

The background of the advertisement is a dark, futuristic digital space. It features glowing blue and cyan light trails, circular patterns, and a central bright light source that creates a lens flare effect. The overall aesthetic is high-tech and cybernetic.

Bitdefender®

GravityZone

PRZEWODNIK ADMINISTRATORA

Bitdefender GravityZone Przewodnik administratora

Data publikacji 2021.04.20

Copyright© 2021 Bitdefender

Notka prawna

Wszelkie prawa zastrzeżone. Żadna część tej publikacji nie może być kopiowana w żadnej formie lub postaci elektronicznej, mechanicznej, w formie fotokopii lub w postaci nagrań głosowych, ani przechowywana w jakimkolwiek systemie udostępniania i wyszukiwania informacji, bez pisemnej zgody upoważnionego przedstawiciela firmy Bitdefender. Umieszczenie krótkich cytatów w recenzjach może być dopuszczalne tylko z powołaniem się na cytowane źródło. Zawartość nie może być w żaden sposób modyfikowana.

Ostrzeżenie i zrzeczenie się odpowiedzialności. Ten produkt i jego dokumentacja są chronione prawami autorskimi. Informacja w tym dokumencie została dostarczona w stanie „w jakim jest” i bez żadnych dodatkowych gwarancji. Dołożyliśmy wszelkich starań w przygotowanie tego dokumentu, jednak autorzy nie ponoszą żadnej odpowiedzialności w stosunku do żadnych osób lub jednostek, w przypadku szkód lub strat spowodowanych lub stwierdzenia, że wynikły one bezpośrednio lub pośrednio z powodu informacji zawartych w tej pracy.

Dokument zawiera odnośniki do stron internetowych, które nie są pod kontrolą firmy Bitdefender. Firma Bitdefender nie odpowiada za zawartość serwisów zewnętrznych. Jeśli odwiedzasz zewnętrzną stronę internetową, wymienioną w tej instrukcji - robisz to na własne ryzyko. Firma Bitdefender umieszcza te odnośniki tylko dla wygody użytkownika, a umieszczenie takiego odnośnika nie pociąga za sobą żadnej odpowiedzialności firmy Bitdefender za zawartość zewnętrznych stron internetowych.

Znaki handlowe. W tym dokumencie mogą występować nazwy i znaki handlowe. Wszystkie zarejestrowane i niezarejestrowane znaki handlowe w tym dokumencie są własnością ich poszczególnych właścicieli, i tak powinny być traktowane.

Spis treści

Wstęp	vii
1. Znaki umowne stosowane w przewodniku	vii
1. O GravityZone	1
2. GravityZone Warstwy Ochronne	2
2.1. Antymalware	2
2.2. Zaawansowana Kontrola Zagrożeń	3
2.3. Zaawansowany Anty-Exploit	4
2.4. Zapora Sieciowa	4
2.5. Kontrola Zawartości	4
2.6. Network Attack Defense	4
2.7. Zarządzanie Aktualizacjami	5
2.8. Kontrola Urządzenia	5
2.9. Pełne szyfrowanie dysku	5
2.10. Sandbox Analyzer	6
2.11. Network Traffic Security Analytics (NTSA)	6
2.12. GravityZone Dostępność Warstw Ochrony	6
3. Architektura GravityZone	7
3.1. GravityZone VA	7
3.1.1. Baza danych GravityZone	7
3.1.2. Serwer Aktualizacji GravityZone	8
3.1.3. Serwer Komunikacji GravityZone	8
3.1.4. Konsola Web (GravityZone Control Center)	8
3.2. Agenci Bezpieczeństwa	8
3.2.1. Bitdefender Endpoint Security Tools	8
3.2.2. Endpoint Security for Mac	11
3.3. Architektura Sandbox Analyzer	11
4. Pierwsze kroki	13
4.1. Łączenie z Control Center	13
4.2. Control Center w skrócie	14
4.2.1. Control Center Przegląd	14
4.2.2. Tabela Danych	16
4.2.3. Paski narzędzi działań	17
4.2.4. Menu Kontekstowe	17
4.2.5. Selektor Widoku	18
4.3. Zarządzanie kontem	19
4.4. Zmiana hasła logowania	21
5. Konta użytkownika	23
5.1. Role użytkownika	24
5.2. Prawa użytkownika	25
5.3. Zarządzanie kontami użytkownika	26
5.3.1. Indywidualne Zarządzanie Kontami Użytkowników	26
5.3.2. Zarządzanie Wieloma Kontami Użytkownika	29

5.4. Resetowanie haseł logowania	33
5.5. Zarządzanie Uwierzytelnieniem Dwuskładnikowym	34
6. Zarządzania Obiektami Sieci	36
6.1. Praca z widokami sieci	38
6.1.1. Komputery i Maszyny Wirtualne	38
6.1.2. Maszyny wirtualne	39
6.2. Komputery	40
6.2.1. Sprawdzanie Statusu Komputerów	40
6.2.2. Przeglądanie szczegóły komputera	44
6.2.3. Organizowanie Komputerów w Grupy	57
6.2.4. Sortowanie, filtrowanie i wyszukiwanie komputerów	59
6.2.5. Uruchamianie Zadań	62
6.2.6. Tworzenie szybkich raportów	75
6.2.7. Przypisywanie polityk	75
6.2.8. Synchronizowanie z Active Directory	77
6.3. Maszyny wirtualne	77
6.3.1. Sprawdzanie Statusu Maszyn Wirtualnych	79
6.3.2. Wyświetlanie Szczegółów Maszyny Wirtualnej	82
6.3.3. Organizuj wirtualne maszyny w grupy	89
6.3.4. Sortowanie, Filtrowanie i Wyszukiwanie dla Maszyn Wirtualnych	91
6.3.5. Działanie zadań na wirtualnych maszynach	95
6.3.6. Tworzenie szybkich raportów	118
6.3.7. Przypisywanie polityk	118
6.3.8. Korzystanie z Menedżera Odzyskiwania dla Zasztyfowanych Woluminów	120
6.3.9. Czyszczenie Licencji	121
6.4. Inwentarz Aktualizacji	121
6.4.1. Przeglądanie Szczegółów Aktualizacji	122
6.4.2. Wyszukiwanie i Filtrowanie Aktualizacji	124
6.4.3. Ignorowanie Aktualizacji	125
6.4.4. Instalowanie Aktualizacji	125
6.4.5. Odinstalowywanie Aktualizacji	127
6.4.6. Tworzenie Statystyk Aktualizacji	129
6.5. Przeglądanie i zarządzanie zadaniami	130
6.5.1. Sprawdzanie statusu zadania	130
6.5.2. Przeglądanie raportów zadania	132
6.5.3. Restartowanie Zadań	132
6.5.4. Usuwanie zadań	133
6.6. Usuwanie punktów końcowych z zasobów sieci	133
6.7. Konfiguracja Ustawień Sieciowych	134
6.7.1. Ustawienia Inwentarza Sieci	135
6.7.2. Czyszczenie Maszyn Offline	135
6.8. Manager uprawnień	137
6.8.1. System Operacyjny	138
6.8.2. Wirtualne środowisko	139
6.8.3. Usuwanie Poświadczeń z Menadżera Poświadczeń	140
7. Polityki Bezpieczeństwa	141
7.1. Zarządzanie politykami	142

7.1.1. Tworzenie polityk	143
7.1.2. Przypisywanie polityk	143
7.1.3. Zmiany ustawień polityk	152
7.1.4. Zmianie nazw polityk	153
7.1.5. Usuwanie polityki	153
7.2. Polityki Komputerów i Maszyn Wirtualnych	154
7.2.1. Ogólne	154
7.2.2. Antymalware	163
7.2.3. Sandbox Analyzer	197
7.2.4. Zapora Sieciowa	201
7.2.5. Ochrona sieci	215
7.2.6. Zarządzanie Aktualizacjami	230
7.2.7. Kontrola Urządzenia	234
7.2.8. Relay	239
7.2.9. Szyfrowanie	241
8. Monitorowanie Panelu	247
8.1. Panel nawigacyjny	247
8.1.1. Odświeżanie Danych Portletów	248
8.1.2. Edytowanie ustawień portletów	248
8.1.3. Dodawanie nowego portletu	249
8.1.4. usuwanie Portletu	249
8.1.5. Zmiana Układu Portletów	249
9. Używanie raportów	250
9.1. Typy Raportu	250
9.2. Tworzenie raportów	255
9.3. Przeglądania i zarządzanie zaplanowanych raportów	258
9.3.1. Przeglądanie raportów	258
9.3.2. Edytowanie zaplanowanego raportu	259
9.3.3. Usuwanie zaplanowanych raportów	260
9.4. Podejmowanie działań związanych z raportami	261
9.5. Zapisywanie raportów	261
9.5.1. Eksportowanie raportów	262
9.5.2. Raporty pobierania	262
9.6. Raporty E-mailów	262
9.7. Drukowanie raportów	263
10. Korzystanie z Sandbox Analyzer	264
10.1. Filtrowanie Kart Zgłoszeń	264
10.2. Przeglądanie Szczegółów Analizy	266
10.3. Ponowne przesłanie próbki	267
10.4. Usuwanie Kart Zgłoszeń	269
10.5. Ręczne Wysyłanie	269
10.6. Zarządzanie infrastrukturą Sandbox Analyzer	271
10.6.1. Sprawdzanie statusu Sandbox Analyzer	271
10.6.2. Konfigurowanie Równoczesnych Detonacji	272
10.6.3. Sprawdzanie Statusu Obrazów WM	273
10.6.4. Konfigurowanie i Zarządzanie obrazami WM	273

11. Dziennik Aktywności Użytkownika	275
12. Powiadomienia	277
12.1. Rodzaje powiadomień	277
12.2. Zobacz powiadomienia	282
12.3. Usuwanie powiadomień	283
12.4. Konfiguracja ustawień powiadomień	284
13. Status Systemu	287
13.1. Status OK	287
13.2. Status Uwaga	288
13.3. Metryki	288
14. Uzyskiwanie pomocy	292
14.1. Bitdefender Wsparcie Techniczne	292
14.2. Prośba o pomoc	293
14.3. Używanie Narzędzi Pomocy	294
14.3.1. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Windows	294
14.3.2. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Linux	295
14.3.3. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Mac	297
14.4. Informacje o produkcie	298
14.4.1. Adresy Internetowe	298
14.4.2. Lokalni Dystrybutorzy	299
14.4.3. Biura Bitdefender	299
A. Aneksy	302
A.1. Wspierane Typy Plików	302
A.2. Typy obiektów sieciowych i statusy	303
A.2.1. Typy obiektów sieci	303
A.2.2. Statusy Obiektów Sieciowych	304
A.3. Typy Pliku Aplikacji	304
A.4. Zmienne systemowe	305
A.5. Obiekty Sandbox Analyzer	306
A.5.1. Obsługiwane Typy Plików i Rozszerzenia do Wysyłania Ręcznego	306
A.5.2. Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania	307
A.5.3. Domyślne Wykluczenia przy Automatycznym Wysyłaniu	307
A.5.4. Zalecane Aplikacje dla Detonacyjnych VM	308
A.6. Procesory Danych	308
Słowniczek	311

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. vii)	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 i chmurze by dostarczać usługę ochrony dla fizycznych punktów końcowych i maszyn wirtualnych opartych na prywatnej i publicznej chmurze.

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 zapewnia wielowarstwową ochronę dla punktów końcowych: antymalware wraz z monitorowaniem behawioralnym, ochronę przed zagrożeniami typu zero-day, czarną listę aplikacji i sandboxa, firewall'a, kontrolę urządzeń i zawartości.

2. GRAVITYZONE WARSTWY OCHRONNE

GravityZone udostępnia następujące warstwy ochrony:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Zaawansowany Anty-Exploit
- Zapora Sieciowa
- Kontrola Zawartości
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne szyfrowanie dysku
- Network Traffic Security Analytics (NTSA)

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 spośród 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 Lekkiemi Silnikami)**

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 podejrzone 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 podejrzone

zachowanie podnosi rating procesu. Gdy próg zostanie osiągnięty, wyzwalany jest alarm.

2.3. Zaawansowany Anty-Exploit

Zaawansowana technologia Anty-Exploit, oparta na uczeniu maszynowym, jest proaktywną technologią, która powstrzymuje ataki zerowe przeprowadzane przez nieuchwytny exploit. 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.

2.4. 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 ostrzeżeniem, gdy nowe węzły dokonują połączenia przez Wi-Fi.

2.5. 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.

2.6. 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, złodziejstwo haseł, wektory infekcji drive-by-download, boty i Trojany.

2.7. 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.

2.8. 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.).

2.9. 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.

2.10. 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. W sandboxie zastosowano obszerny zestaw technologii Bitdefender, aby wykonywać ładunki w zamkniętym środowisku wirtualnym wdrożonym lokalnie, analizować ich zachowanie i zgłaszać wszelkie subtelne zmiany systemowe, które wskazują na złośliwe zamiary.

Sandbox Analyzer wykorzystuje serię czujników do detonacji zawartości ze strumieni ruchu sieciowego, scentralizowanej kwarantanny i serwerów ICAP.

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



Notatka

Funkcjonalność tego modułu zapewnia Sandbox Analyzer On-Premises, który jest dostępny z oddzielnym kluczem licencyjnym.

2.11. Network Traffic Security Analytics (NTSA)

Bitdefender [NTSA_ LONG] ([NTSA_ SHORT]) to rozwiązanie bezpieczeństwa sieciowego, które analizuje strumień 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.

2.12. 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](#)
- [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, przekazując polityki i zadania do chronionych urządzeń końcowych oraz zdarzeniowych raportów do agentów bezpieczeństwa.

3.1.4. Konsola Web (GravityZone Control Center)

Bitdefender rozwiązania ochrony są zarządzane przez GravityZone z poziomu pojedynczego punktu zarządzania, Control Center konsoli WWW, która umożliwia nam łatwiejsze zarządzanie i dostęp całościowego stanu zabezpieczeń, globalnego poziomu zagrożenia oraz kontrolę nadrzędnego zabezpieczenia modułów chroniących wirtualne i fizyczne stanowiska oraz serwery. Zasilana przez Architekturę Gravity, Control Center jest w stanie odpowiedzieć na potrzeby nawet największych organizacji.

Control Center integruje się z zarządzaniem istniejącym systemem i systemem monitorowania, aby uczynić łatwym automatyczne zastosowanie ochrony niezarządzanym stacjom roboczym lub serwerom które pojawiły się w Microsoft Active Directory lub są po prostu wykryte w sieci.

3.2. 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](#)

3.2.1. 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).

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
- Zapora Sieciowa
- Kontrola Zawartości
- Network Attack Defense
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne szyfrowanie dysku

Role Punktów Końcowych

- Power User
- Relay
- Serwerów Buforowania Łatek

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 służą 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 rozproszonymi sieciami, agenci relay pomagają obniżyć wykorzystanie pasma, zapobiegając bezpośredniemu połączeniu chronionych punktów końcowych z urządzeniem 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.

3.2.2. 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](#)

3.3. 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.

Aby używać ten moduł z GravityZone, potrzebujesz zainstalować Sandbox Analyzer On-Premises.

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 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 sześciocyfrowy 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. 19).
4. Kliknij „Zaloguj”.

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

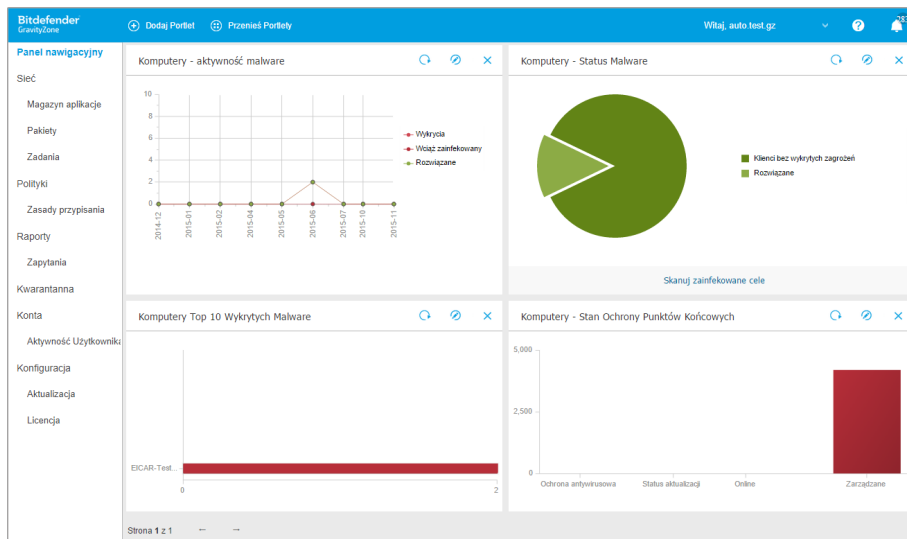


Notatka

Jeżeli zapomniałeś hasła, 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 opcję 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 umożliwi 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.

<input type="button" value="Dodaj"/> <input type="button" value="Pobierz"/> <input type="button" value="Usuń"/> <input type="button" value="Odśwież"/>			
Nazwa raportu	Typ	Powtarzalność	Pokaż raport
<input type="checkbox"/> Raport Aktywności Malware	Aktywność Malware	Tygodniowo	Raport nie został jeszcze wygenerowany

Pierwsza strona -- Strona z 1 -- Ostatnia strona

1 elementów

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 nagłówek.

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

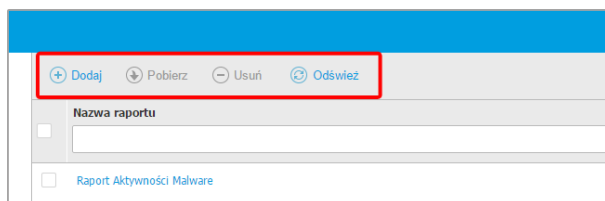
Aby upewnić się, że konsola wyświetla najnowsze informacje, naciśnij przycisk  **Odśwież** w górnej części tabeli.

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:

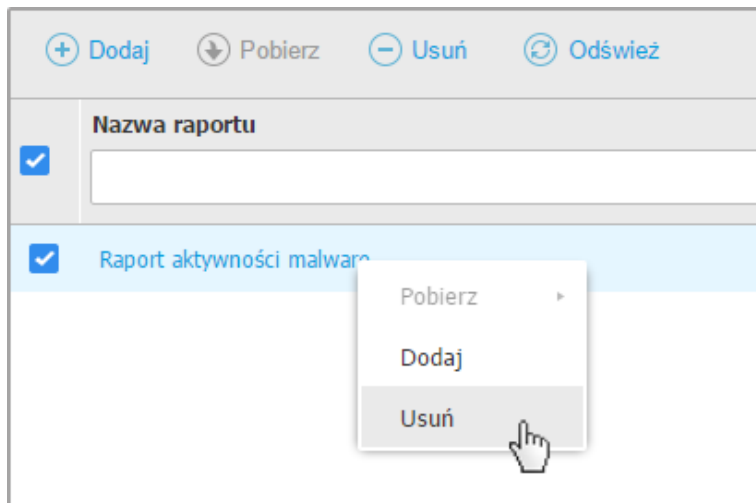
-  Stwórz nowy raport.
-  Pobierz zaplanowany raport.
-  Usuń zaplanowany raport.



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.



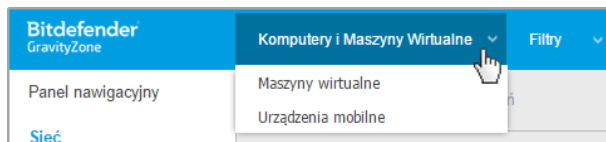
Strona Raportów - menu kontekstowe

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.

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



Przełącznik odsłony



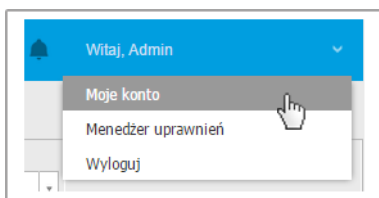
Notatka

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 wygaśnie.** 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) - kompatybilnej 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

Upewnij się, że skopiowałeś i zapisałeś tajny klucz w bezpiecznej lokalizacji. Kliknij **Wydrukuj kopię zapasową**, aby utworzyć plik PDF z

kodek 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 działania 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:

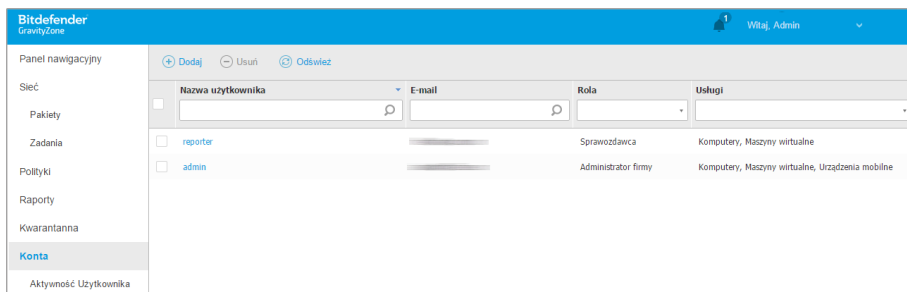
1. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moje konto**.
2. W **Szczegóły Konta**, kliknij **Zmień hasło**.
3. Wprowadź bieżące hasło i nowe hasło w odpowiednich polach.
4. Naciśnij **Zapisz** aby zastosować zmiany.

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



Nazwa użytkownika	E-mail	Rola	Usługi
<input type="checkbox"/> reporter		Sprawozdawca	Komputery, Maszyny wirtualne
<input type="checkbox"/> admin		Administrator firmy	Komputery, Maszyny wirtualne, Urządzenia mobilne

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).
- Użytkownicy usługi bezpieczeństwa GravityZone mogą zarządzać (Komputerami, Maszynami Wirtualnymi).
- 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. 25).

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). Przywileje 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 literę, 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 rolę użytkownika. Szczegółowe informacje o rolach użytkownika znajdują się w „[Role użytkownika](#)” (p. 24).
- **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. 25).
- **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 zostaną wyświetlone dla użytkowników z prawami zarządzania rozwiązaniami, domyślnie, posiadają uprawnienia w całej sieci i usługach bezpieczeństwa.

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

Control Center automatycznie wyśle 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** można 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 powiązаныmi 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 zostaną 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**.

- Wybierz regułę dostępu, którą chcesz usunąć, i kliknij **⊖ Usun**. 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.
- W razie potrzeby wybierz użytkowników, których chcesz wykluczyć. Więcej informacji można znaleźć w [Wyłączeniach Konta Użytkownika](#).
- 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:

- Zaznacz użytkowników, których chcesz wykluczyć. Lub zaznacz pole wyboru u góry tabeli, aby dodać wszystkich użytkowników do listy.
- 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:

- Zaloguj do Control Center.
- Przejdź do strony **Konta**.
- Naciśnij na nazwę użytkownika.
- Podaj nowe hasło w odpowiednim polu (w **Szczegóły**).
- 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 sześciocyfrowego 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. 19)

6. ZARZĄDZANIA OBIEKTAMI SIECI

Strona **Sieć** dostarcza kilka funkcji umożliwiających odkrywanie i zarządzanie wszystkimi komputerami i maszynami wirtualnymi dostępnymi w sieci. Sekcja **Network** składa się z dwóch paneli interfejsu wyświetlających w czasie rzeczywistym status wszystkich obiektów sieciowych:

Nazwa	System oper.	IP	Ostatnio przeglądane	Etykieta
LDC_OPTIPLEX755	Windows	10.10.14.225	Niedostępny	Niedostępny
LDC-W7-520-PC	Windows	10.10.15.22	Niedostępny	Niedostępny
MASTER	Windows NT 4.0	10.10.124.192	Niedostępny	Niedostępny
MASTER-PC	Windows 7 Professional	192.168.1.141	Online	Niedostępny
NPN-DOCL	Windows XP	169.254.199.254	Niedostępny	Niedostępny
NPN-DOCL	Microsoft Windows XP	10.0.2.15	17 Sie 2015, 12:23:43	Niedostępny
NPN-DOCL	Microsoft Windows XP	10.0.2.15	21 Lip 2015, 13:54:33	Niedostępny

Strona Sieci

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

Jednocześnie, wszystkie komputery i maszyny wirtualne 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. 133).



Notatka

Możesz przeglądać i zarządzać tylko grupami, które mają 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. 303).

- 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 paneli 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 paneli 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:

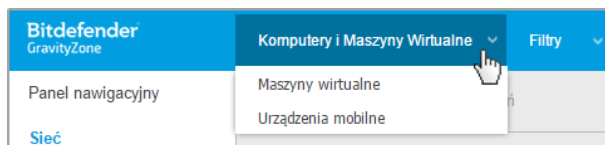
- „[Praca z widokami sieci](#)” (p. 38)
- „[Komputery](#)” (p. 40)
- „[Maszyny wirtualne](#)” (p. 77)
- „[Inwentarz Aktualizacji](#)” (p. 121)
- „[Przeglądanie i zarządzanie zadaniami](#)” (p. 130)

- „Usuwanie punktów końcowych z zasobów sieci” (p. 133)
- „Konfiguracja Ustawień Sieciowych” (p. 134)
- ???
- „Manager uprawnień” (p. 137)

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](#)

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.



WAŻNE

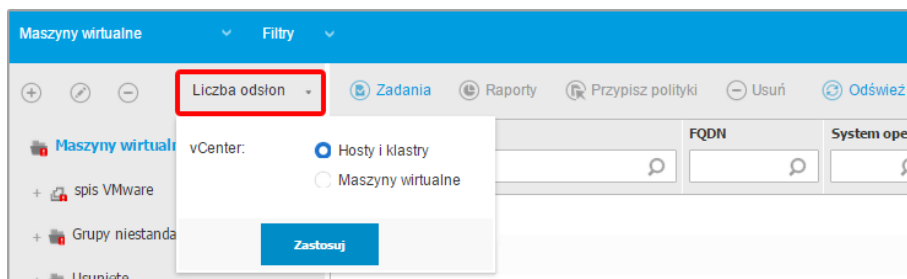
Przypisywanie zasad do maszyn wirtualnych z poziomu **Komputery i Maszyny Wirtualne** może być ograniczone przez menedżera rozwiązania GravityZone podczas konfigurowania serwera vCenter lub serwera Xen na stronie **Konfiguracji > Dostawcy Wirtualizacji**. Aby dowiedzieć się więcej, przejdź do rozdziału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

6.2. 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 [niezarządzone](#) 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. 303) 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. 133).

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 został ręcznie odinstalowany z komputera, podczas gdy ten nie posiadał łączności z GravityZone Control Center. Zwykle, gdy agent bezpieczeństwa jest ręcznie odinstalowywany z komputera, Control Center jest informowana o tym zdarzeniu a komputer oznaczany jako niezarządzany.
- 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 wygaś.
- 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 przycisk **III 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. 40).
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. 59).

- 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 przekąźnikowe:** nazwa, adres IP i etykieta przekąźnika, do którego podłączony jest punkt końcowy.

Maszyna wirtualna		Warstwy bezpieczeństwa	
Nazwa:	DOC1	Punkt końcowy:	Aktywne
FQDN:	doc1		
IP:	10.17.112.18		
System oper.:	Windows 7 Professional		
Etykieta :	<input type="text"/>		
Infrastruktura:	Komputery i Grupy		
Grupa:	Custom Groups		
Stan:	Online		
Ostatnio widziany:	Online		

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.
- 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. 43).

- Status węzłów 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. 255)

- 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 [???](#).

- 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.

Informacje
✕

Ogólne Ochrona Polityka Dzienniki

Ochrona Punktu Końcowego
Bezpieczny ✓

B Agent

Typ: BEST

Wersja produktu: 6.2.25.944

Ostatnia aktualizacja produktu: 27 Październik 2017 11:40:22

Wersja sygnatur: 7.73597

Ostatnia aktualizacja sygnatur: 27 Październik 2017 11:40:22

Podstawowy silnik skanowania: Lokalne Skanowanie

Zastępczy silnik skanowania: Brak

Przegląd

⚙️ Moduły

Antymalware:	Włączony
Zapora Sieciowa:	Wyłączony
Kontr. Zawart.:	Włączony
Użytkownik profesjonalny:	Wyłączony
Kontrola Urządzenia:	Włączony
Zaawansowana Kontrola Zagrożeń:	Włączony

Raportowanie (dzisiaj)

Status szkodliwego oprogramowania: Widok

-> Nie wykryto wirusów

Aktywność Malware: Widok

-> Brak aktywności

Zapisz
Zamknij

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.
 - **Odiedziczona:** 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.

Informacje
✕

Ogólne
Punkt końcowy
Polityka

Szczegóły

Aktywna polityka: rv

Typ: Urządzenie

Przypisanie: Bezpośrednie

Przypisane polityki

Nazwa polityki	Status	Typ	Reguły Przypisania
rv	Zastosowane	Urządzenie	Niedostępny

Pierwsza strona ← Strona z 1 → Ostatnia strona

1 elementów

Zapisz
Zamknij

Okno informacyjne - Polityka

Aby uzyskać więcej informacji dotyczących polityk, zapoznaj się z „Zmiany ustawień polityk.” (p. 152)

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.

Nazwa Punktu końcowego	IP	Etykieta
TA9NSG368T13	10.17.44.243	
TAT6NRHH90MI	10.17.45.101	

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, pierścieniu aktualizacji, datę i godzinę aktualizacji oraz ostatnie sprawdzenie dostępności nowych wersji.



AST-TB-W7X86-2

General Protection Policy Connected Endpoints **Repository details** Scan Logs Troubleshooting

Bitdefender Endpoint Security Tools

BEST (Windows)

Product version (stored locally)

Slow ring:	6.6.18.265
Fast ring:	6.6.19.273

Product version (Bitdefender repository)

Slow ring:	N/A
Fast ring:	N/A
Last update time:	26 June 2020 18:4...
Last check time:	N/A

Security Content

FULL ENGINES (Local Scan)		LIGHT ENGINES (Hybrid Scan)	
Signatures stored locally		Signatures stored locally	
x86:	7.84969	x86:	N/A
x64:	N/A	x64:	7.84969
Signatures in Bitdefender repository		Signatures in Bitdefender repository	
x86:	7.84969	x86:	N/A
x64:	N/A	x64:	7.84969
Last update time:	29 June 2020 14:5...	Last update time:	29 June 2020 14:5...
Last check time:	29 June 2020 16:0...	Last check time:	29 June 2020 16:0...
Status:	● Up to date	Status:	● Up to date

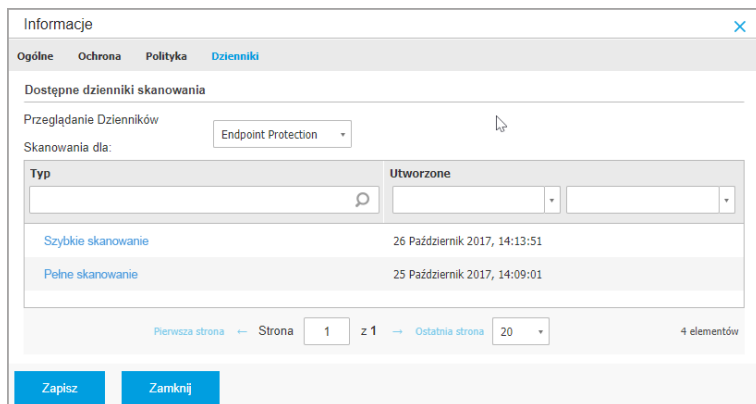
Okno informacyjne - zakładka Szczegóły repozytorium

Zakładka Dzienniki Skanowania

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

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

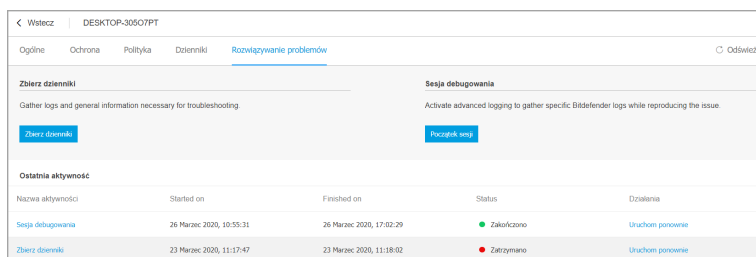
Tabela Rozwiązywanie problemów

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)	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Wiadomości o błędach otrzymane podczas aktualizacji produktu lub treści bezpieczeństwa
Kontrola Zawartości (skanowanie ruchu i kontrola użytkownika)	<ul style="list-style-type: none"> - Witryna się nie wczytuje - Elementy strony internetowej nie są wyświetlane poprawnie
Łączność z usługami w chmurze	<ul style="list-style-type: none"> - Punkt końcowy nie ma łączności z Bitdefender Cloud Services
Ogólne problemy z produktem (rejestrowanie wysokiej szczegółowości)	<ul style="list-style-type: none"> - Odtwórz ogólny zgłoszony problem z pełnym rejestrowaniem

Rodzaje problemów dla maszyn z Linux:

Rodzaj zagadnienia	Przypadek użycia
Antymalware i Aktualizacja	<ul style="list-style-type: none"> - 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)	<ul style="list-style-type: none"> - Odtwórz ogólny zgłoszony problem z pełnym rejestrowaniem

Rodzaje problemów dla Serwerów Bezpieczeństwa:

Rodzaj zagadnienia	Przypadek użycia
Antymalware (skanowanie Dostępowe i Nażądanie)	<p>Jakiegokolwiek nieoczekiwane zachowanie Serwera Bezpieczeństwa wliczając:</p> <ul style="list-style-type: none"> – 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	<p>Jakiegokolwiek nieoczekiwane zachowanie obserwowane z konsoli GravityZone:</p> <ul style="list-style-type: none"> – Wirtualne maszyny nie są poprawnie raportowane w konsoli GravityZone – Problemy polityk (polityka nie jest zastosowana) – Serwer Bezpieczeństwa nie może połączyć się z konsolą GravityZone <p>Notatka Użyj tej metody na polecenie Biznesowego Wsparcia Bitdefender.</p>

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 sugestyjną nazwę dla grupy i naciśnij **OK**. Nowa grupa pojawi się w folderze **Niestandardowe Grupy**.

Zmianie 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. 141).

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.

Nazwa	System oper.	IP	Ostatnio przeglądane	Etykieta
<input type="text"/>	<input type="text"/>	10.10.12.204	<input type="text"/>	<input type="text"/>

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 **Filtryz** 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 dziedziczna), status przypisanej polityki (aktywna, przypisana lub w toku). Możesz również wybrać wyświetlanie jedynie podmioty z politykami modyfikowanymi w trybie Power User.

Typ Bezpieczeństwo **Polityka** Głębokość

Szablon:

Edytowane przez Power User

Typ: Bezpośrednie
 Dziedziczone

Status: Aktywne
 Zastosowane
 Oczekujące

Głębokość: wewnątrz zaznaczonych folderów

Zapisz Anuluj Kasuj

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.

Typ Bezpieczeństwo Polityka **Głębokość**


Filtruj według

Obiekty wewnątrz zaznaczonych folderów
 Wszystkie elementy rekurencyjne

Głębokość: wewnątrz zaznaczonych folderów

Zapisz Anuluj Kasuj

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

górnjej 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.

	Nazwa	System oper.	IP	Ostatnio przeglądane	Etykieta
<input type="checkbox"/>	BHARJOC-TEST	Windows	10.10.12.204	Niedostępny	Niedostępny

Wyszukiwanie komputerów

6.2.5. Uruchamianie Zadań

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

Oto co możesz zrobić:

- „Zainstaluj” (p. 63)
- „Odinstaluj Klienta” (p. 69)
- „Aktualizacja klienta” (p. 70)
- „Rekonfiguruj Klienta” (p. 71)
- „Napraw Klienta” (p. 73)
- „Restartuj maszynę” (p. 74)
- „Przeszukiwanie sieci” (p. 74)

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. 130).

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 instalację:


1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz **Komputery i Wirtualne Maszyny** z selektora widoku.

- Wybierz żadaną 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**.

- Wybierz wpisy (punkty końcowe lub grupy punktów końcowych), na których chcesz zainstalować ochronę.
- Kliknij przycisk  **Zadanie** z górnej strony tabeli i wybierz **Instaluj**. Kreator **Klienta Instalacji** został wyświetlony.


Zainstaluj klienta ✕

Opcje

Teraz
 Zaplanowane

Automatyczny restart systemu (jeżeli potrzebny)

Menedżer uprawnień

<input type="checkbox"/>	Użytkownik	Hasło	Opis	Akcja
<input type="checkbox"/>	admin	*****	Doc1	

Instalowanie Bitdefender Endpoint Security Tools z menu zadań

- 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.

Wdrożeniowiec			
Wdrożeniowiec:		Endpoint Security Relay	
Nazwa	IP	Wybrana Nazwa/IP Serwera	Etykieta
MASTER-PC	192.168.1.141		Niedostępny
NMN-DOC1	10.0.2.15		Niedostępny

Strona 1 z 1, 20 elementów

- 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.
- 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.
- 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.
- 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. 255).

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. 130).



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. 43).

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. 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. 130).

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. 130).


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. 130).

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. 130).

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](#).

- Wybierz pożądaną kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
- Zaznacz pola wyboru dla komputerów na których chcesz dokonać network discovery.
- Kliknij przycisk  **Zadania** z górnej strony tabeli i wybierz **Network Discovery**.
- 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. 130).

6.2.6. Tworzenie szybkich raportów

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

- Przejdź do strony **Sieć**.
- Wybierz **Komputer i Wirtualna Maszyna** dla [selektora widoku](#).
- 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.
- Zaznacz pole wyboru dla komputera, który chcesz uwzględnić w raporcie.
- Kliknij przycisk  **Raport** w górnej części tabeli i wybierz rodzaj raportu z menu.
Aby uzyskać więcej informacji, odwołaj się do „Typy Raportu” (p. 250).
- Konfiguracja opcji raportu. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie raportów” (p. 255).
- 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.

i 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. 154).


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 ???.

6.2.8. 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 dużych sieci Active directory, synchronizacja może zająć więcej czasu.

6.3. Maszyny wirtualne

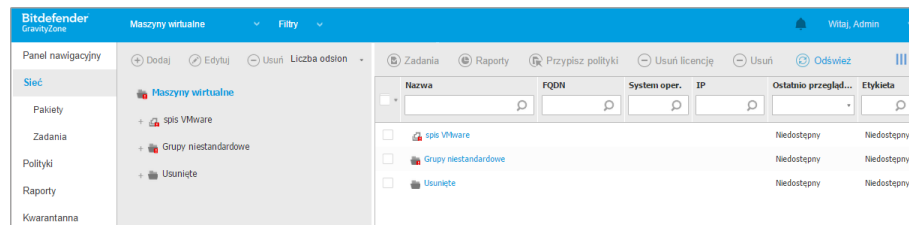
Aby zobaczyć zwirtualizowaną pod swoim kontem infrastrukturę, przejdź do strony **Sieć** i wybierz **Maszyny Wirtualne** z [Selektora widoku](#).



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. 38).



Nazwa	FQDN	System oper.	IP	Ostatnio przegląd...	Etykieta
<input type="checkbox"/> sps VMware					
<input type="checkbox"/> sps VMware				Niedostępny	Niedostępny
<input type="checkbox"/> Grupy niestandardowe				Niedostępny	Niedostępny
<input type="checkbox"/> Usunięte				Niedostępny	Niedostępny

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 **||| 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 maszyny wirtualne wykryte w twojej sieci poza jakimkolwiek Serwerem vCenter lub systemem XenServer.

Lewy panel zawiera menu zwane **Widoki** z którego użytkownik może wybrać rodzaj widoku dla każdego dostawcy technologii 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. 137).

W sekcji **Sieć**, możesz zarządzać wirtualnymi maszynami, 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 wirtualnych](#) z 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. 303) 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. 133).

Stan łączności

Status łączności dotyczy tylko zarządzanych maszyn wirtualnych. 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 może blokować komunikację pomiędzy agentem ochrony a serwerem komunikacji GravityZone.
 - 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 posiadała łączności z Control Center GravityZone. 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 ochrony dotyczy tylko zarządzanych maszyn wirtualnych. 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.
- Klucz licencyjny wygaś.
- Produkt Bitdefender jest nieaktualny.
- Zawartość bezpieczeństwa jest nieaktualna.
- Wykryto złośliwe oprogramowanie.
- 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 zidentyfikować status maszyny wirtualnej przez sprawdzenie odpowiedniej ikony. Szczegółowe informacje znajdują się w [„Sprawdzanie Statusu Maszyn Wirtualnych”](#) (p. 79).
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. 91).

- 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 Przekąźnikowe:** nazwa, adres IP i etykieta przełącznika, do którego podłączona jest maszyna wirtualna.

Informacje			
Ogólne	Ochrona	Polityka	Dzienniki
Maszyna wirtualna		Warstwy bezpieczeństwa	
Nazwa:	TA_EPS_832_BEF4	Punkt końcowy:	Aktywne
FQDN:	ta_eps_832_bef4		
IP:	10.17.47.59		
System oper.:	Windows 8 Pro		
Etykieta :	<input type="text"/>		
Infrastruktura:	Grupy niestandardowe		
Grupa:	Custom Groups		
Stan:	Online		
Ostatnio widziany:	Online		
Nazwa Hosta:			
IP hosta:			
<input type="button" value="Zapisz"/>		<input type="button" value="Zamknij"/>	

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.

- 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. 81).
- 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 (**Wi/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. 255)

- 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. 120).

Informacje
✕

Ogólne
Ochrona
Polityka
Dzienniki

Ochrona Punktu Końcowego
Bezpieczny ✓

B

Agent

Typ: BEST

Wersja produktu: 6.2.25.944

Ostatnia aktualizacja produktu: 27 Październik 2017 11:40:22

Wersja sygnatur: 7.73597

Ostatnia aktualizacja sygnatur: 27 Październik 2017 11:40:22

Podstawowy silnik skanowania: Lokalne Skanowanie

Zastępczy silnik skanowania: Brak

Przegląd

➔

➤ **Moduły**

Antymalware: Włączony

Zapora Sieciowa: Wyłączony

Kontr. Zawart.: Włączony

Użytkownik profesjonalny: Wyłączony

Kontrola Urządzenia: Włączony

Zaawansowana Kontrola Zagrożeń: Włączony

📄 **Raportowanie (dzisiaj)**

Status szkodliwego oprogramowania: Widok

-> Nie wykryto wirusów

Aktywność Malware: Widok

-> Brak aktywności

Zapisz

Zamknij

Okno informacyjne - zakładka Ochrony

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 wirtualna 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.

Informacje ✕

Ogólne Punkt końcowy **Polityka**

Szczegóły

Aktywna polityka: **rv**

Typ: Urządzenie

Przypisanie: Bezpośrednie

Przypisane polityki

Nazwa polityki	Status	Typ	Reguły Przypisania
<input type="text" value="rv"/>	Zastosowane	Urządzenie	Niedostępny

Pierwsza strona ← Strona z 1 → Ostatnia strona

1 elementów

Zapisz Zamknij

Okno informacyjne - Polityka

Aby uzyskać więcej informacji dotyczących polityk, zapoznaj się z „Zarządzanie politykami” (p. 142)

Zakładka Przekaznika

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.

Nazwa Punktu końcowego	IP	Etykieta
TA9NSG368T13	10.17.44.243	
TAT6NRHH90MI	10.17.45.101	

Pierwsza strona ← Strona 1 z 1 → Ostatnia strona 20 2 elementów

Zapisz Zamknij

Okno informacyjne - Relay

Zakładka Dziennik Skanowania

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

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.

Informacje

Ogólne Ochrona Polityka Dzienniki

Dostępne dzienniki skanowania

Przeglądanie Dzienników

Skanowania dla: Endpoint Protection

Typ	Utworzone
Szybkie skanowanie	26 Październik 2017, 14:13:51
Pełne skanowanie	25 Październik 2017, 14:09:01

Pierwsza strona ← Strona 1 z 1 → Ostatnia strona 20 4 elementów

Zapisz Zamknij

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 z XenServer 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 umieszczonych 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 sugestywną nazwę dla grupy i naciśnij **OK**. Nowa grupa wyświetli się w **Grupy Niestandardowe**.

Zmianianie 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. 141).

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.

	Nazwa	System oper.	IP	Ostatnio przeglądane	Etykieta
	<input type="text"/>	<input type="text"/>	10.10.12.204 <input type="button" value="X"/>	<input type="text"/>	<input type="text"/>

Sortowanie komputerów

Filtrowanie Wirtualnych Maszyn

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

Typ	Bezpieczeństwo	Polityka	Moc	Oznaczenie	Głębokość
Filtruj według					
<input type="checkbox"/> Maszyny wirtualne	<input type="checkbox"/> Klastry				
<input type="checkbox"/> Hosty	<input type="checkbox"/> Centra danych				
<input type="checkbox"/> vApps	<input type="checkbox"/> pule zasobów				
<input type="checkbox"/> Foldery	<input type="checkbox"/> Pule				
Głębokość: wewnątrz zaznaczonych folderów					
<input type="button" value="Zapisz"/>		<input type="button" value="Anuluj"/>		<input type="button" value="Kasuj"/>	

Wirtualne Maszyny - Filtrowane po Rodzaju

- **Bezpieczeństwo**. Wybierz zarządzanie ochroną i/lub stan zabezpieczeń, aby przefiltrować maszyny wirtualne.

Typ	Bezpieczeństwo	Polityka	Moc	Oznaczenie	Głębokość
Zarządzanie		Zagrożenia			
<input type="checkbox"/>	Zarządzanie punktami końcowymi	<input type="checkbox"/>	Z problemami bezpieczeństwa		
<input type="checkbox"/>	zarządzanie przez vShield	<input type="checkbox"/>	Bez problemów bezpieczeństwa		
<input type="checkbox"/>	Zarządzany (Przełączniki)				
<input type="checkbox"/>	Niezarządzane				
Głębokość: wewnątrz zaznaczonych folderów					
Zapisz		Anuluj		Kasuj	

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 (Aktywne, Przypisane lub w Toku).

Typ	Bezpieczeństwo	Polityka	Moc	Oznaczenie	Głębokość
Szablon: <input type="text"/>					
<input type="checkbox"/> Edytowane przez Power User					
Typ:	<input type="checkbox"/> Bezpośrednie				
	<input type="checkbox"/> Dziedziczone				
Status:	<input type="checkbox"/> Aktywne				
	<input type="checkbox"/> Zastosowane				
	<input type="checkbox"/> Oczekujące				
Głębokość: wewnątrz zaznaczonych folderów					
Zapisz		Anuluj		Kasuj	

Wirtualne Maszyny - filtrowane po Polotyce

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

Typ Bezpieczeństwo Polityka **Moc** Oznaczenie Głębokość

Pokaż

Online

Offline

Zawieszona

Głębokość: wewnątrz zaznaczonych folderów

Zapisz **Anuluj** **Kasuj**

Wirtualne Maszyny - Filtrowanie po Zasilaniu

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

Typ Bezpieczeństwo Polityka Moc **Oznaczenie** Głębokość

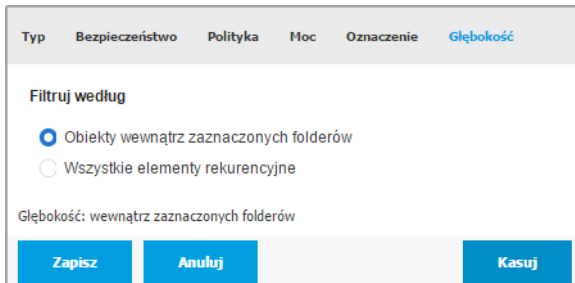
			(+)
Typ	Atrybuty	Wartość / E...	Działania

Głębokość: wewnątrz zaznaczonych folderów

Zapisz **Anuluj** **Kasuj**

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 wyczyścić 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. 96)
- „Zadania Uaktualnienia” (p. 106)
- „Zainstaluj” (p. 109)
- „Odinstaluj Klienta” (p. 113)
- „Aktualizacja” (p. 114)
- „Rekonfiguruj Klienta” (p. 115)
- „Przeszukiwanie sieci” (p. 116)

- „**Restartuj maszynę**” (p. 117)

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.

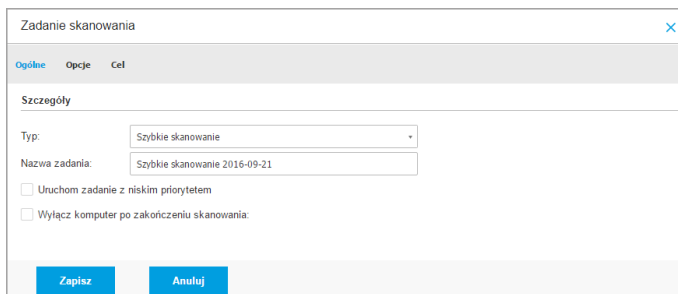
Po utworzeniu zadania, od razu uruchomi się na maszynach wirtualnych będących online w sieci. Jeżeli maszyna wirtualna jest offline, zadanie rozpocznie się zaraz po podłączeniu online.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do „[Przeglądanie i zarządzanie zadaniami](#)” (p. 130).

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 zostanie 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 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.

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. 304).

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.

Ustawienia

Typy plików

Typ: Rozszerzenia niestandardowe

Rozszerzenia: exe X
bat

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-supported). 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 różne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencji (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 podejrzone przez analizę heurystyczną i inne technologie Bitdefendera. To dostarcza wysoki poziom wykrywania, lecz użytkownicy muszą być świadomi możliwych false positives (czyste pliki wykryte jako podejrzone) w niektórych przypadkach. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

Zadania skanowania są skonfigurowane domyślnie żeby ignorować podejrzone pliki. Możesz zmienić domyślną akcję, 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.

- Idź do zakładki **Cel** i dodaj lokalacje które chciałbyś przeskanować na docelowych maszynach wirtualnych.

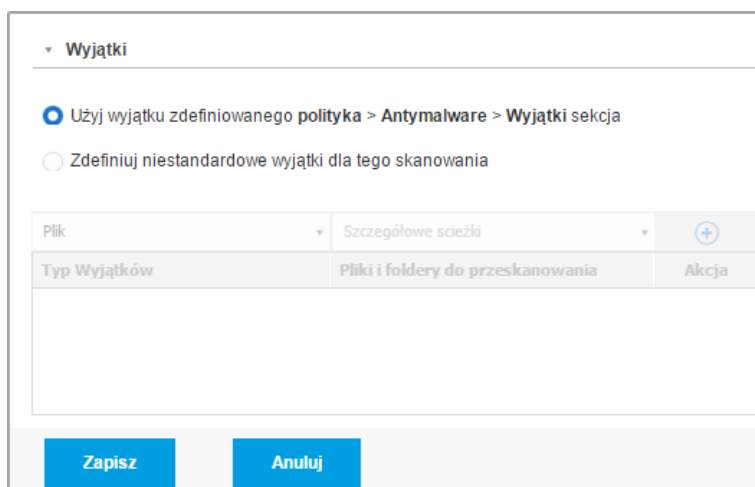
W sekcji **Cel skanowania** możesz dodać nowy filtr lub folder do przeskanowania:

- a. Wybierz wcześniej zdefiniowaną lokalizację 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 zdefiniowaną 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 **Określoną ścieżkę**, 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. 305).
- 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.



Typ Wyjątków	Pliki i foldery do przeskanowania	Akcja
--------------	-----------------------------------	-------

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. 191).

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

Możesz zobaczyć i zarządzać zadaniem na stronie **Siec > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „[Przeglądanie i zarządzanie zadaniami](#)” (p. 130).

i 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. 172).

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](#).

- Wybierz pożądaną kontener z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
- Wybierz docelowe punkty końcowe.
- Kliknij przycisk  **Zadania** z górnej części tabeli i wybierz **Skanowanie Aktualizacji**. Pojawi się nowe okno potwierdzające.
- 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. 121).



Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, zapoznaj się z „[Przeglądanie i zarządzanie zadaniami](#)” (p. 130).

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. 230).

Instalacja aktualizacji

Aby zainstalować jedną lub więcej aktualizacji na docelowych maszynach wirtualnych:

- Przejdź do strony **Sieć**.
- Wybierz **Maszynę Wirtualną** z [selektora widoku](#).
- Wybierz pożądaną kontener z lewego panelu bocznego. Wszystkie punkty końcowe z wybranego kontenera są wyświetlane w tabeli prawego panelu bocznego.
- 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.
- W razie potrzeby użyj opcji sortowania i filtrowania w górnej części tabeli, aby znaleźć określone aktualizacje.
- 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 aktualizacje.

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. 130).

Notatka

- Aby zaplanować wdrożenie aktualizacji, edytuj polityki przypisane do docelowych komputerów i skonfiguruj ustawienia w sekcji **Zarządzanie Aktualizacjami**. Aby uzyskać więcej informacji, zapoznaj się z „[Zarządzanie Aktualizacjami](#)” (p. 230).
- 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. 125).
- 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.

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: **Niezarządzone** z zakładki **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z zakładki **Głębokość**.

- Wybierz podmioty (maszyny wirtualne, hosty, klastry lub grupy) na których chcesz zainstalować ochronę.
- Kliknij przycisk **Zadania** z górnej strony tabelki i wybierz **Instaluj > BEST**. Kreator **Klienta Instalacji** został wyświetlony.

Użytkownik	Hasło	Opis	Akcja
<input type="checkbox"/>	admin	*****	Doc1

Instalowanie Bitdefender Endpoint Security Tools z menu zadań

- 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:

- **Urządzenie GravityZone**, gdy maszyny łączą się bezpośrednio do Urządzenia 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. 130).



Notatka

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


Aktualizacja

Sprawdź 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. 81).

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. 130).

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 pożądaną 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 by było wykonywane co każde 2 godziny. Zadanie rozpocznie się na każdej docelowej maszynie 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. 130).

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. 130).


Restartuj maszynę

Możesz zdalnie uruchomić ponownie wybrane zarządzane maszyny wirtualne.



Notatka

Sprawdź strony [Sieć > Zadania](#) przed ponownym uruchomieniem maszyn wirtualnych. Upřednio 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](#).

6.3.6. Tworzenie szybkich raportów

Możesz wybrać żeby stworzyć błyskawiczne raporty na temat zarządzanych wirtualnych maszyn poczynając 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 „[Typy Raportu](#)” (p. 250).
7. Konfiguracja opcji raportu. Aby uzyskać więcej informacji, odwołaj się do „[Tworzenie raportów](#)” (p. 255)
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.

i 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 maszynie 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. 141)


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. 143).

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. 241).

6.3.9. Czyszczenie Licencji

W ekwipunku Active Directory, vCenter 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 licencje** w górnej części tabeli.
6. Kliknij **Tak** w oknie potwierdzenia, aby kontynuować.

6.4. 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.

Patch Name	KB Nu...	CVE	Bullet...	Patch sever...	Category	Installed / Pend...	Missing / Install...	Affected Pr...
Windows6.1-SP1-Windows7-KB...	Q24799...	1 CVE(s)	MS11-0...	Critical	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)
Windows6.1-SP1-Windows7-KB...	Q25054...	0 CVE(s)	MSWU...	None	Non-Security	0 EP / 0 EP	1 EP / 0 EP	6 Product(s)
Windows6.1-SP1-Windows7-KB...	Q24881...	0 CVE(s)	MSWU...	None	Non-Security	0 EP / 0 EP	1 EP / 0 EP	6 Product(s)
Windows6.1-Windows7-SP1-KB...	Q24916...	1 CVE(s)	MS11-0...	Important	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)
Windows6.1-Windows7-SP1-KB...	Q25062...	1 CVE(s)	MS11-0...	Important	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)

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](#)

6.4.1. 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 aktualizację 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 nieudana.** 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.

6.4.2. Wyszukiwanie i Filtrowanie Aktualizacji

Domyślnie Control Center wyświetla wszystkie dostępne aktualizacje 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.

6.4.3. 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 Aktualizacji](#)” (p. 129).
- 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.

6.4.4. 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 aktualizację, 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. 74).
- 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 otrzymywał 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 umożliwi 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 [???](#).

4. Kliknąć **Instaluj**.

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

i 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 ???.
- 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.

6.4.5. 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.

i 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 aktualizację, 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.

i Notatka

Możesz odinstalować tylko jedną aktualizację 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. 74).
- 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 otrzymywał 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 [???](#).

- 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.

6.4.6. Tworzenie Statystyk Aktualizacji

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.

6.5. 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](#)
- [Usuń zadania](#)

6.5.1. 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.

Nazwa	Typ zadania	Status	Czas startu	Raporty
<input type="checkbox"/> Szybkie skanowanie 2015-08-28	Skanowanie	Oczekujące (0 / 1)	28 Sie 2015, 15:34:18	

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.
- **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.
- **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.

Aby zobaczyć szczegóły każdego pod zadania, wybierz je i sprawdź sekcje **Szczegóły** na dole tabeli.

Nazwa komputera	Status
Doc1 (Win7 x32 SP1 relay)	Oczekujące


Szczegóły statusu zadania

Możesz uzyskać informację na temat:

- Data i czas rozpoczęcia zadania.
- Data i czas końca zadania.
- Opis napotkanych błędów.


6.5.2. 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**. Poczekaaj, aż zostanie wyświetlony raport. Aby uzyskać więcej informacji, odwołaj się do „[Używanie raportów](#)” (p. 250).

6.5.3. 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 podzadaniami, opcja **Uruchom ponownie** jest dostępna jedynie wtedy gdy wszystkie podzadania zostaną ukończone i tylko nieudane podzadania będą wykonywane.

6.5.4. 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 podzadania zostaną anulowane. W tym przypadku, wszystkie podzadania nie zostaną ukończone.

6.6. 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.  **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.

6.7. 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](#)

6.7.1. 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**.

6.7.2. Czyszczenie Maszyn Offline

W sekcji **Czyszczenie maszyn offline**, możesz skonfigurować zaplanowane reguły automatycznego usuwania nieużywanych maszyn wirtualnych z Zasobów Sieci.

Tasks	Offline machines cleanup
Risk Management	Configure rules to automatically delete unused virtual machines from the Network Inventory and clear their license seats.
Policies	+ Add rule X Delete
Assignment Rules	
Reports	
Quarantine	
Accounts	
User Activity	
System Status	
Configuration	
Update	

Rule name	Offline for	Machines name	Location	Deleted(last 24h)	State
<input type="checkbox"/> Rule 3	66 days	...	Custom Groups	0 machines	<input checked="" type="checkbox"/>
<input type="checkbox"/> Rule 4	78 days	...	Custom Groups	0 machines	<input type="checkbox"/>

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 wiralnych.
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**.

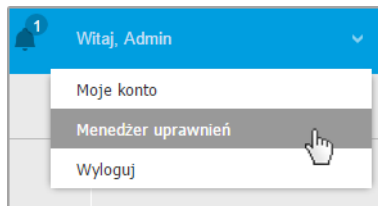
Aby usunąć jedną lub więcej reguł:

1. Użyj pól wyboru, aby wybrać jedną lub więcej reguł.
2. Kliknij przycisk **Usuń** w górnej części tabeli.

6.8. Manager uprawnień

Menadżer Poświadczeń pomaga definiować poświadczenia wymagane podczas dostępu do zasobów Serwera vCenter i do zdalnego uwierzytelniania na różnych systemach operacyjnych w twojej sieci.

Aby otworzyć Menadżera Poświadczeń, kliknij nazwę użytkownika w górnym prawym rogu strony i wybierz **Menadżer Poświadczeń**.



Menu menadżera poświadczeń

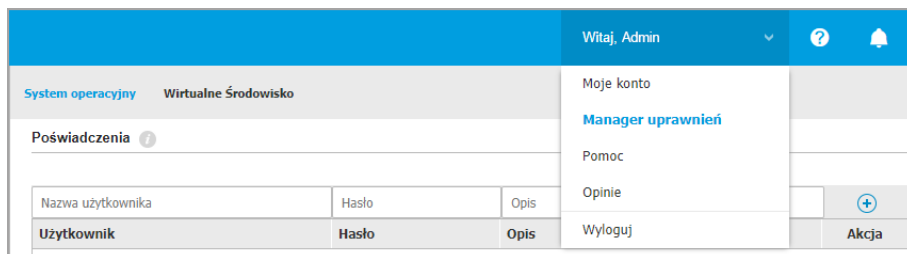
Okno **Menadżer poświadczeń** zawiera dwie zakładki:

- [System Operacyjny](#)
- [Wirtualne środowisko](#)

6.8.1. 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.

6.8.2. 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, pokazując 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.

6.8.3. 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. Polityki określają ustawienia ochrony, które zostaną zastosowane dla docelowych obiektów inwentarza sieci (komputery i maszyny wirtualne).

Natychmiast po instalacji, zasobom obiektów sieciowych zostanie przypisana domyślna polityka, która jest wstępnie skonfigurowana z zalecanymi ustawieniami ochrony. Nie możesz modyfikować ani usuwać domyślnej polityki. Możesz użyć go tylko jako szablonu dla [tworzenie nowej polityki](#).

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**

Nazwa polityki	Utworzono przez	Zmodyfikowany	Cele	Zastosowane/ Oczekujące
Polityka domyślna (domyślny)	root		318	4/ 4461

Strona Polityki

Istniejące polityki są wyświetlane w tabeli. Dla każdej polityki, możesz zobaczyć:

- Nazwa polityki.
- Użytkownik, który stworzył politykę.
- Data i czas ostatniej modyfikacji polityki.

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.

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 metodę tworzenia polityki:
 - **Dodaj nową politykę.**
 - Kliknij przycisk **+** **Dodaj** w górnej części tabeli. Ta Komenda tworzy nową politykę używając domyślnego szablonu polityki.
 - **Sklonuj istniejącą politykę.**
 - a. Zaznacz pole wyboru polityki jaką chcesz powielić.
 - b. Kliknij przycisk **+** **Klonujz** górnej strony tabeli.
3. Konfiguruj ustawienia polityk. Szczegółowe informacje znajdują się w „[Polityki Komputerów i Maszyn Wirtualnych](#)” (p. 154).
4. Naciśnij **Zapisz** aby utworzyć politykę i powrócić do listy polityk.

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.

Możesz przypisać 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**.


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 docelowe punkty końcowe. Możesz wybrać jeden lub kilka punktów końcowych bądź grupy punktów końcowych.
3. Kliknij  **Przypisz politykę** przycisk w górnej części panelu, bądź wybierz opcję **Przypisz politykę** z menu kontekstowego.

Zostaje wyświetlona strona **Przypisania polityk**:

Przypisana Polityka ✕

Opcje

Przypisz następujący szablon polityki Default policy

Dziedziczone z góry

Siła dziedziczenia polityk dla obiektów ⓘ

Cele

jednostka	Polityka	odziedziczone z
<input type="text"/>	<input type="text"/>	
Grupy niestandardowe	Default policy	Komputery i Maszyny Wirtualne

Pierwsza strona — Strona z 1 — Ostatnia strona

1 element

Zakończ Anuluj

Ustawienia Przypisania Polityki

4. 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.
5. W przypadku ostrzeżenia, kliknij link **Wyklucz te elementy docelowe** aby kontynuować.
6. 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.
7. 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.
8. 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 mogą mieć tylko 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 wzięłeś 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 **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

Typ	Wartość
Punkt końcowy może łączyć się do GravityZone	Tak/Nie
Typ sieci	<p>Wireless/Ethernet</p> <p>Przy wyborze Wireless, możesz również dodać SSID sieci.</p> <p> WAŻNE Opcja ta nie ma zastosowania w systemach Linux i Mac.</p>
Nazwa hosta	<p>Nazwa hosta</p> <p>Na przykład: <code>cmp.bitdefender.com</code></p> <p> WAŻNE Możesz także używać wildcard. Gwiazdka (*) zastępuje zero lub więcej znaków, a znak zapytania (?) Zastępuje dokładnie jeden znak. Przykłady: <code>*.bitdefender.com</code> <code>cmp.bitdefend??.com</code></p>

- 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.

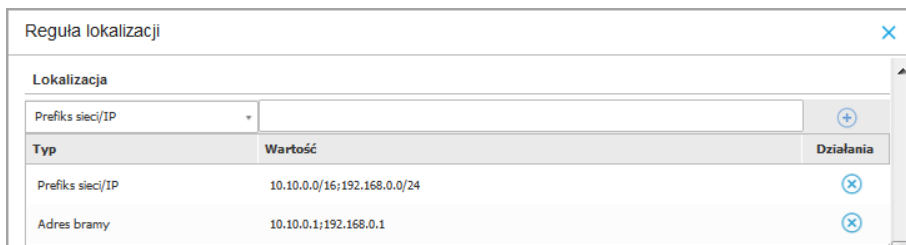


Ostrzeżenie

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		
Lokalizacja		
Typ	Wartość	Działania
Prefiks sieci/IP	10.10.0.0/16;192.168.0.0/24	⊗
Adres bramy	10.10.0.1;192.168.0.1	⊗

Reguła lokalizacji

Kliknij pole **Wartość**, aby edytować istniejące kryteria, a następnie naciśnij **Enter**, aby zapisać zmiany.

Aby usunąć lokalizację, zaznacz ją i kliknij przycisk **⊗ Usunąć**.

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. 148).
 - 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 **⊗ Usunąć** 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.

i 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.

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.

i 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. Znajdź politykę poszukiwaną politykę na liście i naciśnij jej nazwę by edytować.
3. Skonfiguruj ustawienia polityki według uznania. Szczegółowe informacje znajdują się w „[Polityki Komputerów i Maszyn Wirtualnych](#)” (p. 154).
4. 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. Naciśnij nazwę polityki. To otworzy stronę polityki.
3. Wprowadź nazwę nowej polityki.
4. 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 usunąć politykę:

1. Przejdź do strony **Polityki**.
2. Zaznacz pole wyboru polityki, którą chcesz skasować.
3. 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](#)
 - [Antymalware](#)
 - [Sandbox Analyzer](#)
 - [Ochrona sieci](#)
 - [Relay](#)

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. 142).

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](#)

- [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

Bitdefender GravityZone		Witaj, Admin	
Panel nawigacyjny	Ogólne	Szczegóły Polityki	
Sieć	Szczegóły	Nazwa: *	Polityka domyślna (1)
Pakiety	Powiadomienia	<input type="checkbox"/> Pozwól innym użytkownikom na edytowanie tej polityki	
Zadania	Ustawienia	Historia	
Polityki	Komunikacja	Utworzono przez:	Admin
Raporty	Aktualizacja	Stworzony:	Niedostępny
Kwarantanna	Antymalware		

Polityki

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.

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 **B** Bitdefender w pasku systemowym poprzez wybranie **O programie**.

Ustawienia

W tej sekcji możesz konfigurować następujące 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
- **Opcje**
- W tej sekcji możesz zdefiniować następujące 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. Raporty pomogą naszym inżynierom znaleźć co jest powodem problemu i zapobiec jego wystąpieniu następnym razem. Żadne prywatne informacje nie zostaną wysłane.
 - **Wyślij podejrzone pliki wykonywalne do analizy**. Wybierz tę opcję, aby pliki, które wydają się niegodne zaufania lub podejrzane się zachowują będą wysyłane do Laboratoriów Bitdefender do analizy.

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.

Nadrzędny	Nazwa	IP	Niestandardowa Nazwa/IP	Działania
1	MASTER-PC	192.168.1.141		⊗ ⊖ ⊕

Polityki - 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.

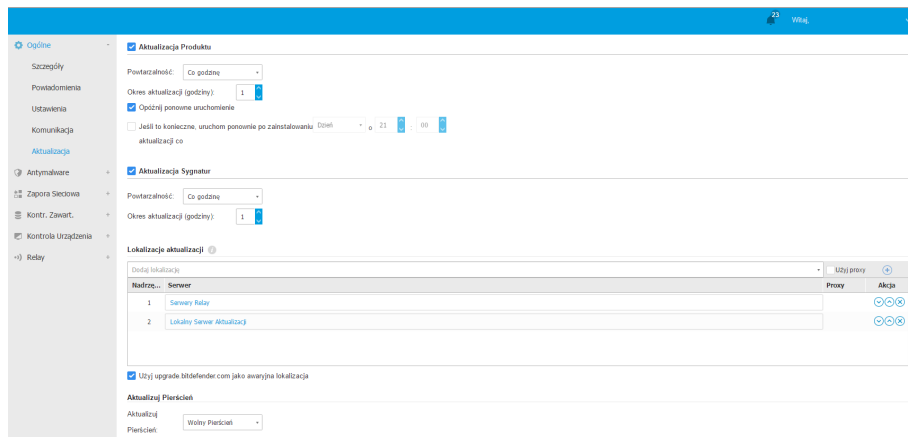
Komunikacja pomiędzy Punktami końcowymi a Usługami w Chmurze

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 - 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.
 - **Przełoż 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, następną 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

Wyłączenie 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, następną jest brana pod uwagę i tak dalej.

Aby usunąć lokalizację z listy, kliknij odpowiedni przycisk  **Usuń**. Można usunąć domyślną lokalizację, 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.

7.2.2. 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.

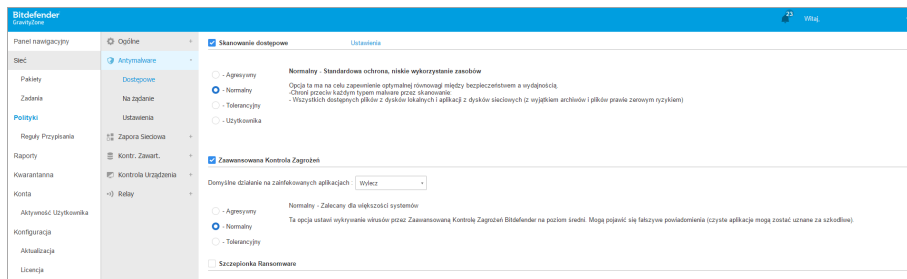
Ustawienia są zorganizowane w poniższych sekcjach:

- [Dostępowe](#)
- [Przy-Wykonywaniu](#)
- [Na żądanie](#)
- [Zaawansowany Anty-Exploit](#)
- [Ustawienia](#)

Dostępowe

W tej sekcji możesz skonfigurować komponenty zapewniające ochronę, gdy jest dostęp do pliku lub aplikacji:

- Skanowanie dostępne
- Szczepionka ransomware



Polityki - Ustawienia Dostępowe

Skanowanie dostępne

Skanowanie na żądanie zapobiega przed dostaniem się nowego malware do systemu 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 dostępne, 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. 304).

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 wyboru **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 niechciana 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-supported). 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 różne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencji (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 **znany** 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. To obejmuje moduł [Zaawansowanej Ochrony przed Zagrożeniami](#).

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 **Kopij 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 nieznanne złośliwe oprogramowanie.

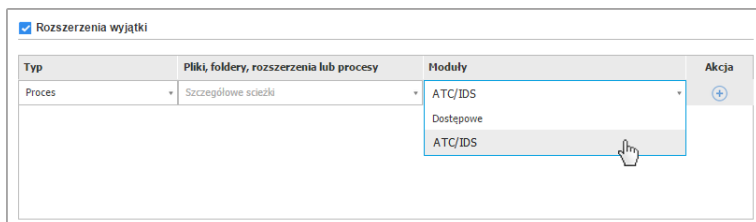
2. Zaawansowana Kontrola Zagrożeń domyślnie będzie próbowała wyleczyć zainfekowane aplikacje. Możesz ustawić inne domyślne działanie, używając dostępnego menu:
 - **Zablokuj**, aby odmówić dostępu do zainfekowanej aplikacji.
 - **Nie podejmuj żadnych akcji**, aby raportować tylko zainfekowane aplikacje 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 - 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. 277).

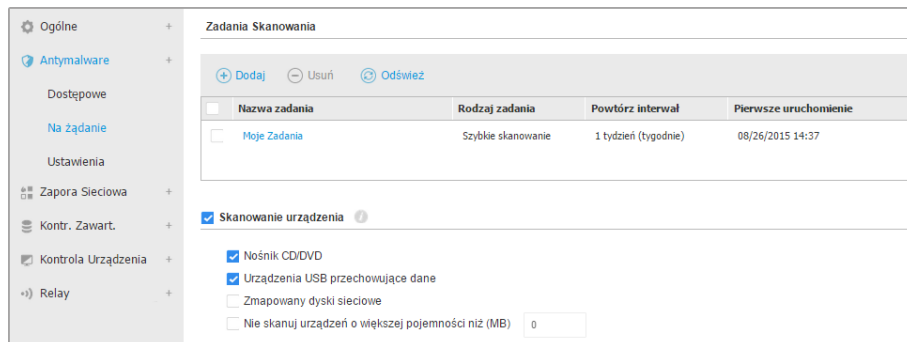
- Sprawdź raport **Audyt Bezpieczeństwa**.
- Sprawdź stronę **Aktywność Ransomware**.

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. 191).

Na żądanie

W tej sekcji możesz dodać i konfigurować skanowanie antymalware, które będą uruchamiać się regularnie na docelowych komputerach, według zdefiniowanego harmonogramu.



The screenshot shows the 'Zadania Skanowania' (Scanning Tasks) configuration page in the Bitdefender GravityZone interface. The page is divided into a left sidebar with navigation options and a main content area. The main content area features a table of scanning tasks and a list of scanning options.

Nazwa zadania	Rodzaj zadania	Powtórz interwał	Pierwsze uruchomienie
<input type="checkbox"/> Moje Zadania	Szybkie skanowanie	1 tydzień (tygodnie)	08/26/2015 14:37

Below the table, there are several checkboxes for scanning options:

- Skanowanie urządzenia
- Nośnik CD/DVD
- Urządzenia USB przechowujące dane
- Zmapowany dyski sieciowe
- Nie skanuj urządzeń o większej pojemności niż (MB)

Polityki - 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 złośliwe oprogramowanie, które może uchronić się przed ochroną w czasie rzeczywistym.

Oprócz regularnego skanowania, możesz również skonfigurować [automatyczne wykrywanie i skanowanie](#) zewnętrznych nośników pamięci.

Zarządzanie Zadaniem skanowania

Tabela Zadań skanowania informuje o istniejących zadaniach 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:

Edytuj zadanie

Ogólne Opcje Cel

Szczegóły

Nazwa zadania:

Uruchom zadanie z niskim priorytetem

Wyłącz komputer po zakończeniu skanowania:

Harmonogram

Czas i data rozpoczęcia: 09/22/2016 11:20

Powtarzalność

Harmonogram zadań do jednorazowego uruchomienia: 1 dzień (dni)

Zawsze uruchamiam zadanie: Nie Pon Wt Śr Czw Pt Sob

Jeśli zaplanowany czas pracy został przegapiony, uruchom zadania jak najszybciej

Pomnij jeśli następnie zaplanowane skanowanie ma się rozpocząć w ciągu mniej niż

1

dzień (dni)

Zapisz Anuluj

Polityki - Konfiguracja Ogólnych Ustawień Zadania Skanowania Na Żądanie

- **Szczegóły.** Wybierz sugestywną 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 swoją 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 następane zaplanowane skanowanie ma się rozpocząć za mniej niż**, a następnie określ 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. 304).

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-supported). 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 różne zaawansowane mechanizmy, które zawierają sygnatury malware, technologie oparte na maszynowym uczeniu się i sztucznej inteligencji (SI). Agent bezpieczeństwa może normalnie usunąć złośliwy kod z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.



WAŻNE

W przypadku określonych typów złośliwego oprogramowania oczyszczenie 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 akcję, 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 lokalizację 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 zdefiniowaną 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, przesunij 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 dostępu 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. 191).

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 urządzeń automatycznie podejmuje 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.

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 nieznanymi exploitami, 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. 184).

- **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. 185).

- **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. 185).

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

Technika	Opis
Ochrona procesu LSASS	Chroni proces LSASS przed wyciekami sekretnej informacji, takich jak hasła i ustawienia zabezpieczeń. Działanie domyślne: Blokuje proces

Techniki anti-exploit 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
Osł Stosu ROP	Wykrywa próby przejścia przepływu kodu przy użyciu techniki ROP, sprawdzając położenie stosu. Domyślna akcja: Proces blokowania
Nielegalne Połączenie ROP	Wykrywa próby przejścia kontroli nad kodem przy użyciu techniki ROP, sprawdzając wywoławczy wrażliwych funkcji systemowych.

Technika	Opis
	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. Domyślna akcja: Proces blokowania

Technika	Opis
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 literę, 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.

The screenshot shows the Bitdefender GravityZone interface. The left sidebar contains navigation options: Panel nawigacyjny, Sieć, Magazyn Aplikacji, Pakiety, Zadania, Polityki, Zasady przypisania, Raporty, Kwarantanna, Konta, Aktywność Użytkownika, Konfiguracja, and Aktualizacja. The central menu includes: Ogólne, Antymalware, Dostępowe, Na żądanie, Ustawienia, Serwery Bezpieczeństwa, Zapora Sieciowa, Kontr. Zawart., Kontrola aplikacji, Kontrola Urządzenia, and Relay. The main content area is titled 'Kwarantanna' and includes: 'Usuń pliki starsze niż (dni):' with a dropdown set to 30; 'Przesyłaj pliki objęte kwarantanną do laboratorium BitDefender co godzinę' with a dropdown set to 1; 'Przeskanuj ponownie pliki kwarantanny po aktualizacji bazy wirusów'; 'Kopuj pliki do kwarantanny przed zastosowaniem działań czyszczących'; 'Pozwól użytkownikom podjąć działania w lokalnej kwarantannie'; and 'Scentralizowana Kwarantanna' with fields for: 'Hasło Archiwum:', 'Potwierdź hasło:', 'Ścieżka udziału:' (set to \\computer\folder), 'Udostępnij Nazwę Użytkownika:' (set to domain\user), and 'Udostępnij Hasło:'.

Scentralizowana Kwarantanna

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 włączone 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 dostępne
- 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.

Typ	Pliki, foldery, rozszerzenia lub procesy	Moduły	Akcja
Plik	Szczegółowe ścieżki	Na żądanie	+

Polityki - 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 (nie dostępne 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 kombinację 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.

- 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.
- Opcjonalnie, kliknij przycisk **Pokaż uwagi**, aby dodać notatkę o regule w kolumnie **Uwagi**.
- 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:

- Kliknij **Eksportuj** w górnej części tabeli wykluczeń.
- 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 się 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.

7.2.3. 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 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. 189).

Po szczegółowe informacje na temat ręcznego przesyłania, zajrzyj do „[Ręczne Wysyłanie](#)” (p. 269). Aby uzyskać szczegółowe informacje o wysyłaniu z API, odnieś się do rozdziałów **Piaskownica** i **Portal Piaskownicy** w [Przewodniku API GravityZone \(On-Premises\)](#).

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. 307).

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 **Sredni** 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???

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. 307).

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 przysyłać 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:

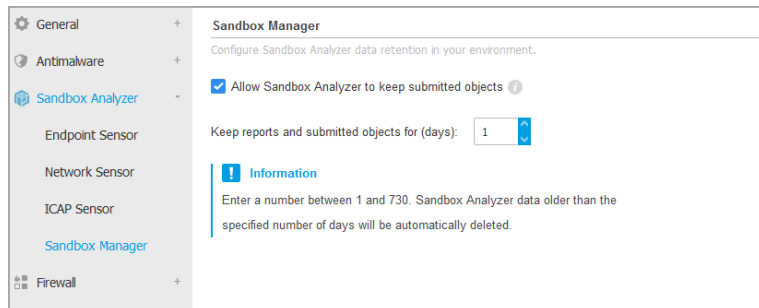
- **Serwer** – IP serwera proxy
 - **Port** - port używany do połączenia z serwerem proxy.
 - **Nazwa użytkownika** – nazwa użytkownika rozpoznawana przez proxy.
 - **Hasło** - poprawne hasło dla określonego użytkownika.
4. Pod **Profil detonacji**, dostosuj poziom złożoności analizy behawioralnej, jednocześnie 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 **Sredni** 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

7.2.4. 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. 204).



WAŻNE

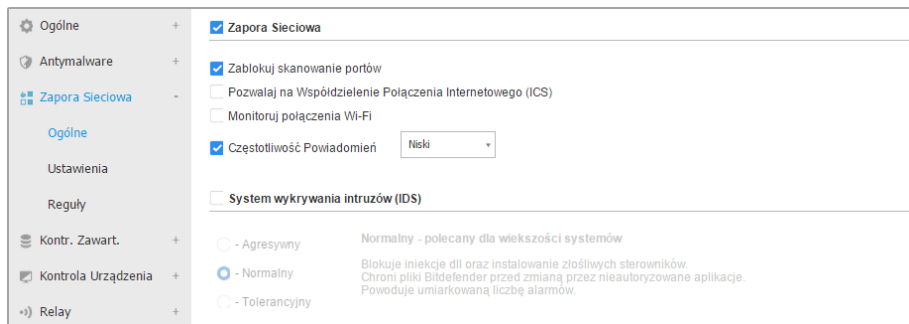
Moduł Zapory Sieciowej jest dostępny jedynie dla wspieranych stacji roboczych Windows.

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 - Ogólne Ustawienia 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 goście 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

Nazwa	Typ	Identyfikacja	MAC	IP	Akcja

Typ	Typ sieci	Niewidzialność Sieci
Przewodowy	Dom / Biuro	Wyłączony
Sieć bezprzewodowa	Miejsce publiczne	Wyłączony

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 menu 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 ograniczenie 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 **Adaptory** 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 profilu 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 **Adaptory**.

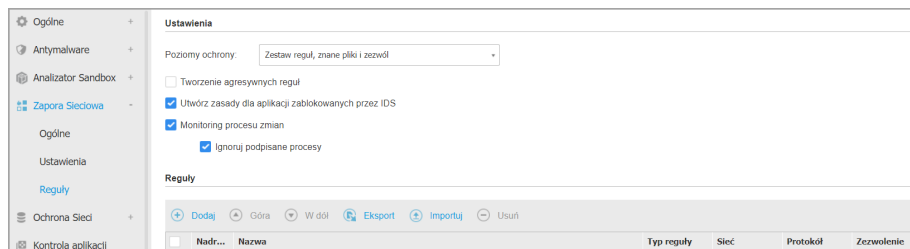
Jeśli wykrywanie oparte na Menadżerze Sieci Windows nie powiedzie się, zostanie podjęta próba wykrywania podstawowego. Profil ogólny użyty jest w przypadkach uważania profilu sieciowego za **Publiczny** a jego ustawienia ukrywania się są **Włączone**.

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 - 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 zablokuj wszystkie inne próby 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 nieznanne 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

Zwyczaj 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 znalezioneego 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 lokalizację 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 menu **Inne**.



Notatka

Numerzy 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 wersję 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, przesuując 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.applicationPath	Ścieżka aplikacji (tylko dla aplikacji bazujących na regułach)
details.commandLine	Linia komend (tylko dla aplikacji bazujących dla reguły)
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 falsz
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
<code>permission.setPermission</code>	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 wypełniona poprawnymi regułami.

7.2.5. 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 będzie 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 wyłączeń.

Ustawienia są zorganizowane w poniższych sekcjach:


- [Ustawienia ogólne](#)
- [Wyjątki globalne](#)

Ogólne	<input checked="" type="checkbox"/> Ochrona Sieci
Antywmalware	Wyłączając ten moduł, wyłączysz wszystkie jego funkcje i nie będziesz mógł modyfikować żadnych ustawień.
Analizator Sandbox	
Zapora Sieciowa	
Ochrona Sieci	Ustawienia ogólne
Ogólne	<input type="checkbox"/> Skanuj SSL
Kontr. Zawart.	<input type="checkbox"/> Pokaż pasek narzędzi przeglądarki (legacy)
Ochrona sieciowa	<input checked="" type="checkbox"/> Doradca wyszukiwania w przeglądarce (legacy)
Ataki Sieciowe	<input type="checkbox"/> Wyjątki globalne ⓘ
Zarządzanie Aktualizacjami	
Kontrola Urządzenia	

Polityki - 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 bezpieczeństwa Bitdefender.

- **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 kombinację określonej liczby znaków. Na przykład, ??? zastępuje każdą kombinację dokładnie 3 znaków.

W poniższej tabeli, znajdziesz znaleźć kilka próbek składni dla określonych adresów (URL).

Składnia	Wyjątek stosowania
<code>www.example*</code>	Dowolny adres URL zaczynający się od <code>www.example</code> (niezależnie od rozszerzenia domeny). Wyjątki nie zostaną zastosowane dla subdomen określonych stron, takich jak <code>subdomain.example.com</code> .
<code>*example.com</code>	Dowolny adres URL kończący się <code>example.com</code> , w tym jego subdomeny.
<code>*example.com*</code>	Dowolny URL zawierający podany ciąg.
<code>*.com</code>	Dowolna strona zawierająca rozszerzenie domeny <code>.com</code> , w tym ich subdomeny. Użyj tej składni, aby wykluczyć ze skanowania całe domeny na najwyższym poziomie.
<code>www.example?.com</code>	Dowolny adres internetowy rozpoczynający się od <code>www.example?.com</code> , gdzie ? może być zastąpiony dowolnym znakiem. Takie strony internetowe mogą zawierać: <code>www.example1.com</code> lub <code>www.exampleA.com</code> .



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 część 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".

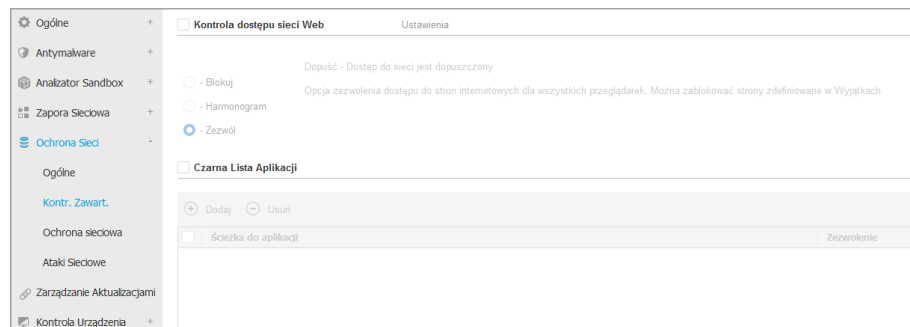
3. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli.

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.

- Standardowa wiadomość wyświetlona dla użytkownika, który wchodzi na zastrzeżoną stronę zawiera kategorie odpowiednią dla strony. Oznacź opcję **Pokaż szczegółowe alerty na kliencie**, jeśli chcesz ukryć te informacje przed użytkownikiem.



Notatka

Ta opcja nie jest dostępna dla systemu MacOS.

- 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 wtedy 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:

- Włącz opcję **Użyj Wykluczeń**.
- Podaj adresy jakie chcesz dopuścić albo zablokować w polu **Adresy Sieciowe**.
- Wybierz **Zezwól** lub **Zablokuj** z menu **Pozwolenia**.
- 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 funkcja 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 informacje mogą zawierać nazwy, 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, że wprowadziłeś 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

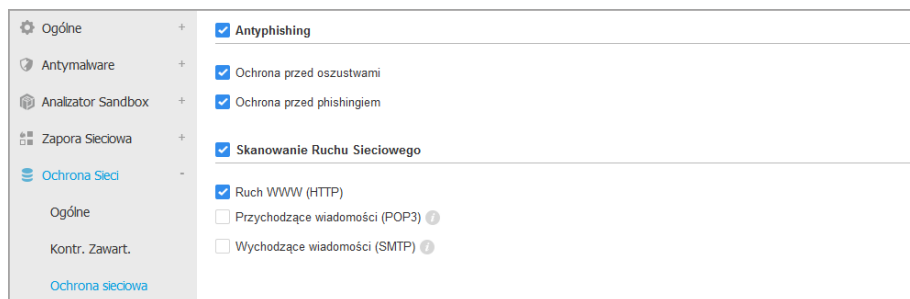
Jeżeli e-mail zawierający zablokowane dane jest zaadresowany do wielu odbiorców, to tylko Ci dla których zostały ustawione wyjątki, otrzymają go.

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 - 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 opcję 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 jest 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.

Ochrona przed atakiem sieciowym		
Ta funkcja to warstwa bezpieczeństwa zaprojektowana do wykrywania technik ataku sieciowego, które próbują uzyskać dostęp do ok. bezpieczeństwa organizacji.		
Techniki Ataku		
<input checked="" type="checkbox"/>	Wstępny dostęp	Zablokuj
<input checked="" type="checkbox"/>	Dostęp do poświadczeń	Zablokuj
<input checked="" type="checkbox"/>	Wykrycie	Zablokuj
<input checked="" type="checkbox"/>	Ruch Poprzeczny	Zablokuj
<input checked="" type="checkbox"/>	Crimeware	Zablokuj
Przywróć ustawienia domyślne		

Polityki - 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, złodziejstwo 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, exploit 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.

7.2.6. 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 Aktualizacji

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 Przełącznikach 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 łączy się z aktualizacją 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 ☹️ Usun 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 wysła 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 **Odlóż 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](#)

7.2.7. 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 będzie 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 agencji 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
Adaptory Bluetooth	x	x

Typ urządzenia	Windows	macOS
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)
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 pożądaných 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 przywoleń 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 różne 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.

Pamięć zewnętrzna Regula

Zezwolenie: * Niestandardowy

Opis: * External Storage

Niestandardowe zezwolenia

Firewire:	Dozwolone
ISA Plug & Play:	Dozwolone
PCI:	Dozwolone
PCMCIA:	Dozwolone
SCSI:	Dozwolone
SD Card:	Dozwolone
USB:	Dozwolone
Other:	Dozwolone

Zapisz Anuluj

Polityki - Kontrola Urządzeń - 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.

Typ reguły	Wyjątek	Opis	Zezwolenie	
<input type="checkbox"/>	ID Urządzenia	USB\VID_0C45&REV1E0A&H	Web Cam	Dozwolone
<input type="checkbox"/>	ID produktu	8192	AMD Ethernet adapters	Dozwolone

Polityki - Kontrola Urządzeń - Wykluczenia

7.2.8. 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 zdefiniowanie 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 aktualizacji:

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 **⊗ Usun**. Można usunąć domyślną lokalizację, jednak nie jest to zalecane.

7.2.9. 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.

Ogólne +

Antymalware +

Zapora Sieciowa +

Ochrona Sieci +

Kontrola aplikacji

Kontrola Urządzenia +

Relay +

Szyfrowanie -

Ogólne

Zarządzanie Szyfrowaniem

Włącz ten moduł, aby rozpocząć zarządzanie szyfrowaniem punktów końcowych za pomocą Centrum Sterowania. Wyłączenie tej funkcji spowoduje pozostawienie woluminu w bieżącym stanie i umożliwi użytkownikom zarządzanie szyfrowaniem lokalnie.

Deszyfruj
Zaznacz tę opcję aby deszyfrować woluminy.

Szyfruj
Zaznacz tę opcję aby szyfrować woluminy. Użytkownicy otrzymają informacje aby wpisać hasło do autoryzacji przed pełnym rozruchem komputera.

Jeśli aktywny jest Moduł Zaufanej Platformy (TPM), nie pytaj o hasło przed uruchomieniem.

Wyjątki ⓘ

Typ	Wykluczone przedmioty	Akcja
	jednostka	+

Pierwsza strona ← Strona 0 z 0 → Ostatnia strona 20 0 elementów

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/desyfrowania.

- **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. 243).

● 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 niezasyfrowanym punkcie końcowym:
 - Szyfrowanie przebiega bez konieczności podawania hasła.
 - Ekran autoryzacji przed uruchomieniem nie pojawia się podczas uruchamiania urządzenia.
- Na punkcie końcowym zasyfrowanym hasłem:
 - Hasło zostało usunięte.
 - Wolumin pozostaje niezasyfrowany.
- Zasyfrowany lub niezasyfrowany 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 niezasyfrowany.

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 ???.

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 kliknij **Usuń** .

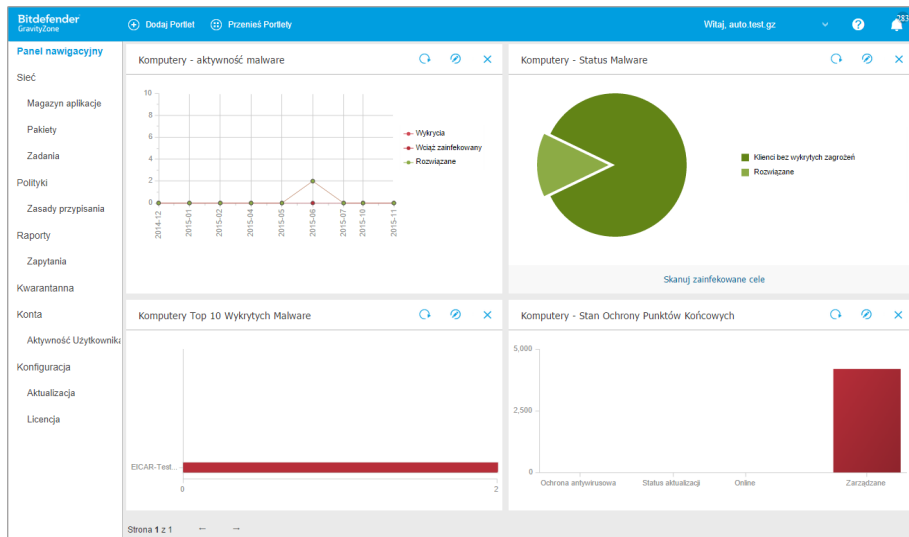
8. MONITOROWANIE PANELU

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. Możesz **edytować** ustawienia portletu, **dodać** 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 roboczego (**Komputery** lub **Maszyny Wirtualne**)
 - 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. 250)

4. W zakładce **Celem** 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

Oto dostępne typy raportów dla maszyn fizycznych i wirtualnych:

Aktywność antyphishingowa

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 trakcie 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.

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

Kliknięcie **Dodaj wykluczenia** dla wybranej detekcji automatycznie utworzy wpis w **Globalne Wykluczenia** w sekcji **Ochrona Sieci**.

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.

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.

Audyt Bezpieczeństwa

Zawiera informacje na temat zdarzeń związanych z bezpieczeństwem, które miały miejsce na wybranym celu. Informacja odnosi się do następujących zdarzeń:

- Wykrywanie Malware
-
-
-
-
- Zdarzenia Network Attack Defense
- Detekcja Ransomware

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.

Stan aktualizacji

Pokazuje status aktualizacji agenta bezpieczeństwa 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.

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.

9.2. Tworzenie raportów

Możesz utworzyć dwie kategorie raportów:


- **Raporty natychmiastowe.** Natychmiastowe raporty są 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.

Stwórz raport ✕

Szczegóły

Typ:

Nazwa: *

Ustawienia

Teraz
 Zaplanowane

Odstępy między raportami:

Pokaż: Wszystkie punkty końcowe
 Tylko punkty końcowe z zablokowanymi stronami

Dostawa: Wyślij e-mailem

Wybierz Cel

Komputery i Maszyny Wirtualne

Wybrano grupy

Opcje Raportowania

4. Wybierz interesujący cię rodzaj raportu z menu. Aby uzyskać więcej informacji, odwołaj się do „[Typy Raportu](#)” (p. 250).
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**.

Nazwa raportu	Typ	Powtarzalność	Pokaż raport
Raport Aktywności Malware	Aktywność Malware	Tygodniowo	22 Sie 2015 - 09:02

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. 261)

Wszystkie raporty składają się z sekcji podsumowania (górną część raportu) i sekcji szczegółów (dolną 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 szczegółów dostarcza informacji o wybranym obiekcie sieciowym.

Notatka

- Aby skonfigurować informacje wyświetlone na wykresie, naciśnij 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 zostaną zmienione 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 sugestywną 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, wszystkie informacje będą dostępne, 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 być 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**.

- Wybierz raport, który chcesz usunąć.
- 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:

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.

10. 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:

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](#)
- [Usuwanie Kart Zgłoszeń](#)
- [Dokonuj ręcznego przesyłania](#)

10.1. 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. 306).
- **wskaznik 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 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.

- **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.

10.2. 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
- Punkt końcowy, który wysłał próbkę do Sandbox Analyzer
- 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 / zakończenia / 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.
- Pozostawianie 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.

10.3. Ponowne przesłanie próbk

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](#)

10.4. 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.

i 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.

10.5. 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.

i 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 jakiegokolwiek innej obsługiwanej przeglądarki internetowej wymienionej w „[Łączenie z Control Center](#)” (p. 13).

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 wiele wirtualnych maszyn jednocześnie gdzie można 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**.

10.6. 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](#)

10.6.1. 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**.

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.

- **Maksymalna 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 opcję.

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.

Tę 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.

10.6.2. 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**.

10.6.3. 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**.

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.

10.6.4. Konfigurowanie i Zarządzanie obrazami WM

Budowanie Maszyn Wirtualnych do detonacji

Aby detonować próbki z wykorzystaniem 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**.

11. 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](#).

Aby zbada zapis aktywności użytkownika, przejdź do strony **Konta > Aktywność użytkownika**.

Uzytkownik	Rola	Akcja	Obszar	Cel	Utworzone
------------	------	-------	--------	-----	-----------

Strona aktywności użytkownika

Aby wyświetlić zapisane wydarzenia, które Cię interesują, musisz zdefiniować wyszukiwanie. Uzupełnij dostępne pola kryteriami wyszukiwania i naciśnij przycisk **Szukaj**. Wszystkie wpisy pasujące do twoich kryteriów zostaną wyświetlone w tabeli.

Kolumny tabeli dostarczają przydatnych informacji na temat wymienionych wydarzeń:

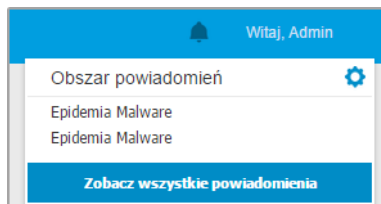
- Nazwa użytkownika, który wykonał akcję.
- Rola użytkownika.
- Akcja, która spowodowała zdarzenie.
- Rodzaj obiektów konsoli na które miała wpływ akcja.
- Określ obiekty konsoli, na które miała wpływ akcja.
- Czas wystąpienia zdarzenia.

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.

12. 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  w prawym górnym rogu Control Center wyświetli liczbę nowych wykrytych zdarzeń. Klikając ikonę wyświetla się Obszar Powiadomień zawierający listę wykrytych zdarzeń.

12.1. 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. 284).

Dostępność formatu Syslog: JSON, CEF

Licencja wygaśa

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 firmy został osiągnięty.

To powiadomienie jest wysyłane, gdy liczba chronionych serwerów osiągnie limit określony na kluczu licencyjnym.

Musisz mieć uprawnienia do **Zarządzania Firmą**, aby zobaczyć to powiadomienie.

Dostępność formatu Syslog: JSON, CEF

Limit wykorzystania licencji serwera został prawie osiągnięty

To powiadomienie jest wysyłane, gdy użyto 90% dostępnych miejsc na licencji dla serwerów.

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 kluczu 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
- 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

Kopia zapasowa bazy danych

To powiadomienie informuje cie o stanie zaplanowanych kopii zapasowych bazy danych, czy są udane czy nie. Jeżeli kopia zapasowa bazy danych nie powiedzie się, powiadomienie wyświetli powód niepowodzenia.

Dla uzyskania szczegółów na temat konfiguracji bazy danych kopii zapasowych GravityZone, zapoznaj się z Podręcznikiem Instalacyjnym GravityZone.

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

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

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

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

Integracja Out of Sync

To powiadomienie informuje o problemach z integracją i nie można ich już synchronizować. Może się tak zdarzyć z powodu różnych czynników, takich jak szczegóły integracji, które uległy zmianie, lub tymczasowa niedostępność serwera.

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

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 urządzenie 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

12.2. Zobacz powiadomienia

Aby zobaczyć powiadomienia naciśnij przycisk  **Powiadomienia** i naciśnij **Zobacz wszystkie powiadomienia**. Wyświetlana jest tabela zawierająca wszystkie powiadomienia.

Typ	Utworzone
Epidemia Malware	4 Cze 2015, 18:09:21

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 się pod tabelą.

12.3. 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** 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. 284).

12.4. 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.

Powiadomienie	Widoczność
<input checked="" type="checkbox"/> Epidemia Malware	<input checked="" type="checkbox"/> Pokaż w Control Center
<input checked="" type="checkbox"/> Licencja wygasa	<input type="checkbox"/> Wyślij e-mailem
<input checked="" type="checkbox"/> Limit wykorzystania licencji został o...	
<input checked="" type="checkbox"/> Limit wykorzystania licencji został pr...	
<input checked="" type="checkbox"/> Aktualizacja dostępna	
<input checked="" type="checkbox"/> Połączenie z Internetem	
<input checked="" type="checkbox"/> Połączenie SMTP	
<input checked="" type="checkbox"/> Użytkownicy urządzeń mobilnych b...	
<input checked="" type="checkbox"/> Kopia zapasowa bazy danych	

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. 277). 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 `syslog`.
Aby dowiedzieć się w jaki sposób konfigurować serwery `syslog`, zapoznaj się z Podręcznikiem Instalacyjnym GravityZone.
- **Wyślij przez e-mail** określa rodzaje zdarzeń jakie są wysyłane na określone adresy e-mail. W tym przypadku, wymaga podania adresu e-mail w odpowiednim polu, naciśnij **Enter** po każdym adresie.

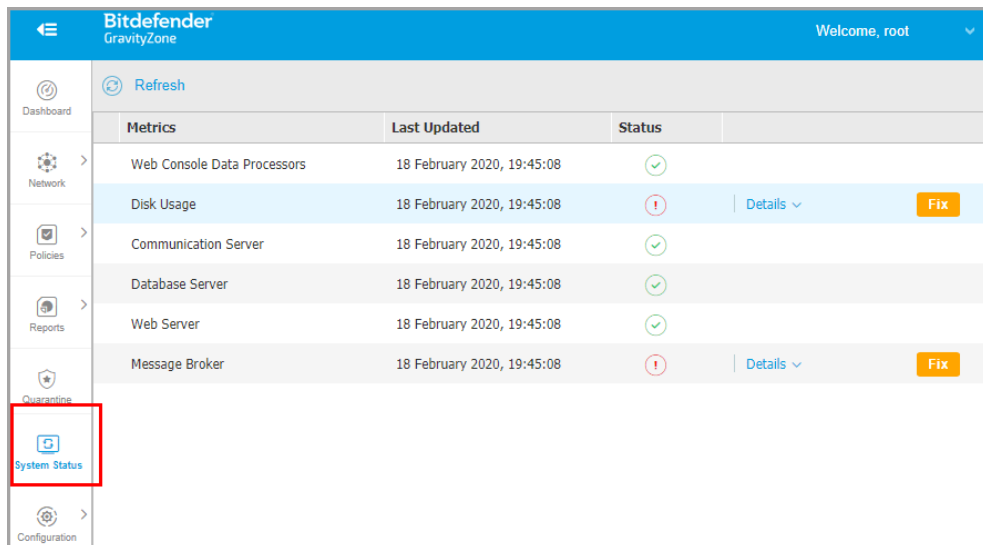
Konfiguracja

- **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 opcję **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 **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**.

13. 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 formie siatki.






	Metrics	Last Updated	Status	
Network	Web Console Data Processors	18 February 2020, 19:45:08	OK	
	Disk Usage	18 February 2020, 19:45:08	Warning	Details Fix
Policies	Communication Server	18 February 2020, 19:45:08	OK	
	Database Server	18 February 2020, 19:45:08	OK	
Reports	Web Server	18 February 2020, 19:45:08	OK	
	Message Broker	18 February 2020, 19:45:08	Warning	Details Fix


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. 308).


Kolumna **Ostatnio Zaktualizowane** wyświetla datę i czas ostatniego sprawdzania statusu metryki.

Kolumna **Status** wyświetla stan każdej metryki:  **OK** lub  **Uwaga**. Metryka **Status** jest aktualizowana co każde 15 minut lub za każdym razem gdy klikniesz  **Odśwież**.

13.1. Status OK


Status OK  wskazuje, że metryka zachowuje się normalnie. W tym przypadku żadne dodatkowe informacje nie są wyświetlane.

13.2. 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.

Refresh			
Metrics	Last Updated	Status	
Database Server	09 October 2019, 08:47:08		Details ^
Appliance	Details		
10.17.44.111	The service is inactive since Wed 2019-10-09 08:46:52 UTC; 13s ago		

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.

Database Server		Details ^	Fix
Appliance	Details		
10.17.43.29	The service is inactive since Mon 2020-02-17 16:09:29 UTC; 5min ago		

Szczegóły Metryki

Status metryki wróci na  **OK** jak zostanie naprawiona.



Notatka

W przypadku innych problemów związanych z metrykami skontaktuj się w [Centrum Wsparcia Biznesowego](#).

13.3. 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 kompletnej liście procesorów używanych przez Control Center odnieś się do „Procesory Danych” (p. 308).

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 urządzeniami zostało przerwane.
Urządzenie wirtualne jest wyłączone	Wirtualne urządzenie używające tej usługi jest wyłączone.

14. UZYSKIWANIE POMOCY

Bitdefender stara się zapewnić swoim klientom najwyższy poziom szybkiej i dokładnej pomocy technicznej. Jeżeli męczą 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.

14.1. 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 dostępna 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.

14.2. Prośba o pomoc

Możesz poprosić o pomoc za pośrednictwem naszego Centrum Wsparcia Online. Wypełnij [formularz kontaktowy](#) i wyślij go do nas.

14.3. 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.

14.3.1. 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 lokalacji 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 lokalację 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 lokalacji i znajdź archiwum o nazwie ST_[computername]_[currentdate]. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

14.3.2. 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 chcesz 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

14.3.3. 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.

14.4. Informacje o produkcji

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 jakiegokolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

14.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com

C e n t r u m

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 Spam: spam_submission@bitdefender.com

Raportowanie Abuse: abuse@bitdefender.com

Strona: <http://www.bitdefender.com>

14.4.2. 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.

14.4.3. 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; 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
	Maszyna wirtualna
	Wirtualna maszyna Relay
	Złoty obraz
	Nutanix Inventory
	Nutanix Prism
	Klaster Nutanix
	VMware inventory
	VMware vCenter
	Centrum danych VMware
	Pula zasobów VMware
	Klaster VMware
	Citrix Inventory
	XenServer
	Xen Pool
	Inwentarz Amazon EC2
	Integracja Amazon EC2
	Region Amazon EC2 / Microsoft Azure

Ikona	Typ
	Strefa Dostępności Amazon EC2 / Microsoft Azure
	Microsoft Azure inventory
	Integracja Microsoft Azure
	VMware vApp









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 następniej tabeli znajdziesz wszystkie dostępne statusy ikon i ich opisy.



Notatka

Tabela 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
	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. 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.5. Obiekty Sandbox Analyzer

A.5.1. 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.5.2. 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, pscl, 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.5.3. Domyślne Wykluczenia przy Automatycznym Wysyłaniu

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgg, png, txt.

A.5.4. 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
Mozilla Thunderbird Microsoft Outlook	eml

A.6. Procesory Danych

Nazwa	Szczegóły
Przekazujący Żądanie Procesora	Przekazuje zapytania procesora w rozproszonych środowiskach
VMware Hypervision Integrator	Synchronizuje VMware inventory i inne informacje z GravityZone
Citrix Hypervisor Integrator	Synchronizuje Xen inventory i inne informacje z GravityZone

Nazwa	Szczegóły
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
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

Nazwa	Szczegóły
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
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 kliknięcia. 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. Choć 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 przedsięwzięcia, będące próbą 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 zrekompileowanych 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 ułamki 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 szkodenia 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 zawierają 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 najmniejbezpiecznych 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 uruchamiać 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.