędzy 0 a 365 w polu **Usuń powiadomienia po (dni)**.
   - Wybierz pole wyboru **Włącz odświeżanie powiadomień** jeśli chcesz, aby obszar powiadomień automatycznie aktualizował się co 60 sekund.
   - Dodatkowo, możesz wysłać powiadomienia mailem do konkretnych odbiorców. Wpisz adresy e-mail w dedykowanym polu, naciskając klawisz `Enter` po każdym adresie.

4. W sekcji **Włącz Powiadomienia** możesz wybrać rodzaj powiadomień jakie chcesz otrzymywać od GravityZone. Możesz również skonfigurować widoczność i opcje wysyłania indywidualne dla każdego rodzaju powiadomień.

   Wybierz jakie chcesz powiadomienia z listy. Aby uzyskać więcej informacji, odwołaj się do „Rodzaje powiadomień” (p. 485). Podczas wyboru rodzaju powiadomienia, możesz skonfigurować jego swoiste opcje (jeśli dostępne) w obszarze po prawej stronie:

Widoczność

- **Pokaż w Control Center** określa rodzaje zdarzeń wyświetlanych w Control Center, z pomocą przycisku **Powiadomienia**.
- **Logi do serwera** określa typ zdarzenia wysyłanego do pliku `syslog`, w przypadku skonfigurowania syslogu.

  Aby dowiedzieć się w jaki sposób konfigurować serwery syslog, zapoznaj się z Podręcznikiem Instalacyjnym GravityZone.
- **Wyślij przez e-mail** określa rodzaje zdarzeń jakie sa wysyłane na określone adresy e-mail. W tym przypadku, wymaga podania adresu e-mail w odpowiednim polu, naciśnij `Enter` po każdym adresie.

Konfiguracja

- **Użyj niestandardowego progu** - pozwala na definiowanie progu dla występujących zdarzeń, z których wybrane powiadomienia są wysyłane.

  Dla przykładu, powiadomieni o epidemii Malware jest wysyłane domyślnie do użytkowników którzy mają przynajmniej 5% zarządzanych obiektów zainfekowanych przez to samo złośliwe oprogramowanie. Aby zmienić wartość dla progu epidemii malware, włącz opcje **Użyj niestandardowego progu**, następnie podaj wartość jaką chcesz w polu **Próg Epidemii Malware** .
- Jako powiadomienie **Backupu Bazy danych** możesz wybrać powiadamianie jedynie, gdy aktualizacja bazy danych nie powiodą się. Zostaw tą opcję odznaczoną, jeśli chcesz być informowany o wszystkich zdarzeniach powiązanych z kopią zapasową baz danych.
- Dla **Wydarzenia statusu Security Server**, możesz wybrać zdarzenieSecurity Server, które będzie uruchamiało ten typ powiadomienia:

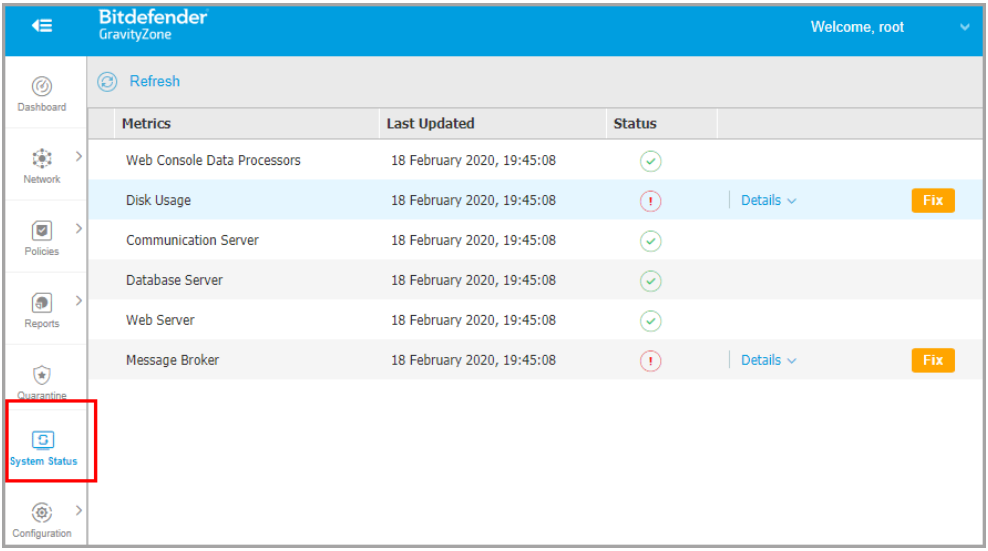
- **Przedawnione** - powiadamia, za każdym razem gdy Security Server w twojej sieci jest przedawniona.
- **Wyłączone** - informuje za każdym razem Security Server zostanie wyłączony w twojej sieci.
- **Wymagany restart** - informuje za każdym razem Security Server że sieć wymaga ponownego uruchomienia.

- Dla **Status Zadania**, możesz wybrać typ statusu który wywoła ten typ powiadomienia:
  - **Dowolny status** - powiadamia za każdym razem o wykonaniu wysłanego z Control Center zadania z dowolnym statusem.
  - **Jedynie nieudane** - powiadamia za każdym razem o nieudanym zadaniu wysłanym z Control Center.

5. Kliknij **Zapisz**.

15. STATUS SYSTEMU

Strona **Status systemu** wyświetla informacje o stanie zdrowia wdrożenia GravityZone, ułatwiając Ci wgląd gdy coś pójdzie nie tak. Ta strona dostarcza metryki systemowe, ich status, kiedy zostały zaktualizowane, wszystko wyświetlone w formacie siatki.



Strona Status Systemu

Kolumna **Metryki** wyświetla wszystkie wskaźniki monitorowane przez GravityZone Control Center. Po więcej informacji o każdej metryce i wiadomościach statusu, odnieś się „Procesory Danych” (p. 522).

Kolumna **Ostatnio Zaktualizowane** wyświetla datę i czas ostatniego sprawdzania statusu metryki.

Kolumna **Status** wyświetla stan każdej metryki: **OK** lub **Uwaga**. Metryka **Status** jet aktualizowana co każde 15 minut lub za każdym razem gdy klikniesz **Odśwież**.

15.1. Status OK

Status OK wskazuje, że metryka zachowuje się normalnie. W tym przypadku żadne dodatkowe informacje nie są wyświetlane.

15.2. Status Uwaga

Status Uwaga wskazuje, że metryka nie działa z normalnymi parametrami.

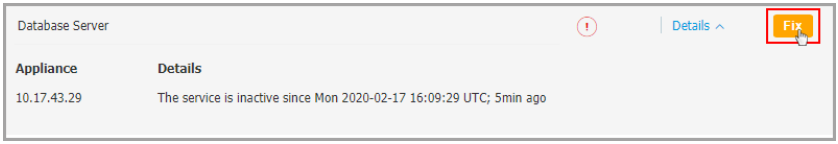
W tym przypadku musisz zbadać co się stało i naprawić aktualne usterki:

1. Kliknij **Szczegóły** aby rozwinąć dodatkowe informacje powiązane z badaną metryką.

Szczegóły Metryki

- W **Urządzenia** możesz znaleźć adresy IP zagrożonych maszyn.
- W **Szczegóły** możesz zobaczyć informacje dotyczące konkretnych metryk.

2. Kliknij **Napraw** aby naprawić metrykę i GravityZone zajmie się resztą.



Szczegóły Metryki

Status metryki wróci na **OK** jak zostanie naprawiona.

Notatka
W przypadku innych problemów związanych z metrykami skontaktuj się w Centrum Wsparcia Biznesowego.

15.3. Metryki

Strona **System Status** zawiera informacje na temat następujących metryk:

- Procesory danych konsoli internetowej

- Użycie Dysku
- Serwer komunikacji
- Serwer bazodanowy
- Serwer Sieciowy
- Agent Wiadomości

Procesory danych konsoli internetowej

Ta metryka monitoruje stan procesorów danych, które są wykorzystywane do kompilowania danych wyświetlonych w Control Center.

Wiadomość Statusu Uwaga	Szczegóły
`Procesory, które zawiodły na tym urządzeniu: < procesor tabeli danych> .`	Jeden lub więcej procesorów danych jest zatrzymanych.
`Urządzenie wirtualne jest wyłączone`	Wirtualne urządzenie używające usług Konsoli Web jest wyłączone.

Po kompletną listę procesorów używanych przez Control Center odnieś się do „Procesory Danych” (p. 522).

Użycie Dysku

Ta metryka monitoruje ilość miejsca na dysku używaną przez każde wirtualne urządzenie, ile wolnego miejsca zostało i całkowite miejsce na dysku. Jeżeli któryś dysk jest wykorzystanych powyżej 80%, metryka wyświetla status **Uwaga**.

Wiadomość Statusu Uwaga	Szczegóły
`Używane miejsce na dysku (nazwa dysku)`	Jeden lub więcej dysków jest wykorzystywany powyżej 80% maksymalnej pojemności.
`Urządzenie wirtualne jest wyłączone`	Zgłoszone wirtualne urządzenie jest wyłączone.

Serwer komunikacji

Ta metryka monitoruje połączenie pomiędzy agentami bezpieczeństwa zainstalowanymi na punktach końcowych i Serwerem Bazy Danych.

Wiadomość Statusu Uwaga	Szczegóły
`Ta usługa jest nieaktywna od <data>`	Usługa przestała działać.

Serwer bazodanowy

Ta metryka monitoruje status bazy danych GravityZone.

Wiadomość Statusu Uwaga	Szczegóły
`Ta usługa jest nieaktywna od <data>`	Usługa przestała działać na jednym z urządzeń.
`Urządzenie wirtualne jest wyłączone`	Wirtualne urządzenie używające Serwera Bazy Danych jest wyłączone.

Serwer Sieciowy

Ta metryka monitoruje stan serwera sieciowego hostującego GravityZone Control Center.

Wiadomość Statusu Uwaga	Szczegóły
`Ta usługa jest nieaktywna od <data>`	Serwer przestał działać na jednym z urządzeń.
`Urządzenie wirtualne jest wyłączone`	Wirtualne urządzenie używające tego serwera jest wyłączone.

Agent Wiadomości

Ta metryka monitoruje stan usługi message broker na urządzeniach z rolami Konsola Web i Serwer Komunikacji.

Wiadomość Statusu Uwaga	Szczegóły
`Usługa brokera wiadomości jest wyłączona na tych urządzeniach`	Usługa przestała działać na jednym z urządzeń.
`Połączenie sieciowe między urządzeniami nie powiodło się`	Połączenie pomiędzy dwoma urządzenia zostało przerwane.
`Urządzenie wirtualne jest wyłączone`	Wirtualne urządzenie używające tej usługi jest wyłączone.

16. UZYSKIWANIE POMOCY

Bitdefender stara się zapewnić swoim klientom najwyższy poziom szybkiej i dokładnej pomocy technicznej. Jeżeli męczy cię jakiś problem lub masz pytania dotyczące produktu Bitdefender, przejdź do naszego Centrum Wsparcia Online. Oferuje kilka zasobów, które możesz użyć do szybkiego znalezienia rozwiązania lub odpowiedzi. Jeśli wolisz, możesz skontaktować się z Obsługą Klienta Bitdefender. Nasi przedstawiciele ds. pomocy technicznej szybko odpowiedzą na twoje pytania oraz zapewnią ci niezbędną pomoc.

Notatka
Możesz dowiedzieć się więcej na temat usług wsparcia jakie oferujemy i sposobów jej udzielania w Centrum pomocy.

16.1. Bitdefender Wsparcie Techniczne

Bitdefender Centrum Pomocy, to miejsce gdzie uzyskasz wszelką pomoc dla Twoich produktów Bitdefender.

Możesz użyć kilku źródeł, aby szybko znaleźć rozwiązanie problemu lub odpowiedź:

- Znana baza artykułów
- Bitdefender forum pomocy
- Dokumentacja produktu

Możesz również użyć ulubionej wyszukiwarki, aby znaleźć więcej informacji o ochronie komputera, produktach Bitdefender i firmie.

Znana baza artykułów

Bazą wiedzy Bitdefender jest dostępne w internecie repozytorium informacji na temat produktów Bitdefender produktów. Przechowuje czytelne raporty z trwających działań zespołu Bitdefender odnośnie pomocy technicznej i naprawiania błędów oraz bardziej ogólne artykuły dotyczące ochrony antywirusowej, szczegółowego zarządzania rozwiązaniami produktu Bitdefender oraz wielu innych zagadnień.

Baza wiedzy Bitdefender jest publiczna i bezpłatna. Informacje, które zawiera, stanowią kolejny sposób na dostarczenie klientom Bitdefender, potrzebnej wiedzy technicznej i wsparcia. Prawidłowe żądania informacji lub raportów o błędach, pochodzące od klientów Bitdefender, w końcu znajdują drogę do Bazy Wiedzy

Bitdefender. jako raporty informujące o poprawkach, sposoby ominięcia problemów czy pliki pomocy produktu i teksty informacyjne.

Baza Wiedzy Bitdefender dla produktów biznesowych jest dostepna w każdej chwili na http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne.

Bitdefender forum pomocy

Forum pomocy technicznej Bitdefender pozwala użytkownikom Bitdefender uzyskać pomoc oraz pomagać innym osobom korzystającym z produktu. Możesz tu opublikować dowolny problem lub pytanie dotyczące twoich produktów Bitdefender.

Pracownicy ds. pomocy technicznej Bitdefender monitorują forum sprawdzając nowe wpisy i zapewniając pomoc. Odpowiedź lub rozwiązanie można także uzyskać od bardziej zaawansowanego użytkownika programu Bitdefender.

Przed zamieszczeniem problemu lub pytania przeszukaj forum w celu znalezienia podobnych lub powiązanych tematów.

Forum pomocy technicznej Bitdefender jest dostępne pod adresem http://forum.bitdefender.com w 5 językach: angielskim, niemieckim, francuskim, hiszpańskim i rumuńskim. Aby uzyskać dostęp do sekcji poświęconej produktom biznesowym, kliknij łącze **Ochrona dla biznesu**.

Dokumentacja produktu

Dokumentacja produktu jest najbardziej kompletnym źródłem informacji o produkcie.

Najłatwiejszy sposób aby dostać się do dokumentacji jest poprzez stronę w Control Center **Pomoc & Wsparcie**. Kliknij swoją nazwę użytkownika w prawym górnym rogu konsoli, wybierz **Pomoc & Wsparcie**, a następnie link przewodnika, którym jesteś zainteresowany. Podręcznik zostanie otwarty w nowej karcie przeglądarki.

Dokumentację można też sprawdzić i pobrać w Centrum Pomocy w sekcji **Dokumentacja** dostępnej na każdej stronie pomocy technicznej.

16.2. Prośba o pomoc

Możesz poprosić o pomoc za pośrednictwem naszego Centrum Wsparcia Online. Wypełnij formularz kontaktowy i wyślij go do nas.

16.3. Używanie Narzędzi Pomocy

Narzędzie wsparcia GravityZone jest stworzone żeby pomagać użytkownikom i łatwo uzyskać potrzebne informacje ze wsparcia technicznego. Uruchom Narzędzie Wsparcia na zagrożonych komputerach i wyślij otrzymane archiwum z informacjami o problemach do wsparcia przedstawiciela Bitdefender.

16.3.1. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Windows

Uruchamianie aplikacji Support Tool

Aby wygenerować dziennik na zagrożonym komputerze, użyj jednej z następujących metod:

- Wiersz poleceń

  Dla problemów z BEST, zainstalowanego na komputerze.

- Problem z instalacją

  Dla sytuacji gdzie BEST nie jest zainstalowany na komputerze i instalacja kończy się niepowodzeniem.

Metoda wiersza poleceń

Używając wiersza poleceń możesz zbierać logi bezpośrednio z zainfekowanego komputera. Metoda ta przydaje się w sytuacjach gdy nie masz dostępu do Centrum Kontroli GravityZone lub komputer nie komunikuje się z konsolą.

1. Otwórz wiersz polecenia z uprawnieniami administratora.
2. Przejdź do folderu instalacji produktu. Domyślna ścieżka to:

   ```
   C:\Program Files\Bitdefender\Endpoint Security
   ```

3. Zbieraj i zapisuj logi, uruchamiając to polecenie:

   ```
   Product.Support.Tool.exe collect
   ```

   Dzienniki są domyślnie zapisywane w `C:\Windows\Temp`.

   Opcjonalnie, jeśli chcesz zapisać dziennik Support Tool w niestandardowej lokalizacji, użyj ścieżki opcji:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Przykład:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Podczas wykonywania polecenia można zauważyć na ekranie pasek postępu. Po zakończeniu procesu dane wyjściowe wyświetlają nazwę archiwum zawierającego dzienniki i ich lokalizację.

By wysłać logi do Biznesowej Pomocy Bitdefender przejdź do `C:\Windows\Temp` lub do niestandardowej lokacji i znajdź archiwum o nazwie `ST_[computername]_[currentdate]`. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

Problem z instalacją

1. By pobrać BEST Support Tool kliknij tutaj.
2. Uruchom plik wykonywalny jako administrator. Zostanie wyświetlone okno.
3. Wybierz lokację by zapisać archiwum logów.

   Podczas zbierania logów zauważysz pasek postępu na ekranie. Po zakończeniu procesu dane wyjściowe wyświetlają nazwę archiwum i ich lokalizację.

By wysłać logi do Biznesowej Pomocy Bitdefender przejdź do wybranej lokacji i znajdź archiwum o nazwie `ST_[computername]_[currentdate]`. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

16.3.2. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Linux

Dla systemów operacyjnych Linux, Narzędzie Wsparcia jest zintegrowane wraz z agentem bezpieczeństwa Bitdefender.

Aby zebrać informacje na temat systemu Linux przy pomocy Narzędzia Wsparcia, uruchom następujące polecenia:

```
# /opt/BitDefender/bin/bdconfigure
```

korzystając z następujących dostępnych opcji:

- `--help` aby wyświetlić listę wszystkich poleceń Narzędzia Wsparcia
- `enablelogs` aby włączyć produkt i dziennik modułu komunikacyjnego (wszystkie usługi zostaną automatycznie uruchomione ponownie)
- `disablelogs` aby wyłączyć produkt i dzienniki modułu komunikacyjnego (wszystkie usługi zostaną automatycznie uruchomione ponownie)
- `deliverall`, aby utworzyć:
  - Archiwum zawierające logi produktu i modułu komunikacyjnego dostarczone do folderu `/tmp` w następującym formacie: `bitdefender_machineName_timeStamp.tar.gz`.

    Po utworzeniu archiwum:

    1. Zostanie wyświetlony monit, jeżeli zachcesz wyłączyć dzienniki. W razie potrzeby, usługi są automatycznie ponownie uruchamiane.
    2. Zostanie wyświetlony monit, czy chcesz usunąć dzienniki.
- `deliverall -default` dostarcza pewne informacje jak w poprzedniej opcji, lecz domyślne akcje nie będą uwzględniane w dzienniku bez potwierdzenia ze strony użytkownika (dzienniki zostają wyłączone i skasowane).

Możesz także uruchomić polecenie `/bdconfigure` bezpośrednio z pakietu BEST (pełny lub downloader) bez zainstalowanego produktu.

Aby zaraportować zdarzenie GravityZone dotyczące twojego systemu Linux, przejdź do kolejnego kroku, wykorzystując wcześniej opisane opcje:

1. Uruchom produkt oraz dziennik modułu komunikacyjnego.
2. Spróbuj odtworzyć problem.
3. Wyłącz dzienniki.
4. Utwórz archiwum dzienników.
5. Odbierz bilet mailowego wsparcia używając formularza dostępnego na stronie **Pomoc & Wsparcie** Control Center, wraz z opisem zdarzenia i załączonym archiwum dziennika.

Narzędzie Wsparcia dla Linux dostarcza następujące informacje:

- `etc`, `var/log`, `/var/crash` (jeśli dostępne) oraz foldery `var/epag` z `/opt/BitDefender`, zawierają dzienniki i ustawienia Bitdefender
- Plik `/tmpvar/log/BitDefender/bdinstall.log` zawierający informacje dotyczące instalacji
- Plik `network.txt`, zawierający ustawienia sieci / informacje połączenia maszyny
- Plik `product.txt`, zawierający zawartość wszystkich plików `update.txt` z `/opt/BitDefender/var/lib/scan` i rekursywna pełna lista wszystkich plików z `/opt/BitDefender`
- Plik `system.txt` zawiera ogólne informacje systemowe (dystrybucja, wersja jądra, dostępna pamięć RAM, wolna przestrzeń dyskowa)
- Plik `users.txt`, zawierający informacje o użytkowniku
- Pozostałe informacje dotyczące produktu związane z systemem, takie jak zewnętrzne połączenia procesów i wykorzystanie procesora
- Logi systemowe

16.3.3. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Mac

Składając zapytanie do Zespołu Wsparcia Technicznego Bitdefender należy podać następujące informacje:

- Szczegółowy opis problemu, który napotkałeś.
- Zrzut ekranu (jeśli dotyczy) dokładnego błędu wiadomości, która się pojawi.
- Log Narzędzia Wsparcia.

Aby zebrać informacje o systemie Mac przy użyciu Narzędzia Wsparcia:

1. Pobierz archiwum ZIP zawierające narzędzie pomocy technicznej.
2. Weź plik **BDProfiler.tool** z archiwum.
3. Otwórz okno Terminala.
4. Przejdź do lokalizacji pliku **BDProfiler.tool**.
   Na przykład:

```
cd /Users/Bitdefender/Desktop;
```

5. Dodaj uprawnienia do wykonywania do pliku:

```
chmod +x BDProfiler.tool;
```

6. Uruchom narzędzie.

   Na przykład:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Naciśnij `Y` i wprowadź hasło, gdy zostaniesz poproszony o podanie hasła administratora.

   Poczekaj kilka minut, aż narzędzie zakończy generowanie logu. Znajdziesz plik archiwum wyników (**Bitdefenderprofile_output.zip**) na pulpicie.

16.4. Informacje o produkcie

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 18 lat Bitdefender uzyskał niekwestionowaną reputację dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiekolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

16.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com
Centrum pomocy:http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne
Dokumentacja: gravityzone-docs@bitdefender.com
Lokalni Dystrybutorzy:http://www.bitdefender.com/partners
Program partnerski: partners@bitdefender.com
Rzecznik prasowy: pr@bitdefender.com
Wysyłanie Próbek Wirusów: virus_submission@bitdefender.com
Wysyłanie Próbek Spamu: spam_submission@bitdefender.com
Raportowanie Abuse: abuse@bitdefender.com

Strona: http://www.bitdefender.com

16.4.2. Lokalni Dystrybutorzy

Lokalni dystrybutorzy Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych.

Wyszukiwanie dystrybutora Bitdefender w danym kraju:

1. Odwiedź http://www.bitdefender.com/partners.
2. Przejdź do **Lokalizator Partnera**.
3. Informacje kontaktowe lokalnych dystrybutorów Bitdefender powinny wyświetlić się automatycznie. Jeśli to się nie stanie, wybierz kraj, w którym mieszkasz, aby wyświetlić te informacje.
4. Jeśli w swoim kraju nie możesz znaleźć dystrybutora Bitdefender, skontaktuj się z nami, wysyłając e-mail na adres enterprisesales@bitdefender.com.

16.4.3. Biura Bitdefender

Biura Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych. Ich adresy oraz dane kontaktowe są wypisane poniżej.

Stany Zjednoczone

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (sprzedaż&pomoc techniczna): 1-954-776-6262
Sprzedaż: sales@bitdefender.com
Internet: http://www.bitdefender.com
Centrum pomocy: http://www.bitdefender.com/support/business.html

Francja

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Faks: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73

Adres e-mail: b2b@bitdefender.fr
Strona internetowa: http://www.bitdefender.fr
Centrum pomocy: http://www.bitdefender.fr/support/business.html

Hiszpania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Faks: (+34) 93 217 91 28
Telefon (biuro i sprzedaż): (+34) 93 218 96 15
Telefon (pomoc techniczna): (+34) 93 502 69 10
Sprzedaż: comercial@bitdefender.es
Strona internetowa: http://www.bitdefender.es
Centrum pomocy: http://www.bitdefender.es/support/business.html

Niemcy

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (biuro i sprzedaż): +49 (0) 2304 94 51 60
Telefon (pomoc techniczna): +49 (0) 2304 99 93 004
Sprzedaż: firmenkunden@bitdefender.de
Strona internetowa: http://www.bitdefender.de
Centrum pomocy: http://www.bitdefender.de/support/business.html

Anglia i Irlandia

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (sprzedaż&pomoc techniczna): (+44) 203 695 3415
Adres e-mail: info@bitdefender.co.uk
Sprzedaż: sales@bitdefender.co.uk
Strona internetowa: http://www.bitdefender.co.uk

Centrum pomocy: http://www.bitdefender.co.uk/support/business.html

Rumunia

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Faks: +40 21 2641799
Telefon (sprzedaż&pomoc techniczna): +40 21 2063470
Sprzedaż: sales@bitdefender.ro
Strona internetowa: http://www.bitdefender.ro
Centrum pomocy: http://www.bitdefender.ro/support/business.html

Zjednoczone Emiraty Arabskie

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (sprzedaż&pomoc techniczna): 00971-4-4588935 / 00971-4-4589186
Faks: 00971-4-44565047
Sprzedaż: sales@bitdefender.com
Internet: http://www.bitdefender.com
Centrum pomocy: http://www.bitdefender.com/support/business.html

A. Aneksy

A.1. Wspierane Typy Plików

Antymalwarowe silniki skanowania załączone w rozwiązaniu ochrony Bitdefender mogą skanować wszystkie typy plików, które mogą zawierać zagrożenia. Lista poniżej zawiera najbardziej pospolite typy plików, które są analizowane.

{*; 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 obiektów sieciowych i statusy

A.2.1. Typy obiektów sieci

Każdy typ obiektu dostępny w stronie **Sieć** jest reprezentowany jako swoista ikona. Znajdź w tabeli tak zwaną ikonę i opis dla wszystkich dostępnych typów obiektów.

Ikona	Typ
	Grupa Sieci
	Komputer
	Komputer Relay
	Komputer Serwera Exchange
	Komputer Relay Serwera Exchange
	Maszyna wirtualna
	Wirtualna maszyna Relay
	Złoty obraz
	Maszyna Wirtualna Serwera Exchange
	Maszyna wirtualna Relay Exchange Server
	Maszyna Wirtualna z vShield
	Maszyna Wirtualna Relay z vShield
	Nutanix Inventory
	Nutanix Prism
	Klaster Nutanix
	VMware inventory
	VMware vCenter
	Centrum danych VMware
	Pula zasobów VMware
	Klaster VMware

Ikona	Typ
	Citrix Inventory
	XenServer
	Xen Pool
	Inwentarz Amazon EC2
	Integracja Amazon EC2
	Region Amazon EC2 / Microsoft Azure
	Strefa Dostępności Amazon EC2 / Microsoft Azure
	Microsoft Azure inventory
	Integracja Microsoft Azure
	Security Server
	Security Server z vShield
	Host bez Security Server
	Hostowany przez Security Server
	VMware vApp
	Użytkownik Urządzenia Mobilnego
	Urządzenie Mobilne

A.2.2. Statusy Obiektów Sieciowych

Każdy obiekt sieciowy może posiadać odrębny status w zależności od indywidualnego stanu zarządzania, kwestii bezpieczeństwa, łączności i podobnych. W następnej tabeli znajdziesz wszystkie dostępne statusy ikon i ich opisy.

Notatka
Tabelka poniżej zawiera kilka ogólnych przykładów statusu. Stosowane mogą być te same typy, pojedyncze lub łączone, do wszystkich typów obiektów sieciowych takich jak grupy, komputery itp.

Ikona	Stan
	Host bez Serwera Bezpieczeństwa, Odłączony
	Maszyna Wirtualna, Offline, Niezarządzana

Ikona	Stan
	Maszyna Wirtualna, Online, Niezarządzana
	Maszyna Wirtualna, Online, Zarządzana
	Maszyna Wirtualna, Online, Zarządzana, Z Problemami
	Maszyna wirtualna w oczekiwaniu na ponowne uruchomienie
	Maszyna Wirtualna, Zawieszona
	Maszyna Wirtualna, Usunięta

A.3. Typy Pliku Aplikacji

Silnik zwalczający złośliwe oprogramowanie dołączony do programu Bitdefender można skonfigurować tak, aby skanował jedynie pliki aplikacji (lub programów). Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików.

Ta kategoria zawiera pliki o następujących rozszerzeniach:

```
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 plików filtrowania załączników

Moduł Kontroli zawartości dostępny w Security for Exchange umożliwia filtrowanie załączników e-maili na podstawie typu pliku. Typy dostępne w Control Center zawierają następujące rozszerzenia plików:

Pliki wykonywalne

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Obrazy

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

Multimedia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archiwa

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

Arkusze kalkulacyjne

fm3; ods; wk1; wk3; wks; xls; xlsx

Prezentacje

odp; pps; ppt; pptx

Dokumenty

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Zmienne systemowe

Niektóre z ustawień dostępnych w konsoli wymagają podania ścieżki na komputerach docelowych. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.

Oto lista predefiniowanych zmiennych systemowych:

`%ALLUSERSPROFILE%`
Folder profil wszystkich użytkowników. Typowa ścieżka:

```
C:\Documents and Settings\All Users
```

`%APPDATA%`
folder danych aplikacji zalogowanego użytkownika. Typowa ścieżka:

```
C:\Users\{username}\AppData\Roaming
```

`%LOCALAPPDATA%`
Tymczasowe pliki Aplikacji. Typowa ścieżka:

```
C:\Users\{username}\AppData\Local
```

`%PROGRAMFILES%`
Folder Program Files. Typowa ścieżka to `C:\Program Files`.

`%PROGRAMFILES(X86)%`
Folder Program Files dla 32-bitowej aplikacji (w 64-bitowym systemie). Typowa ścieżka:

```
C:\Program Files (x86)
```

`%COMMONPROGRAMFILES%`
Folder Common Files. Typowa ścieżka:

```
C:\Program Files\Common Files
```

`%COMMONPROGRAMFILES(X86)%`
Folder Common Files dla 32-bitowej aplikacji (w 64-bitowym systemie). Typowa ścieżka:

```
C:\Program Files (x86)\Common Files
```

`%WINDIR%`
Katalog Windows lub SYSROOT. Standardowa ścieżka to `C:\Windows`.

`%USERPROFILE%`
Ścieżka do folderu profilu użytkownika. Typowa ścieżka:

```
C:\Users\{username}
```

Na macOS folder profilu użytkownika odpowiada folderowi domowemu. Użyj `$HOME` lub ~ podczas konfiguracji wykluczeń.

A.6. Narzędzia Kontroli Aplikacji

Aby ustawić reguły Kontroli Aplikacji na podstawie Hasha pliku wykonywalnego lub thumbprinta certyfikatu, musisz pobrać następujące narzędzia:

- **Fingerprint**, aby uzyskać niestandardową wartość HASHa.
- **Thumbprint**, aby uzyskać niestandardową wartość thumbprinta certyfikatu.

Fingerprint

Kliknij Tutaj aby pobrać plik wykonywalny Fingerprinta, lub idź do http://download.bitdefender.com/business/tools/ApplicationControl/

Aby uzyskać hash aplikacji:

1. Otwórz okno **Wiersz polecenia**.
2. Przejdź do lokalizacji narzędzia Fingerprint. Na przykład:

   ```
   cd/users/fingerprint.exe
   ```

3. Aby wyświetlić wartość Hasha aplikacji, uruchom następującą komendę:

   ```
   fingerprint <application_full_path>
   ```

4. Wróć do Control Center i konfiguruj regułę opartą na otrzymanej wartości. Aby uzyskać więcej informacji odwołaj się do „Kontrola Aplikacji” (p. 338).

Thumbprint

Kliknij Tutaj aby pobrać plik wykonywalny Thumbprinta, lub idź do http://download.bitdefender.com/business/tools/ApplicationControl/

Aby zdobyć certyfikat thumbprinta:

1. Uruchom **Wiersz poleceń** jako administrator.
2. Przejdź do lokalizacji narzędzia Thumbprint. Na przykład:

   ```
   cd/users/thumbprint.exe
   ```

3. Aby wyświetlić thumbprint certyfikatu, uruchom następujące komendy:

```
thumbprint <application_full_path>
```

4. Wróć do Control Center i konfiguruj regułę opartą na otrzymanej wartości. Aby uzyskać więcej informacji odwołaj się do „Kontrola Aplikacji” (p. 338).

A.7. Obiekty Sandbox Analyzer

A.7.1. Obsługiwane Typy Plików i Rozszerzenia do Wysyłania Ręcznego

Obsługiwane są następujące rozszerzenia plików i można je ręcznie zdetonować w Sandbox Analyzer:

`Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.`

Sandbox Analyzer jest w stanie wykryć wyżej wymienione typy plików, także jeśli są one zawarte w archiwach następujących typów: `7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, skompresowane archiwum LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ .`

A.7.2. Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania

Wstępne filtrowanie zawartości określi konkretny typ pliku za pomocą kombinacji, która implikuje treść i rozszerzenie obiektu. Oznacza to, że plik wykonywalny z rozszerzeniem `.tmp` zostanie rozpoznany jako aplikacja i jeśli okaże się podejrzany, zostanie wysłany do Sandbox Analyzer.

- Aplikacje - pliki o formacie PE32, w tym między innymi następujące rozszerzenia: `exe, dll, com .`

- Dokumenty - pliki o formacie dokumentu, w tym między innymi następujące rozszerzenia: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm , Dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf .`
- Skrypty: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.`
- Archiwa: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.`
- E-maile (zapisane w systemie plików): `eml, tnef .`

A.7.3. Domyślne Wykluczenia przy Automatycznym Wysyłaniu

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.`

A.7.4. Zalecane Aplikacje dla Detonacyjnych VM

Sandbox Analyzer On-Premises wymaga pewnych aplikacji, aby były zainstalowane na detonacyjnych maszynach wirtualnych, aby mogły otwierać przesłane próbki.

Aplikacje	Typy plików
Pakiet Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Domyślny system 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

Aplikacje	Typy plików
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Procesory Danych

Nazwa	Szczegóły
Przekazujący Żądanie Procesora	Przekazuje zapytania procesora w rozproszonych środowiskach
VMware Hypervision Integrator	Synchronizuje VMware inverntory i inne informacje z GravityZone
Citrix Hypervisor Integrator	Synhronizuje Xen inventory i inne informacje z GravityZone
Integrator Ogólnej Wirtualizacji	Synchronizuje Nutanix, Amazon EC2 i Azure inventory z GravityZone
Integrator NTSA	Synchronizuje status integracji Network Traffic Security Analytics (NTSA) i wysyła aktualizacje licencji do urządzenia NTSA
Synchronizator zasobów komputera w Active Directory	Synchronizuje inwentarz komputerów Active Directory z GravityZone
Synchronizator zasobów grup Active Directory	Synchronizuje inwentarz grup Active Directory z GravityZone
Synchronizator Importu Użytkowników Active Directory	Synchronizuje konta Active Directory z GravityZone (wykorzystywane do linkowania kont AD z kontami GravityZone)
Synchronizator listy użytkowników Active Directory	Synchronizuje inwentarz użytkowników Active Directory z GravityZone
Procesor Email	Kolejkuje emaile do wysłania z GravityZone
Procesor Raportów	Przetwarza raporty i portlety
Wdrożyciel Windows Security Agent	Wdraża agent bezpieczeństwa Bitdefender na urządzenia z Windows

Nazwa	Szczegóły
Wdrożyciel Serwera Bezpieczeństwa	Wdraża Wirtualne Urządzenia Ochrony
Menedżer Licencji	Zarządza licencjami zainstalowanych punktów końcowych
Procesor Powiadomień Mobile Push	Wysyła powiadomienia push do chronionych urządzeń mobilnych
Wdrożyciel Linux i macOS Security Agent	Wdraża agenta Bitdefender GravityZone Enterprise Security for Virtualized Environments (SVE) na urządzeniach z Linux i macOS
Zestawy Punktów Końcowych i narzędzie do aktualizacji produktu	Pobiera i publikuje pakiety i aktualizacje produktu Bitdefender
Aktualizator GravityZone	Automatycznie aktualizuje GravityZone gdy skonfigurowany. Aktualizuje wersję Wirtualnych Urządzeń GravityZone
Czyszczenie Pakietu	Czyści nieużywane paczki plików
Procesor Problemów Związanych z Bezpieczeństwem	Przetwarza problemy z bezpieczeństwem dla obiektów w sekcji Sieć
Procesor Kopii Zapasowej	Przeprowadza kopię zapasową bazy danych GravityZone
Procesor Powiadomień	wysyła powiadomienia użytkownikom
Procesor Zdarzeń Systemowych	Obsługuje zdarzenia z infrastruktury (Kontrola Aplikacji, Analizator Sandbox, Serenity, SVA) lub integracji (Exchange, Nutanix, NSX)
Wdrożyciel Pakietu Uzupełniającego HVI	Obsługuje instalację, aktualizacje i usuwanie dodatkowych pakietów HVI dla hostów XEN
Procesor Ponownego Uruchomienia Zadania HVI	Zarządza zadaniami ponownego uruchomienia na hostach HVI
Procesor Zasilania i Statusu Online	Oblicza stan zasilania i stan łączności komputerów i maszyn wirtualnych
Procesor Czyszczenia Maszyn Offline	Usuwa wyłączone maszyny z sieci

Nazwa	Szczegóły
Menedżer Zadań w tle	Obsługuje i uruchamia zadania i procesy w tle

Słowniczek

Adware

Adware jest często łączony z aplikacją, która może być używana bezpłatnie tak długo, jak użytkownik zgadza się na adware. Ponieważ aplikacje typu adware są zazwyczaj instalowane po zaakceptowaniu przez użytkownika warunków umowy licencyjnej określającej cele aplikacji, zadanie ochrony przed takim adware nie jest wykonywane.

Jednak reklamy typu pop-up mogą być irytujące, a w niektórych wypadkach mogą obniżyć wydajność systemu. Ponadto informacje zbierane przez niektóre aplikacje tego typu mogą rodzić obawę naruszenia prywatności użytkowników, którzy nie byli w pełni świadomi warunków umowy licencyjnej.

Aktualizacja

Nowa wersja oprogramowania lub sprzętu przeznaczona do zastąpienia starszej wersji tego samego produktu. Dodatkowo standardowe procedury instalacyjne dla aktualizacji często sprawdzają, czy na komputerze zainstalowana jest starsza wersja produktu. Jeśli nie, nie możesz zainstalować aktualizacji.

Bitdefender posiada własny moduł uaktualnienia, który pozwala tobie manualnie wprowadzać uaktualnienia lub przeprowadzać to automatycznie.

Antimalware Scanning Storm

Intensywne korzystanie z zasobów systemowych, które występuje, gdy oprogramowanie antywirusowe jednocześnie skanuje wielu maszyn wirtualnych na jednym fizycznym hoście.

Archiwum

Dysk, taśma, lub katalog, który zawiera pliki kopii zapasowej.

Plik, który zawiera jeden lub więcej plików w skompresowanym formacie.

Ataki celowe

Cyber-ataki, które koncentrują się głównie na korzyściach finansowych lub osłabieniu reputacji. Celem może być osoba, firma, oprogramowanie lub system. Ataki te są przeprowadzane etapami, przez długi okres czasu, przy użyciu jednego lub więcej punktów infiltracji. Są prawie niewidoczne. Dostrzega się najczęściej, gdy szkoda została już dokonana.

Backdoor

Luka w obszarze bezpieczeństwa systemu celowo pozostawiona przez projektantów lub administratorów systemu. Luki nie zawsze są pozostawione w złej wierze. Niektóre systemy operacyjne są dostarczane z kontami uprzywilejowanymi przeznaczonymi do użytku przez serwis techniczny lub opiekunów ds. programowania po stronie sprzedawcy.

Bootkit

Bootkit to złośliwy program mający zdolność zarażania głównego rekordu ładującego (MBR), rekordu rozruchowego woluminu (VBR) lub sektora rozruchowego. Bootkit pozostaje aktywny nawet po ponownym uruchomieniu systemu.

Ciasteczka

W przemyśle internetowym ciasteczka (ang. cookies) są określane jako małe pliki zawierające informacje o poszczególnych komputerach, które mogą być analizowane i wykorzystywane przez reklamodawców, aby śledzić online Twoje zainteresowania i gusta. W tej dziedzinie technologia związana z plikami cookie nadal się rozwija, a celem tego jest profilowanie reklam tak, aby były bezpośrednio związane z Twoimi zainteresowaniami. Z jednej strony dla wielu ludzi stanowi to obosieczny miecz: jest efektywne i trwałe, gdyż wyświetlane są tylko reklamy na interesujący Cię temat. Z drugiej strony śledzi każdy Twój ruch oraz kliknięcie. Dlatego są one tematem publicznej dyskusji w kwestii prywatności. Wiele osób czuje się obrażonymi z powodu bycia obserwowanymi jako "Numer SKU" (kod kreskowy na opakowaniu, który jest skanowany przez sklepy przy zakupach). Mimo że ten ten punkt widzenia może się wydawać ekstremalny, w niektórych przypadkach ma swoje uzasadnienie.

Exploit

Exploit to generalne metoda do uzyskania nieautoryzowanego dostępu do komputera poprzez lukę w ochronie systemu i pozostawia system podatny na atak.

Fałszywy alarm

Pojawia się, kiedy skaner identyfikuje plik jako zainfekowany, gdy w rzeczywistości nie jest zainfekowany.

Grayware

Klasa aplikacji oprogramowania pomiędzy legalnym a złośliwym oprogramowaniem. Chociaż nie są tak szkodliwe jak złośliwe oprogramowanie, które wpływa na integralność systemu, ich zachowanie jest niepokojące i prowadzi do niepożądanych sytuacji, takich jak kradzieże danych i nieautoryzowane użycie, niepożądane reklamy. Najbardziej popularne aplikacje grayware to spyware i adware.

Heurystyczny

Oparta na regułach metoda rozpoznawania nowych wirusów. Ta metoda skanowania nie polega na określonych sygnaturach wirusów. Zaletą skanowania heurystycznego jest to, że nie jest ono podatne na zmylenie przez nowy wariant znanych wirusów. Jednakże może czasami zgłaszać wykrycie podejrzanego kodu w normalnych programach generując tzw. "fałszywe alarmy".

IP

Protokół internetowy – protokół routingu w protokole TCP/IP który jest odpowiedzialny za adresowanie IP, fragmentację oraz ponowne składanie pakietów IP.

Keylogger

Keyloggery to aplikacje, które zapisują wszystkie naciśnięcia klawiszy.

Keyloggery nie są szkodliwe z założenia. Można ich używać dla celów zgodnych z prawem, np. po to, żeby legalnie monitorować aktywność pracowników lub dzieci. Jednak cyberprzestępcy coraz częściej używają ich w celu wyrządzenia szkody (np. do zbierania prywatnych danych, takich jak dane do logowania lub numer ubezpieczenia społecznego).

Makrowirus

Typ wirusa komputerowego, który jest zakodowany jako makro w danym dokumencie. Wiele aplikacji jak np. Microsoft Word i Excel wspiera makra.

Aplikacje te pozwalają Ci umiejscowić makro w dokumencie i wykonywać je za każdym razem, kiedy dokument jest otwierany.

Nieheurystyczny

Ta metoda skanowania opiera się na określonych sygnaturach wirusów. Zaletą skanowania nieheurystycznego jest to, że nie jest ono podatne na wprowadzanie w błąd przez obiekty wydające się być wirusem, a także nie generuje fałszywych alarmów.

Oprogramowanie szpiegujące (spyware)

Każde oprogramowanie, które zbiera dane o użytkowniku podczas połączenia z internetem bez jego wiedzy, zazwyczaj w celach reklamowych. Aplikacje spyware występują zazwyczaj jako ukryte komponenty programów freeware albo shareware, które mogą być pobrane z internetu. Jednakże należy pamiętać że większość aplikacji shareware oraz freeware nie ma w sobie żadnego spyware. Po zainstalowaniu, spyware monitoruje aktywność użytkownika w internecie i przesyła informacje w tle do kogoś innego. Spyware może także zbierać informacje o adresach e-mail, a nawet hasła i numery kart kredytowych.

Spyware jest prostym programem podobnym do konia trojańskiego, którego użytkownicy instalują nieświadomie podczas instalacji innego programu. Pospolitym sposobem by zostać ofiarą spyware jest pobranie niektórych z obecnie dostępnych programów współdzielonych w sieciach typu peer-to-peer.

Abstrahując od kwestii etyki i prywatności, spyware okrada użytkownika używając pamięci komputera i także zużywając przepustowość łącza internetowego podczas wysyłania informacji z powrotem do swojej bazy drogą internetową. Ponieważ spyware zużywa pamięć i zasoby systemowe, aplikacje pracujące w tle mogą powodować zawieszenie się systemu lub jego ogólną niestabilność.

Phishing

Wysyłanie wiadomości e-mail do użytkownika przez osobę podającą się za przedstawiciela uprawnionego do tego przedsiębiorstwa, będące próba skłonienia użytkownika do podania informacji poufnych, wykorzystywanych w akcie kradzieży tożsamości. E-mail przekierowuje użytkownika na stronę internetową gdzie jest on proszony o zaktualizowanie informacji osobistych np. haseł, informacji dotyczących kart kredytowych, ubezpieczenia socjalnego i nr konta bankowego, które uprawniona organizacja już posiada. Strona internetowa jest fałszywa i umieszczona w internecie tylko po to, żeby wykraść informacje o użytkowniku.

Plik raportu

Plik, który zapisuje zaistniałe akcje. Bitdefender utrzymuje plik raportu udostępniając skanowaną ścieżkę dostępu, foldery, ilość archiwów i skanowanych plików, ilość zainfekowanych i podejrzanych plików jakie zostały znalezione.

Podejrzane pliki i ruch w sieci

Podejrzane pliki to te, które mają wątpliwą reputację. Ten ranking opiera się na wielu kryteriach, między innymi: istnienie podpisu cyfrowego, liczba wystąpień w sieci, użyta paczka itd. Ruch sieciowy jest uważany za podejrzany, gdy odbiega od wzorca. Na przykład niewiarygodne źródło, żądania połączenia z nietypowymi portami, zwiększone wykorzystanie przepustowości, przypadkowy czas połączeń itp.

Port

Interfejs komputera, do którego podłączasz urządzenie. Komputery osobiste mają różne rodzaje portów. Wewnątrz znajduje się kilka portów dla połączeń dyskowych, podłączania monitorów i klawiatur. Na zewnątrz komputery osobiste mają porty dla połączeń modemowych, drukarek, myszy i innych urządzeń peryferyjnych.

Natomiast w sieciach TCP/IP i UDP jest to punkt końcowy połączenia logicznego. Numer portu pokazuje, jakiego typu jest dany port. Np. port 80 jest używany dla ruchu HTTP.

Przeglądarka

Aplikacja używana do lokalizowania i wyświetlania stron internetowych.

Ransomware

Złośliwe oprogramowanie, które blokuje Ci komputer lub blokuje dostęp do plików i aplikacji. Ransomware będzie żądał, że zapłacisz określoną sumę(opłata ransomware) w zamian za klucz deszyfrujący, który pozwoli odzyskać dostęp do komputera i plików.

Robak

Program, który propaguje się przez sieć mnożąc się w czasie poruszania. Nie może się podłączyć do innych programów.

Rootkit

Rootkit jest zestawem narzędzi programowych, który daje dostęp do systemu na poziomie administratora. Termin ten był początkowo używany dla systemów operacyjnych UNIX w odniesieniu do zrekompilowanych narzędzi, które udostępniały intruzom prawa administracyjne, pozwalając im ukryć ich obecność, żeby nie byli widoczni dla administratorów systemu.

Głównym zadaniem rootkitów jest ukrywanie procesów, plików, zdarzeń logowania i raportów. Mogą również przechwytywać dane z terminali, połączeń

sieciowych lub urządzeń peryferyjnych, jeśli zawierają odpowiedni rodzaj oprogramowania.

Rootkity nie są zagrożeniem z założenia. Na przykład systemy, a nawet niektóre aplikacje ukrywają krytyczne pliki używając właśnie rootkitów. Jednak często są one używane do ukrywania złośliwego oprogramowania lub intruza w systemie. Gdy są połączone z wirusami, są wielkim zagrożeniem dla spójności działania i bezpieczeństwa systemu. Mogą monitorować ruch, tworzyć backdoory w systemie, zmieniać pliki i logi oraz unikać wykrycia.

Rozszerzenie pliku

Część nazwy pliku, która wskazuje na rodzaj danych przechowywanych w pliku.

Wiele systemów operacyjnych, np. Unix, VMS, i MS-DOS, używa rozszerzeń nazwy pliku. Zwykle składają się z jednego do trzech znaków (niektóre stare systemy operacyjne akceptują nie więcej niż trzy). Przykłady obejmują "c" jako kod źródłowy C, "ps" jako PostScript, "txt" jako tekst.

Sektor startowy:

Sektor na początku każdego dysku, który rozpoznaje budowę dysku (rozmiar sektora, rozmiar klastra itd.). Sektor rozruchowy zawiera również program uruchamiający system operacyjny.

Skrypt

Inna nazwa dla makra lub pliku wsadowego to skrypt. Skrypt jest listą komend, które mogą być wykonywane bez udziału użytkownika.

Spam

Elektroniczne śmieci lub komentarze grup dyskusyjnych. Ogólnie znane jako niechciane wiadomości e-mail.

sygnatura malware

Sygnatury złośliwego oprogramowania to urywki kodu wypakowane z rzeczywistych próbek tego oprogramowania. Są one używane przez programy antywirusowe do dopasowywania wzorców i wykrywania złośliwego oprogramowania. Sygnatury są również użyte do usunięcia kodu malware z zainfekowanych plików.

Baza Danych Sygnatur Złośliwego Oprogramowania Bitdefender to zbiór sygnatur złośliwego oprogramowania uaktualniany co godzinę przez naukowców Bitdefender, zajmujących się złośliwym oprogramowaniem.

Szkodliwe oprogramowanie

Malware to ogólne określenie oprogramowania, które zostało stworzone do szkodzenia za pomocą "złośliwego oprogramowania". Nie jest jeszcze w powszechnym użyciu, ale jego popularność jako główny produkt do określenia wirusów, koni trojańskich, robaków, i złośliwych kodów mobilnych rośnie.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol - Protokół Kontroli Transmisji/Protokół internetowy) – zespół protokołów sieciowych szeroko używanych w internecie, zapewniający komunikację pomiędzy połączonymi sieciami komputerów z różną architekturą sprzętową i różnymi systemami operacyjnymi. TCP/IP zawieraja standardy dotyczące komunikacji komputerów oraz połączeń sieciowych i ruchu.

Trojan

Niszczycielski program, który ukrywa się jako niegroźna aplikacja. W przeciwieństwie do wirusów, konie trojańskie nie powielają się, ale mogą być tak samo szkodliwe. Jednym z najniebezpieczniejszych typów koni trojańskich jest program zapewniający, że pozbędzie się wirusów z Twojego komputera, a który w rzeczywistości wprowadza wirusy do komputera.

Nazwa pochodzi z powieści Homera "Iliada", w której Grecy podarowali olbrzymiego konia swoim wrogom, Trojanom, pozornie jako znak pokoju. Gdy jednak Trojanie wprowadzili konia do miasta, greccy żołnierze wymknęli się z pustego wnętrza konia i otworzyli bramy miasta pozwalając pozostałym na wejście i podbicie Troi.

Warstwy bezpieczeństwa

GravityZone zapewnia ochronę poprzez serię ról i modułów, całościowo nazywanych warstwami ochrony, które są podzielone na Endpoint Protection (EPP) lub core protection i różne dodatki. Endpoint Protection zawiera Antymalware, Zaawansowaną Kontrolę Zagrożeń, Zaawansowany Anty-Exploit, Zaporę Sieciową, Kontrolę Zawartości, Kontrolę Urządzeń, Network Attack Defense, Power User i Relay. Dodatki zawierają warstwy ochrony takie jak Security for Exchange i Sandbox Analyzer.

Po więcej informacji na temat warstw ochrony dostępnych w twoim rozwiązaniu GravityZone odnieś się do „GravityZone Warstwy Ochronne” (p. 2).

Wiersz poleceń
W interfejsie linii poleceń użytkownik wpisuje polecenia w przestrzeni znajdującej się na ekranie, używając języka poleceń.

Windows Downloader
Jest to ogólna nazwa programu mającego podstawową funkcję pobierania zawartości w celu niechcianego lub złego zamiaru.

Wirus
Program lub fragment kodu, który jest załadowany na Twoim komputerze bez Twojej wiedzy i uruchamia się wbrew Twojej woli. Większość wirusów może się również replikować. Wszystkie wirusy komputerowe są tworzone przez człowieka. Prosty wirus, który umie się skopiować kilka razy jest stosunkowo łatwy do utworzenia. Nawet tak prosty wirus jest niebezpieczny, ponieważ szybko wykorzysta całą dostępną pamięć i przyczyni się do zatrzymania pracy systemu. Bardziej niebezpiecznym typem wirusa jest ten, który jest zdolny przenosić się przez sieci i łamać systemy bezpieczeństwa.

Wirus polimorficzny
Wirus, który zmienia swoją formę za każdym razem, kiedy zainfekuje kolejny plik. Ponieważ nie mają one stałego wzoru binarnego, są trudne do rozpoznania.

Wirus sektora rozruchowego
Wirus, który infekuje boot sektor dysku stałego lub stację dyskietek. Próba uruchomienia systemu z dyskietki zainfekowanej wirusem tego typu spowoduje, że wirus uaktywni się w pamięci. Od tego momentu za każdym razem, kiedy będziesz uruchamiał system, wirus będzie aktywny w pamięci.

Zasobnik systemowy
Wprowadzony w systemie Windows 95 zasobnik systemowy znajduje się na pasku zadań Windows (zwykle u dołu obok zegara) i zawiera miniaturowe ikony zapewniające łatwy dostęp do funkcji systemowych, takich jak faks, drukarka, modem, głośność i nie tylko. Aby wyświetlić informacje szczegółowe i sterowniki, kliknij dwukrotnie ikonę lub kliknij ją prawym przyciskiem myszy.

Zdarzenia
Działanie lub wydarzenie wykryte przez program. Zdarzenia mogą być czynnościami użytkownika takimi jak: kliknięcie myszą lub naciśnięcie klawisza albo zdarzeniami systemowymi takimi, jak kończenie się pamięci.

Złodziej haseł

Złodziej haseł zbiera fragmenty danych, które mogą być nazwami kont i przypisanymi do nich hasłami. Te skradzione dane są następnie wykorzystywane do złych celów, takich jak przejęcia kont.