Bitdefender®

GravityZone

INSTRUKCJA INSTALACJI

Bitdefender GravityZone
Instrukcja Instalacji

Data publikacji 2021.01.15

Notka prawna

Spis treści

Wstęp

Przewodnik służy Partnerom Bitdefender, którzy dostarczają GravityZone jako usługę ochrony dla swoich klientów. Przewodnik jest zaprojektowany dla Administratorów IT zajmujących się ochroną sieci w swojej firmie oraz swoich klientów.

Te dokumenty służą pomocą przy wdrożeniu agentów ochrony Bitdefender na wszystkich rodzajach punktów końcowych w zarządzanych firmach, oraz jak skonfigurować rozwiązanie GravityZone.

1. Znaki umowne stosowane w przewodniku

Konwencje Typograficzne

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

Wygląd	Opis
`wzorzec`	Zgodne nazwy poleceń i składnia ścieżki, nazwy plików, konfiguracja punktu wejścia i wyjścia dla wyświetlanego tekstu są drukowane przy `stałej szerokości` znaków.
http://www.bitdefender.com	Nawiązania (linki) URL odnoszą do innych miejsc takich jak serwery http czy ftp.
gravityzone-docs@bitdefender.com	Adresy Email zostały umieszczone w tekście dla informacji kontaktowych.
„Wstęp” (p. vi)	To odnośnik do linka wewnętrznego umiejscowionego w dokumencie.
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, są to notatki graficznie wyróżnione, zwracające Państwa uwagę na dodatkowe informacje odnoszące się do aktualnego paragrafu.

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

WAŻNE
Ten znak wymaga Państwa uwagi i jego pomijanie nie jest zalecane. 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 jednym produktem z ujednoliconą konsolą zarządzania dostępną w chmurze, której gospodarzem jest Bitdefender lub jednym wirtualnym urządzeniem instalowanym w siedzibie firmy i stanowi jeden punkt wdrażania, egzekwowania i zarządzania zasadami zabezpieczeń dla dowolnej liczby urządzeń końcowych i dowolnego typu w dowolnym miejscu.

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

2. GRAVITYZONE WARSTWY OCHRONNE

GravityZone udostępnia następujące warstwy ochrony:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- HyperDetect
- Zaawansowany Anty-Exploit
- Zapora Sieciowa
- Kontrola Zawartości
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne Szyfrowanie Dysku
- Security for Exchange
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Analityka Ryzyka Punktu Końcowego (ERA)
- Email Security

2.1. Antymalware

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

Technologia skanowania antymalware Bitdefender opiera się na następujących warstwach ochrony:

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

środowisku wirtualnym, aby sprawdzić jego wpływ na system i upewnić się, że nie stanowi zagrożenia. Jeśli zagrożenie zostało wykryte, uniemożliwione jest uruchomienie programu.

Silniki Skanowania

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

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

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

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

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

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

2.2. Zaawansowana Kontrola Zagrożeń

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

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

2.3. HyperDetect

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

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

2.4. Zaawansowany Anty-Exploit

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

2.5. Zapora Sieciowa

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

2.6. Kontrola Zawartości

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

2.7. Network Attack Defense

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

2.8. Zarządzanie Aktualizacjami

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

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

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

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

2.9. Kontrola Urządzenia

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

2.10. Pełne Szyfrowanie Dysku

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

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

2.11. Security for Exchange

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

WAŻNE
Security for Exchange ma za zadanie chronić całą organizację Exchange, do której należy chroniony serwer Exchange. Oznacza to, że chroni wszystkie aktywne skrzynki pocztowe, w tym użytkownika/pokój/sprzęt/współdzielone skrzynki pocztowe.

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

2.12. Sandbox Analyzer

Bitdefender Sandbox Analyzer zapewnia potężną warstwę ochrony przeciwko zaawansowanym zagrożeniom działającą automatycznie, dzięki dogłębnej analizie podejrzanych plików, które nie są jeszcze podpisane przez silniki skanowania Bitdefender. Sandbox wykorzystuje zestaw rozszerzonych technologii Bitdefendera aby detonować złośliwe oprogramowanie w izolowanym środowisku wirtualnym utrzymywanym przez Bitdefender, analizując ich zachowanie i raportując drobne zmiany, które wskazują na złośliwe intencje.

Sandbox Analyzer automatycznie zgłasza podejrzane pliki, ukryte dla usług antywirusowych opartych na sygnaturach, znajdujące się na zarządzanych punktach końcowych. Dedykowana heurystyka osadzona w module dostępowym Antimalware z Bitdefender Endpoint Security Tools uruchamia proces wysyłania.

Usługa Sandbox Analyzer jest w stanie zapobiec uruchamianiu nieznanych zagrożeń w punkcie końcowym. Działa w trybie monitorowania lub blokowania, umożliwiając lub odmawiając dostępu do podejrzanego pliku do czasu otrzymania werdyktu. Sandbox Analyzer automatycznie rozwiązuje wykryte zagrożenia zgodnie z działaniami naprawczymi określonymi w polityce bezpieczeństwa dla systemów, których dotyczy problem.

Dodatkowo, Sandbox Analyzer pozwala na ręczne przesłać próbki bezpośrednio z Control Center pozwalając Tobie zdecydować, co dalej z nimi zrobić.

WAŻNE
Manualne zgłoszenie jest dostępne dla użytkowników GravityZone z uprawnieniem **Zarządzaj Sieciami**

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

2.13. Endpoint Detection and Response (EDR)

Endpoint Detection and Response to komponent korelacji incydentów, zdolny do identyfikowania zaawansowanych zagrożeń lub ataków w toku. W ramach naszej kompleksowej i zintegrowanej Platformy Ochrony Punktów Końcowych, EDR łączy inteligencję urządzeń w całej sieci przedsiębiorstwa. To rozwiązanie jest pomocne w wysiłkach zespołów reagujących na incydenty, które mają na celu zbadanie i reagowanie na zaawansowane zagrożenia.

Poprzez Bitdefender Endpoint Security Tools można aktywować moduł ochrony o nazwie Czujnik EDR na zarządzanych punktach końcowych, aby zebrać dane sprzętu i systemu operacyjnego. Metadane są gromadzone i przetwarzane po obu stronach struktury klient-serwer.

Ten komponent dostarcza szczegółowych informacji o wykrytych incydentach, interaktywnej mapie incydentów, działaniach naprawczych i integracji z Sandbox Analyzer i HyperDetect.

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

2.14. Analityka Ryzyka Punktu Końcowego (ERA)

Analityki Ryzyka punktu końcowego (ERA) identyfikuje, ocenia i usuwa słabości punktów końcowych z Windows poprzez skanowanie ryzyka bezpieczeństwa (na żądanie lub zaplanowane przez politykę), biorąc pod uwagę ogromną liczbę wskaźników ryzyka. Po zeskanowaniu sieci przy użyciu pewnych wskaźników ryzyka, uzyskasz przegląd stanu ryzyka sieciowego za pomocą pulpitu nawigacyjnego **Zarządzanie ryzykiem** , dostępnego w menu głównym. Będziesz mógł automatycznie rozwiązać pewne zagrożenia bezpieczeństwa z GravityZone Control Center i zobaczyć zalecenia dotyczące łagodzenia narażeń punktu końcowego

2.15. Email Security

Przez Email Security możesz kontrolować dostarczanie email, filtrowanie wiadomości i stosować polityki w całej firmie by powstrzymać wyrafinowane, wycelowane zagrożenia email, wliczając Business Email Compromise (BEC) i CEO fraud. cloud_email_sec] wymaga obsługi kont by zyskać dostęp do konsoli. Po więcej informacji odnieś się do Bitdefender Email Security Podręcznika Użytkownika

2.16. 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 GravityZone Dostępność Warstw Ochrony .

3. ARCHITEKTURA GRAVITYZONE

Rozwiązanie GravityZone zawiera następujące składniki:

- Konsola Webowa (Control Center)
- Security Server
- Agenci Bezpieczeństwa

3.1. Konsola Web (GravityZone Control Center)

Control Center interfejs oparty na przeglądarce integruje się z istniejącym systemem zarządzania i monitoringu systemu co upraszcza nam automatyczne zastosowanie ochrony na niezarządzanych stacjach i serwerach.

3.2. Security Server

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

Notatka
Twoja licencja produktu może nie zawierać tej funkcji.

Security Server musi być zainstalowany na jednym lub kilku hostach tak, aby pomieścić wiele chronionych maszyn wirtualnych.

3.3. 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

3.3.1. Bitdefender Endpoint Security Tools

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

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

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

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

Warstwy bezpieczeństwa

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

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- HyperDetect
- Zapora Sieciowa
- Kontrola Zawartości
- Network Attack Defense
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne Szyfrowanie Dysku
- Security for Exchange
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Analityka Ryzyka Punktu Końcowego (ERA)

Role Punktów Końcowych

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

Power User

Administratorzy Control Center mogą przyznawać prawa Power User użytkownikom punktów końcowych poprzez ustawienia polityk. Moduł Power User umożliwia uprawnienia administratora na poziomie użytkownika, umożliwiając użytkownikowi

dostęp do punktów końcowych i modyfikację ustawień zabezpieczeń za pomocą lokalnej konsoli. Control Center jest powiadamiana, gdy punkt końcowy jest w trybie Power User i administrator Control Center zawsze może nadpisać ustawienia lokalnych zabezpieczeń.

WAŻNE
Moduł ten jest dostępny wyłącznie dla komputerów stacjonarnych i serwerów obsługiwanych systemów operacyjnych Windows. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 20).

Relay

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

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

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

Agenci Bitdefender Endpoint Security Tools Relay służą do następujących czynności:

- Wykrywanie wszystkich niezabezpieczonych punktów końcowych w sieci.

  Funkcjonalność ta jest niezbędna do wdrażania agenta bezpieczeństwa w środowisku chmury GravityZone.
- Wdrażanie agenta endpoint w sieci lokalnej.
- Aktualizacja chronionych punktów końcowych w sieci.
- Zapewnienie komunikacji pomiędzy Control Center i podłączonymi punktami końcowymi.
- Działa jako serwer proxy dla chronionych punktów końcowych.
- Optymalizowanie ruchu sieciowego podczas aktualizacji, wdrożenia, skanowania i innych konsumujących zasoby zadań.

Serwerów Buforowania Łatek

Punkty końcowe z rolą Relay mogą również działać jako Serwer Buforowania Aktualizacji. Po włączeniu tej roli, Relay służą do przechowywania aktualizacji oprogramowania pobranych ze stron internetowych dostawców i dystrybuowania ich do docelowych punktów końcowych w sieci. Kiedy podłączony punkt końcowy ma oprogramowanie z brakującymi aktualizacjami, pobiera je z serwera, a nie ze strony internetowej producenta, optymalizując w ten sposób generowany ruch i obciążenie sieci.

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

Ochrona Exchange

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

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

3.3.2. Endpoint Security for Mac

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

Warstwy bezpieczeństwa

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

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Kontrola Zawartości
- Kontrola Urządzenia
- Pełne Szyfrowanie Dysku

3.4. Architektura Sandbox Analyzer

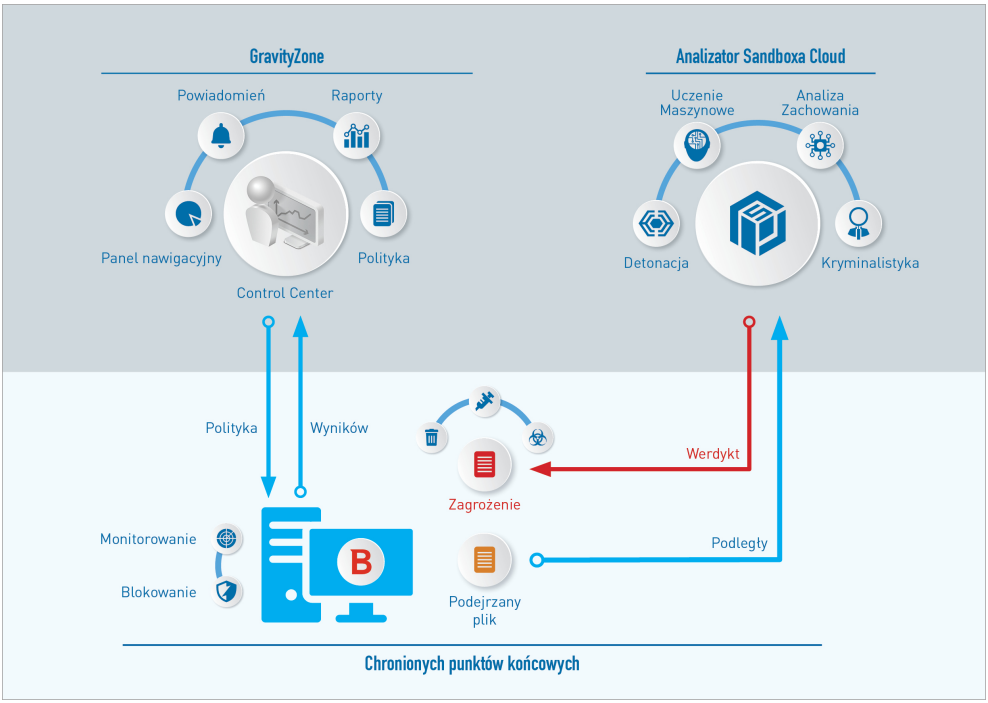
Bitdefender Sandbox Analyzer zapewnia potężną warstwę ochrony przed zaawansowanymi zagrożeniami, wykonując automatyczną, szczegółową analizę podejrzanych plików, które jeszcze nie zostały podpisane przez silniki antimalware Bitdefender.

Sandbox Analyzer zawiera następujące komponenty:

- **Sandbox Analyzer Portal**. Ten komponent jest hostowanym serwerem komunikacyjnym używanym do obsługi żądań między punktami końcowymi a klastrem sandbox Bitdefender.
- **Sandbox Analyzer Klaster**. Ten komponent jest hostowaną infrastrukturą sandbox, w której zachodzi przykładowa analiza behawioralna. Na tym poziomie przesłane pliki są detonowane na maszynach wirtualnych z systemem Windows 7.

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

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



Architektura Sandbox Analyzer

Po aktywacji usługi Sandbox Analyzer z Control Center na punktach końcowych:

1. Agent bezpieczeństwa Bitdefender rozpoczyna przesyłanie podejrzanych plików odpowiadających regułom ochrony określonym w zasadach.
2. Po przeanalizowaniu pliku, odpowiedź jest odsyłana do Portalu, a następnie do punktu końcowego.
3. Jeśli plik zostanie wykryty jako niebezpieczny, użytkownik zostaje powiadomiony i podejmowane są działania naprawcze.

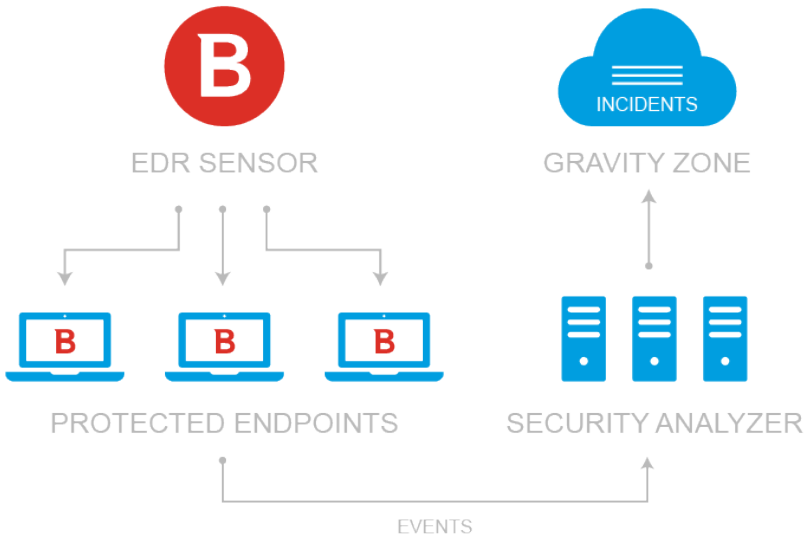
Wyniki analizy zachowywane są w bazie Sandbox Analyzer z zapisanym hashem pliku. Gdy poprzednio analizowany plik jest przesyłany z innego punktu końcowego, odpowiedź jest natychmiast odsyłana, ponieważ wyniki są już dostępne w bazie danych.

3.5. Architektura EDR

Aby zidentyfikować zaawansowane zagrożenia i ataki w toku, EDR potrzebuje danych dotyczących sprzętu oraz jego systemu operacyjnego. Niektóre z surowych danych są przetwarzane lokalnie, a algorytmy uczenia maszynowego w Security Analytics wykonują bardziej złożone zadania.

EDR zawiera dwa główne komponenty:

- Sensor incydentów, który zbiera dane procesów i raportuje zachowanie punktów końcowych i aplikacji.
- Analityka Bezpieczeństwa, część zestawu technologii Bitdefender używanych do interpretowania metadanych zebranych przez Incydent Sensorów.



Przepływ EDR z punktu końcowego do Centrum Kontroli

4. WYMAGANIA

Wszystkie rozwiązania GravityZone są instalowane i zarządzane przez Control Center.

4.1. Control Center

Dostęp do konsoli webowej Control Center, wymagane jest co następuje:

- 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.

4.2. Ochrona Punktu Końcowego

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować agentów bezpieczeństwa GravityZone na punktach końcowych sieci. W tym celu, potrzebujesz użytkownika z prawami administracyjnymi Control Center nad usługami jakie potrzebujesz zainstalować i nad punktami końcowymi sieci, którą zarządzasz.

Wymagania dla agenta bezpieczeństwa są różne, w zależności od tego, czy ma dodatkowe role serwera, takie jak Relay, Ochrona Exchange lub Serwer pomocniczy zarządzania aktualizacjami. W celu uzyskania większej ilości informacji na temat ról agenta, zobacz „Agenci Bezpieczeństwa” (p. 9).

4.2.1. Sprzęt komputerowy

Agent bezpieczeństwa bez ról

Użycie procesora

Docelowe systemy	Typ procesora	Wspierane systemy operacyjne (OS)
Stacje robocze	Procesory kompatybilne z Intel® Pentium, 2 GHz bądź szybsze	Systemy Operacyjne Microsoft Windows
	Intel® Core 2 Duo, 2 GHz lub szybszy	macOS
Inteligentne Urządzenia	Procesory kompatybilne z Intel® Pentium, 800 MHZ lub szybsze	Systemy osadzone Microsoft Windows
Serwery	Minimum: procesory kompatybilne z Intel® Pentium, 2.4 GHz	Systemy operacyjne Microsoft Windows Server i Linux
	Rekomendowane: procesory wielordzeniowe Intel® Xeon, 1.86 GHz lub szybsze	

Ostrzeżenie
Procesory ARM obecnie nie są wspierane.

Wolna pamięć RAM

Podczas instalacji (MB)

OS	POJEDYNCZY SILNIK					
	Skan. Lokalne		Skan. Hybrydowe		Scentraliz. Skan.	
	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	n/d	n/d	n/d	n/d

Do codziennego użycia (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokalny	Hybryda	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serwer Aktual.
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* Pomiar pokrycia dziennego użycia klientów punktów końcowych, bez brania pod uwagę dodatkowych zadań, takich jak skanowanie na żądanie lub aktualizacje produktu.

Wolna przestrzeń dyskowa

Podczas instalacji (MB)

OS	POJEDYNCZY SILNIK						PODWÓJNY SILNIK			
	Skan. Lokalne		Skan. Hybrydowe		Scentraliz. Skan.		Scentraliz. + Lokalne Skan.		Scentraliz. + Hybrydowe Skan.	
	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/d	n/d	n/d	n/d	n/d	n/d	n/d	n/d

Do codziennego użycia (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokalny	Hybryda	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serwer Aktual.
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* Pomiar pokrycia dziennego użycia klientów punktów końcowych, bez brania pod uwagę dodatkowych zadań, takich jak skanowanie na żądanie lub aktualizacje produktu.

Agent bezpieczeństwa z rolą relay

Rola relay wymaga dodatkowych zasobów sprzętowych w porównaniu z podstawową konfiguracją agenta bezpieczeństwa. Wymagania te dotyczą obsługi serwera aktualizacji i pakietów instalacyjnych obsługiwanych przez punkt końcowy:

Ilość podłączonych punktów końcowych	CPU wspierający serwer aktualizacji	RAM	Wolna przestrzeń dyskowa dla serwera aktualizacji
1-300	minimum to procesor Intel® Core™ i3 bądź równoważny, 2 vCPU na rdzeń	1.0 GB	10 GB
300-1000	minimum to procesor Intel® Core™ i5 bądź równoważny, 4 vCPU na rdzeń	1.0 GB	10 GB

Ostrzeżenie

- Procesory ARM obecnie nie są wspierane.
- Agenci Relay wymagają dysków SSD, aby obsługiwać dużą liczbę operacji odczytu / zapisu.

WAŻNE

- Jeśli chcesz zapisać pakiety instalacyjne i aktualizacje na innej partycji niż ta, w której zainstalowany jest agent, upewnij się, że obie partycje mają wystarczającą ilość wolnego miejsca na dysku (10 GB), w przeciwnym razie agent przerwie instalację. Jest to konieczne tylko podczas instalacji.
- W punktach końcowych Windows muszą być włączone linki symboliczne lokalne do lokalnych

Agent Bezpieczeństwa z Rolą Ochrony Exchange

Kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni dyskowej na partycji gdzie zainstalowano agenta bezpieczeństwa.

Rozmiar kwarantanny zależy od liczby elementów przechowywanych oraz ich wielkości.

Domyślnie, agent jest instalowany na systemowej partycji.

Agent bezpieczeństwa z funkcją serwera pomocniczego aktualizacji łatek.

Agent z rolą serwera pomocniczego łatek musi spełniać następujące wymagania zbiorcze:

- Wszystkie wymagania sprzętowe pojedynczego agenta bezpieczeństwa (bez ról).
- Wszystkie wymagania sprzętowe dla roli Relay.
- Dodatkowo 100 GB wolnej przestrzeni dyskowej dla składowania ściągniętych łatek

WAŻNE
Jeśli chcesz zapisać poprawki na innej partycji niż ta, na której zainstalowany jest agent, upewnij się, że obie partycje mają wystarczającą ilość wolnego miejsca na dysku (100 GB), w przeciwnym razie agent przerwie instalację. Jest to konieczne tylko podczas instalacji.

4.2.2. Wspierane systemy operacyjne

system Windows w wersji na komputery stacjonarne

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Aktualizacja Windows 10 z 10 październik 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)

- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Ostrzeżenie
Bitdefender nie obsługuje Windows Insider Program builds.

Windows Tablet and Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Serwer

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Linux

WAŻNE
Punkty końcowe Linux używają miejsc licencji z puli licencji dla systemów operacyjnych serwera.

- Ubuntu 14.04 LTS lub wyższy
- Red Hat Enterprise Linux / CentOS 6.0 lub wyżej(2)
- SUSE Linux Enterprise Server 11 SP4 lub wyższy
- OpenSUSE Leap 42.x
- Fedora 25 lub wyższy(1)
- Debian 8.0 lub wyższy
- Oracle Linux 6.3 lub nowszy
- Amazon Linux AMI 2016.09 lub nowszy
- Amazon Linux 2

Ostrzeżenie
(1) W Fedora 28 i wyżej, Bitdefender Endpoint Security Tools wymaga ręcznej instalacji pakietu `libnsl`, uruchamiając następujące polecenie:

```
sudo dnf install libnsl -y
```

(2) Dla minimalnych instalacji CentOS Bitdefender Endpoint Security Tools wymaga ręcznej instalacji pakietu `libnsl` poprzez następujące polecenie:

```
sudo yum install libnsl
```

Wymagania Active Directory

Gdy integrujesz punkty końcowe z Linux z domeną Active Directory przez System Security Services Daemon (SSSD) upewnij się, że narzędzia **ldbsearch, krb5-user,** and **krb5-config** są zainstalowane i kerberos jest poprawnie skonfigurowany.

```
/etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
```

```
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = DOMAIN.NAME
        dns_lookup_realm = true
        dns_lookup_kdc = true
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        fcc-mit-ticketflags = true
        default_keytab_name = FILE:/etc/krb5.keytab

[realms]
        DOMAIN.NAME = {
                        kdc = dc1.domain.name
                        kdc = dc2.domain.name
                        admin_server = dc.domain.com
                        default_domain = domain.com
        }

[domain_realm]
 domain.name = DOMAIN.NAME
 .domain.name = DOMAIN.NAME

[appdefaults]
 pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

Notatka
We wszystkich wpisach rozróżniane są wielkie i małe litery.

Wsparcie skanowania Dostępowego

Skanowanie dostępowe jest dostępne dla wszystkich gościnnych systemów operacyjnych. Na systemach Linux, skanowanie dostępowe jest dostarczane w następujących sytuacjach:

Wersje Jądra	Dystrybucje Linux	Wymagania Dostępowe
2.6.38 lub wyższe*	Red Hat Enterprise Linux / CentOS 6.0 lub wyżej Ubuntu 14.04 lub wyższy SUSE Linux Enterprise Server 11 SP4 lub wyższy OpenSUSE Leap 42.x Fedora 25 lub wyższy Debian 9.0 lub wyższy Oracle Linux 6.3 lub nowszy Amazon Linux AMI 2016.09 lub nowszy	Opcja jądra **fanotify** musi być włączona.
2.6.38 lub wyższe	Debian 8	**Fanotify** musi być włączone i ustawione na tryb egzekwowania, a następnie pakiet jądra musi zostać przebudowany. Więcej szczegółów znajdziesz w tym artykule KB.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender zapewnia wsparcie poprzez **DazukoFS** z prekombilowanymi modułami jądra.
Wszystkie inne jądra	Wszystkie inne obsługiwane systemy plików	Moduł **DazukoFS** musi zostać skompilowany ręcznie. Aby uzyskać więcej informacji, odwołaj się do „Ręcznie skompiluj moduł DazukoFS.” (p. 57).

* Z pewnymi ograniczeniami opisanymi poniżej.

Ograniczenia Skanowania Dostępowego

Wersje Jądra	Dystrybucje Linux	Szczegóły
2.6.38 lub wyższe	Wszystkie wspierane systemy	Monitory skanowania dostępowego montowały udziały sieciowe tylko w tych warunkach: • **Fanotify** jest włączone zarówno w systemach zdalnych, jak i lokalnych. • Udział jest oparty na systemach plików CIFS i NFS. **Notatka** Skanowanie dostępowe nie skanuje udziałów sieciowych podłączonych za pomocą SSH lub FTP.
Wszystkie jądra	Wszystkie wspierane systemy	Skanowanie dostępowe nie jest obsługiwane w systemach z **DazukoFS** dla udziałów sieciowych zamontowanych na ścieżkach już chronionych przez moduł dostępowy.

Obsługa Endpoint Detection and Response (EDR)

Przejdź do tej strony internetowej , aby uzyskać pełną i aktualną listę wersji jądra i dystrybucji Linuksa, które obsługują Sensor EDR.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Kontrola Zawartości nie jest wspierana w macOS Big Sur (11.0).

4.2.3. Obsługiwane systemy plików

Bitdefender instaluje się na i chroni następujące systemy plików:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

Notatka
Skanowanie dostępowe nie wspiera NFS i CIFS/SMB.

4.2.4. Obsługiwane przeglądarki

Przeglądarka bezpieczeństwa Endpoint jest weryfikowana do pracy z następującymi przeglądarkami:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.2.5. Security Server

Security Server jest wstępnie skonfigurowaną wirtualną maszyną działającą na Ubuntu Server 12.04 LTS (3.2 kernel).

Notatka
Twoja licencja produktu może nie zawierać tej funkcji.

Platformy Wirtualizacji

Bitdefender Security Server może zostać zainstalowany na następujących platformach wirtualizacyjnych:

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

  Notatka
  Funkcja Zarządzania Obciążeniem w vSphere 7.0 nie jest obsługiwana.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- Stacje robocze VMware 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (włączając Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp i XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 lub Windows Server 2008 R2, 2012, 2012 R2 (zawierający Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (zawierający KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism z AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism z AOS 5.6, 5.11 STS
- Nutanix Prism z AHV 20170830.115, 20170830.301 i 20170830.395 Community Edition
- Nutanix Prism wersja 2018.01.31 (Community Edition)

Notatka
Wsparcie dla innych platform wirtualizacji może być dostarczone na życzenie.

Pamięć i Procesor

Przydział zasobów pamięci i procesora dla Security Server zależy od liczby i rodzaju maszyn wirtualnych uruchomionych na hoście. Poniższa tabela zawiera zalecane zasoby, które mają być przyznane:

Liczb chronionych VMs	RAM	CPU
1-50 maszyn wirtualnych	2 GB	2 CPU
51-100 maszyn wirtualnych	2 GB	4 CPU
101-200 maszyn wirtualnych	4 GB	6 CPU

Miejsce na dysku twardym

Musisz mieć 8 GB miejsca na dysku na każdym hoście Security Server.

Security Server Dystrybucja na Hostach

Chociaż nie jest to obowiązkowe, Bitdefender rekomenduje zainstalowanie Security Server na każdym fizycznym hoście w celu poprawy wydajności.

Opóźnienie Sieciowe

Opóźnienie komunikacji między Security Server a chronionymi punktami końcowymi musi być mniejsze niż 50 ms.

Obciążenie Ochrony Pamięci Masowej

4.2.6. Wykorzystanie Ruchu

- **Ruch aktualizacji produktu pomiędzy punktem końcowym klienta a serwerem aktualizacji**

  Każda periodyczna aktualizacja produktu Bitdefender Endpoint Security Tools podczas pobierania generuje następujący ruch dla każdego klienta punktu końcowego:

  – Dla systemu operacyjnego Windows: ~20 MB

  – Dla systemu operacyjnego Linux: ~26 MB

  – On macOS: ~25 MB

- **Pobrany ruch aktualizacji zawartości zabezpieczeń między klientem punktu końcowego a serwerem aktualizacji (MB/dzień)**

Typ Serwera Aktualizacji	Typ Silnika Skanowania		
	Lokalny	Hybryda	Scentraliz.
Relay	65	58	55
Bitdefender publiczny serwer aktualizacji	3	3.5	3

- **Ruch Centralnego Skanowania pomiędzy klientem punktu końcowym i Security Server**

Przeskanowane Obiekty	Typ Ruchu		Pobrano (MB)	Przesłano (MB)
Pliki*	Pierwsze skanowanie		27	841
	Skanowanie buforowane		13	382
Strony internetowe**	Pierwsze skanowanie	Ruch sieciowy	621	Niedostępny
		Security Server	54	1050
	Skanowanie buforowane	Ruch sieciowy	654	Niedostępny
		Security Server	0.2	0.5

* Dostarczone dane zostały zmierzone na 3.49 GB plików (6'658 plików), z których 1.16 GB to przenośne pliki wykonywalne (PE).

** Dostarczone dane zostały wyliczone z najwyższych pozycji rankingów 500 stron internetowych.

- **Ruch hybrydowego skanowania pomiędzy klientem punktu końcowego a Usługą Chmury Bitdefender**

Przeskanowane Obiekty	Typ Ruchu	Pobrano (MB)	Przesłano (MB)
Pliki*	Pierwsze skanowanie	1.7	0.6
	Skanowanie buforowane	0.6	0.3
Ruch sieciowy**	Ruch sieciowy	650	Niedostępny
	Usługi w Chmurze Bitdefender	2.6	2.7

* Dostarczone dane zostały zmierzone na 3.49 GB plików (6'658 plików), z których 1.16 GB to przenośne pliki wykonywalne (PE).

** Dostarczone dane zostały wyliczone z najwyższych pozycji rankingów 500 stron internetowych.

Notatka
Letencja sieciowa pomiędzy klientem punktu końcowego i Serwerem Chmury Bitdefender muszi wynosić poniżej 1 sekundy.

- **Ruch między klientami Bitdefender Endpoint Security Tools Relay a serwerem aktualizacji do pobierania zawartości zabezpieczeń**

  Klient z rolą Bitdefender Endpoint Security Tools Relay pobiera ~16 MB / na dzień* z serwera aktualizacji.

  * Dostępne wraz z klientem Bitdefender Endpoint Security Tools zaczynając od wersji 6.2.3.569.

- **Ruch pomiędzy klientami punktów końcowych i konsolą webowoą Control Center**

  przeciętny ruch to 618 KB / dzień jest generowany pomiędzy punktem końcowym klienta i webowej konsoli Control Center.

4.3. Ochrona Exchange

Security for Exchange jest dostarczany przez Bitdefender Endpoint Security Tools, który jest w stanie chronić zarówno system plików jak i serwer pocztowy Microsoft Exchange.

4.3.1. Obsługiwane Środowiska Microsoft Exchange

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2019 z rolą Edge Transport lub Mailbox
- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox
- Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox

Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG).

4.3.2. Wymagania systemowe

Security for Exchange jest kompatybilny z dowolnym fizycznym lub wirtualnym 64- bitowym serwerem (Intel lub AMD) uruchamiając obsługiwaną wersję serwera Microsoft Exchange i rolę. Aby uzyskać więcej informacji na temat wymagań systemowych Bitdefender Endpoint Security Tools, odwołaj się do „Agent bezpieczeństwa bez ról” (p. 17).

Zalecana dostępność zasobów serwera:

- Wolna pamięć RAM: 1 GB
- Wolne miejsce na dysku: 1 GB

4.3.3. Inne Wymagania Oprogramowania

- Dla Microsoft Exchange Server 2013 z Service Pack 1: KB2938053 od Microsoft.
- Dla Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 lub wyższy

4.4. Pełne Szyfrowanie Dysku

GravityZone Full Disk Encryption pozwala na obsługę BitLocker w punktach końcowych Windows i FileVault oraz w narzędziu wiersza poleceń diskutil w punktach końcowych macOS poprzez Control Center.

W celu ochrony danych, moduł zapewnia pełne szyfrowanie dysku dla woluminów rozruchowych i woluminów non-boot na dyskach stałych. Zapisuje również klucze odzyskiwania na wypadek, gdyby użytkownicy zapomnieli hasła.

Moduł szyfrowania wykorzystuje istniejące zasoby sprzętu w Twoim środowisku GravityZone.

Z perspektywy oprogramowania wymagania są prawie takie same jak w przypadku BitLocker, FileVault i narzędzia wiersza polecenia diskutil, a większość ograniczeń dotyczy tych narzędzi.

Dla Windows

GravityZone Szyfrowanie obsługuje funkcję BitLocker, począwszy od wersji 1. 2, na komputerach z i bez chipu Moduł Platformy Zaufanej (TPM)

GravityZone obsługuje funkcję BitLocker na punktach końcowych z następującymi systemami operacyjnymi:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise

- Windows 8 Pro
- Windows 7 Ultimate (z TPM)
- Windows 7 Enterprise (z TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (z TPM)

* BitLocker nie dotyczy tych systemów operacyjnych i musi być zainstalowany osobno. Aby uzyskać więcej informacji na temat wdrażania BitLocker w systemie Windows Server, zapoznaj się z artykułami KB, udostępnionymi przez firmę Microsoft:

- https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server
- https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

WAŻNE
GravityZone nie obsługuje szyfrowania w systemie Windows 7 i Windows 2008 R2 bez modułu TPM.

Szczegółowe wymagania dotyczące BitLocker znajdziesz w artykule KB firmy Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Dla Mac

GravityZone obsługuje FileVault i diskutil na punktach końcowych MacOS z następującymi systemami operacyjnymi:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.5. Porty Komunikacji GravityZone

GravityZone jest rozwiązaniem rozproszonym, oznacza to, że jego komponenty komunikują się ze sobą poprzez sieć lokalną lub Internet. Każdy komponent wykorzystuje serię portów do komunikacji z pozostałymi. Musisz się upewnić, że te porty są otwarte dla GravityZone.

Aby otrzymać więcej informacji na temat portów GravityZone, patrz ten artykuł KB.

5. INSTALOWANIE OCHRONY

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować agenty bezpieczeństwa GravityZone na punktach końcowych. W tym celu potrzebny jest użytkownik GravityZone Control Center z uprawnieniami administratora w punktach końcowych zarządzanych przez Ciebie.

5.1. Zarządzanie Licencjami

GravityZone jest licencjonowany z jednym kluczem dla wszystkich usług bezpieczeństwa, z wyjątkiem Pełnego Szyfrowania Dysku, do którego dołączony jest oddzielny klucz.

Możesz wypróbować GravityZone za darmo przez 30 dni. W okresie próbnym wszystkie funkcje są w pełni dostępne i można korzystać z usługi na dowolnej liczbie komputerów. Przed zakończeniem okresu próbnego, jeśli chcesz nadal korzystać z usług, należy zdecydować się na płatną subskrypcję i dokonać zakupu.

Aby kupić licencje, skontaktuj się z sprzedawcą Bitdefender lub skontaktuj sie z nami poprzez e-mail enterprisesales@bitdefender.com.

5.1.1. Szukanie sprzedawcy

Nasi sprzedawcy przekażą Ci potrzebne informacje i pomogą wybrać licencje najlepiej pasującą do twoich potrzeb.

Aby znaleźć sprzedawcę Bitdefender w twoim państwie:

1. Przejdź do strony Lokalizacja Partnerów na stronie Bitdefender.
2. Wybierz kraj w którym mieszkasz, aby zobaczyć dostępne informacje kontaktowe partnerów Bitdefender.
3. Jeśli w swoim kraju nie możesz znaleźć sprzedawcy Bitdefender, skontaktuj się z nami, wysyłając e-mail na adres enterprisesales@bitdefender.com.

5.1.2. Aktywowanie Licencji

Przy zakupie płatnego abonamentu po raz pierwszy, klucz licencyjny jest wydawane dla Ciebie. Subskrypcja GravityZone jest włączona przez aktywowanie tego klucza licencyjnego.

Ostrzeżenie
Aktywacja licencji nie dołącza jej możliwości do aktywnej licencji. Zamiast tego, nowa licencja zastępuje starą. Na przykład, aktywowanie 10 licencji punktów

końcowych, na działającą wcześniej licencje dla 100 punktów końcowych, NIE da wyniku subskrypcji dla 110 punktów końcowych Wręcz przeciwnie, to zmniejszy liczbę określonych punktów końcowych ze 100 do 10.

Klucz licencyjny zostanie wysłany do Ciebie w wiadomości e-mail po zakupieniu. W zależności od umowy o świadczenie usług, gdy Twój klucz licencyjny jest wydawany, usługodawca może aktywować go dla Ciebie. Alternatywnie, możesz aktywować twoja licencję ręcznie, dzięki poniższym krokom:

1. Zaloguj się do Control Center korzystając ze swojego konta.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. Sprawdź szczegóły obecnej licencji w sekcji **Licencja**.
4. W sekcji **Licencja**, wybierz typ **Licencja**.
5. W polu **Klucz licencyjny** podaj klucz licencyjny.
6. Naciśnij przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o wpisanym kluczu licencyjnym.
7. Kliknij **Zapisz**.

5.1.3. Sprawdzanie szczegółów aktualnej licencji

zobacz szczegóły twojej licencji:

1. Zaloguj się do Control Center używając konta Partnera lub Administratora firmy.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. Sprawdź szczegóły obecnej licencji w sekcji **Licencja**. Możesz nacisnąć również przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o posiadanym kluczu licencyjnym.

5.2. Instalowanie Ochrony Endpoint

W zależności od konfiguracji maszyn i środowiska sieci, możesz wybrać, aby zainstalować tylko agenty bezpieczeństwa lub aby użyć także Security Server. W tym ostatnim przypadku, trzeba najpierw zainstalować Security Server, a następnie agenty bezpieczeństwa.

Zaleca się, aby użyć Security Server jeśli maszyny mają mało zasobów sprzętowych.

WAŻNE
Tylko Bitdefender Endpoint Security Tools wspiera połączenie do Security Server. Aby uzyskać więcej informacji, odwołaj się do „ Architektura GravityZone" (p. 9).

5.2.1. Instalowanie Security Server

Security Server jest dedykowana maszyną wirtualną, która deduplikuje i centralizuje większość fikcjonalności antymalware dla klientów, działających jako serwer.

Notatka
Twoja licencja produktu może nie zawierać tej funkcji.

Musisz zainstalować Security Server na jednym lub więcej hostach tak, aby dostosować liczbę wirtualnych maszyn, które będą chronione.

Musisz wziąć pod uwagę liczbę chronionych maszyn wirtualnych, zasoby dostępne dla Security Server na hoście, tak jak połączenie sieciowe pomiędzy Security Server i chronionymi maszynami wirtualnymi.

Agent bezpieczeństwa zainstalowany na maszynach wirtualnych łączy się do Security Server za pośrednictwem protokołu TCP/IP, używając szczegółów podczas instalacji szczegółów lub poprzez polityki.

Pakiet Security Server jest dostępny dla pobierania z Control Center w kilku różnych formatach, kompatybilne z głównymi wirtualnymi platformami.

Pobieranie Pakietów Instalacyjnych Security Server

Aby pobrać pakiety instalacyjne Security Server:

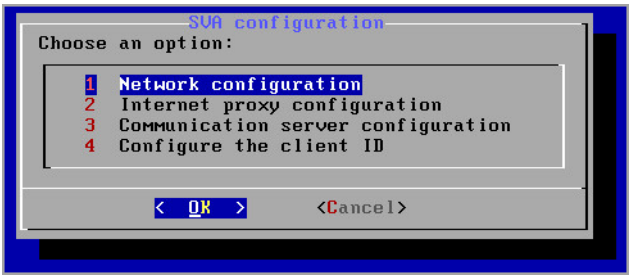
1. Przejdź do strony **Sieć > Pakiety**.
2. Wybierz Domyślny Pakiet Security Server.
3. Kliknij przycisk **Pobierz** w górnej części tabeli i wybierz typ pakietu z menu.
4. Zapisz wybrany pakiet w odpowiedniej lokalizacji.

Wdrażanie Paczek instalacyjnych Security Server

Gdy masz pakiet instalacyjny, wdróż go na hosta używając preferowanego narzędzia do instalacji maszyny wirtualnej.

Po wdrożeniu, ustawSecurity Server w ten sposób:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere). Alternatywnie, możesz połączyć się z urządzeniem przez SSH.
2. Zaloguj się używając domyślnych poświadczeń.
   - Nazwa użytkownika: `root`
   - Hasło:`sve`
3. Uruchom komendę `sva-setup`. Będziesz miał dostęp do interfejsu konfiguracyjnego urządzenia.



Security Server interfejs konfiguracji (menu główne)

Aby poruszać się po menu i opcjach, użyj klawisza `Tab` i strzałek. Aby wybrać konkretną opcję, naciśnij `Enter`.

4. Konfiguruj ustawienia sieciowe.

   Security Server wykorzystuje protokół TCP/IP do komunikowania się z innym komponentem GravityZone. Możesz skonfigurować urządzenie, aby automatycznie uzyskiwało ustawienia sieciowe z serwera DHCP lub możesz ręcznie skonfigurować ustawienia, tak jak opisano w następującym dokumencie:

   a. Z głównego menu, wybierz **Konfiguracja Sieci**.

   b. Wybierz interfejs sieciowy.

   c. Wybierz tryb konfiguracji IP:

      - **DHCP**, jeśli chcesz aby Security Server automatycznie pozyskiwał ustawienia sieci z serwera DHCP.

- **Statyczny**, jeśli serwer DHCP jest niedostępny lub rezerwacja IP dla tego urządzenia została dokonana na serwerze DHCP. W tym przypadku, musisz ręcznie skonfigurować ustawienia sieci.
  i. Wprowadź nazwę hosta, adres IP, maskę sieci, bramę i DNS serwera w odpowiednich polach.
  ii. Wybierz **OK** aby zapisać zmiany.

Notatka
Jeżeli łączysz się z urządzeniem przez klienta SSH, zmieniając ustawienia sieci, natychmiast zostanie zakończona twoja sesja.

5. Konfiguruj ustawienia proxy.

   Jeżeli serwer proxy jest używany wewnątrz sieci, musisz dostarczyć jego szczegóły tak by Security Server mógł komunikować się z Control Center GravityZone.

   Notatka
   Tylko proxy z podstawowym uwierzytelnianiem są obsługiwane.

   a. Z głównego menu, wybierz **Konfiguracja Internetowego proxy**.
   b. Wprowadź nazwę hosta, nazwę użytkownika, hasło i domenę w odpowiednim polu.
   c. Wybierz **OK** aby zapisać zmiany.
6. Skonfiguruj adres Serwera Komunikacyjnego.
   a. Z głównego menu, wybierz **Konfiguracja serwera Komunikacyjnego**.
   b. Wprowadź jeden z następujących adresów dla Serwera Komunikacji:
      - `https://cloud-ecs.gravityzone.bitdefender.com:443`
      - `https://cloudgz-ecs.gravityzone.bitdefender.com:443`

      WAŻNE
      Ten adres musi być taki sam jak ten, który pojawia się w ustawieniach polityki Control Center. Aby sprawdzić link, idź do strony **Polityki**, dodaj lub otwórz politykę niestandardową, nawiguj do sekcji **Ogólne > Komunikacja > Przypisanie Komunikacji Punktu Końcowego** sekcji i wprowadź nazwę serwera

komunikacyjnego w polu nagłówka kolumny. Prawidłowy serwer pojawi się w wynikach wyszukiwania.

c. Wybierz **OK** aby zapisać zmiany.

7. Konfiguruj ID klienta.
   a. Z menu głównego wybierz **Konfiguruj ID klienta**.
   b. Wprowadź ID firmy.

      ID składa się z 32 znaków, które można znaleźć poprzez wejście na stronę szczegółów firmy w Control Center.
   c. Wybierz **OK** aby zapisać zmiany.

5.2.2. Instalowanie Agentów Bezpieczeństwa

Aby chronić swoje fizyczne i wirtualne punkty końcowe, musisz zainstalować agenta bezpieczeństwa na każdym z nich. Poza zarządzaniem ochroną na lokalnym punkcie końcowym, agent bezpieczeństwa komunikuje się także z Control Center, aby otrzymywać polecenia administratora i wysyłać wyniki swoich działań.

Aby dowiedzieć się więcej o dostępnych agentach bezpieczeństwa, przejdź do „Agenci Bezpieczeństwa" (p. 9).

Na maszynach z systemem Windows, agenty bezpieczeństwa mogą mieć dwie role i możesz je zainstalować następująco:

1. Jako prosty agent bezpieczeństwa dla Twoich punktów końcowych.
2. Jako Relay działający jako agent bezpieczeństwa, a takze jako serwer komunikacyjny, proxy i serwer aktualizacji dla innych punktów końcowych w sieci.

Ostrzeżenie

- Pierwszy punkt końcowy, na którym zainstalujesz ochronę musi posiadać rolę Relay, w innym wypadku nie będziesz w stanie zdalnie zainstalować agenta bezpieczeństwa na innym punkcie końcowym w tej samej sieci.
- Relay punktu końcowego musi być włączony i online w celu komunikacji i łączności agentów z Control Center.

Możesz zainstalować agenty bezpieczeństwa na fizycznym lub wirtualnym punkcie końcowym poprzez uruchomienie pakietów lokalnie lub poprzez uruchomienie zadania zdalnie z Control Center.

To bardzo ważne żeby dokładnie czytać i śledzić instrukcje aby przeprowadzić instalacje.

W trybie normalnym, agenty bezpieczenstwa mają minimalny interfejs użytkownika. Dopuszcza tylko użytkowników aby sprawdzić status ochrony i uruchomić podstawowe zadania bezpieczeństwa (aktualizacje i skanowanie), bez zapewnienia dostępu do ustawień.

Jeśli został włączony przez administratora sieci poprzez paczkę instalacyjną i polityki bezpieczeństwa, agent bezpieczeństwa może również uruchomić Tryb Power User na punktach końcowych z systemem Windows, pozwalając użytkownikowi punktu końcowego wyświetlać i modyfikować ustawienia polityk. Niemniej jednak administrator Control Center może zawsze kontrolować, zawsze ustawienia polityk są stosowane, zastępując tryb Power User.

Domyślnie, wyświetlany język interfejsu użytkownika na chronionych punktach końcowych Windows jest ustawiony w czasie instalacji na język Twojego konta GravityZone.

W systemie Mac język wyświetlania interfejsu użytkownika jest ustawiony na czas instalacji w oparciu o język systemu końcowego punktu końcowego. W systemie Linux agent bezpieczeństwa nie ma zlokalizowanego interfejsu użytkownika.

Aby zainstalować interfejs użytkownika w innym języku na wybranych punktach końcowych Windows, możesz stworzyć pakiet instalacyjny i ustawić preferowany język w opcjach konfiguracyjnych. Ta opcja nie jest dostępna dla punktów końcowych Mac i Linux. Aby uzyskać więcej informacji o tworzeniu paczek instalacyjnych, odwołaj się do „Tworzenie pakietów instalacyjnych” (p. 43).

Przygotowywanie do Instalacji

Przed instalacja, wykonaj poniższe kroki przygotowawcze, aby upewnić się, że wszystko się uda:

1. Upewnij się, że docelowe punkty końcowe spełniają minimalne wymagania sprzętowe. Dla niektórych punktów końcowych, możesz potrzebować zainstalować ostatni dostępny service pack dla systemu operacyjnego lub wolne miejsce na dysku. Sprządź listę punktów końcowych, które nie spełniają niezbędnych wymogów, aby można było je wykluczyć z zarządzania.
2. Odinstaluj (nie tylko wyłącz) każde oprogramowanie antymalware, lub ochronę Internetu z docelowych punktów końcowych. Uruchomienie agenta bezpieczeństwa jednocześnie z innym oprogramowaniem ochronnym na punkcie końcowym, może wpływać na ich działanie i spowodować problemy z systemem.

Wiele niekompatybilnych programów bezpieczeństwa jest automatycznie wykrywanych i usuwanych w czasie instalacji.

Aby dowiedzieć się więcej i sprawdzić listę oprogramowania zabezpieczającego wykrytego przez Bitdefender Endpoint Security Tools dla bieżących systemów operacyjnych Windows, zobacz ten artykuł KB.

WAŻNE
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.

3. Instalacja wymaga praw administracyjnych i dostępu do internetu. Jeśli docelowe punkty końcowe znajdują się w domenie Active Directory, należy użyć poświadczeń administratora domeny do zdalnej instalacji. W przeciwnym razie upewnij się, że posiadasz niezbędne poświadczenia dla wszystkich punktów końcowych.
4. Punkty końcowe muszą mieć połączenie z Control Center.
5. Zaleca się, aby używać statycznego adresu IP dla serwera Relay. Jeśli nie ustawiłeś statycznego adresu IP, użyj nazwy hosta maszyny.
6. Podczas wdrażania agenta za pośrednictwem Relaya Linux muszą być spełnione następujące dodatkowe 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`.

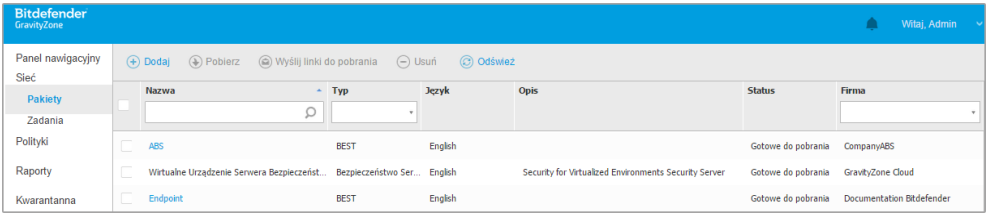
   - Docelowe punkty końcowe Windows muszą mieć włączone Zasoby Administracyjne i udostępnianie Sieciowe.
   - Docelowe punkty końcowe dla systemu Linux i Mac muszą mieć włączoną obsługę SSH.

7. Począwszy od macOS High Sierra (10.13), po zainstalowaniu Endpoint Security for Mac ręcznie lub zdalnie, użytkownicy są proszeni o zatwierdzenie rozszerzeń jądra Bitdefender na swoich komputerach. Dopóki użytkownicy nie zaakceptują rozszerzeń jądra Bitdefender, niektóre funkcje Endpoint Security for Mac nie będą działać. Aby wyeliminować interwencję użytkownika, możesz wstępnie zatwierdzić rozszerzenia jądra Bitdefender, dodając je do białej listy za pomocą narzędzia do zarządzania urządzeniami przenośnymi.

Instalacja lokalna

Jednym sposobem na instalację agenta bezpieczeństwa na punkcie końcowym jest lokalne uruchomienie pakietów instalacyjnych.

Możesz tworzyć i zarządzać pakietami instalacyjnymi na stronie **Sieć > Pakiety** .



Strona Pakietów

Ostrzeżenie

- Pierwsza maszyna, na której zainstalujesz zabezpieczenie musi mieć rolę Relay, w przeciwnym razie nie będziesz w stanie wdrożyć agenta bezpieczeństwa na innych punktach końcowych w sieci.
- Maszyna Relay musi być włączona i widoczna online, aby klienci mieli połączenie z Control Center.

Gdy pierwszy klient zostanie zainstalowany, zostanie on wykorzystany do wykrycia innych punktów końcowych w tej samej sieci, bazując na mechanizmie wykrywania sieci. Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „Jak działa wyszukiwanie sieci” (p. 59).

Aby lokalnie zainstalować agenta bezpieczeństwa na punkcie końcowym, należy wykonać następujące kroki:

1. Utwórz pakiet instalacyjny według swoich potrzeb.

Notatka
Ten krok nie jest obowiązkowym, jeśli pakiet już został stworzony dla sieci w ramach twojego konta.

2. Pobierz pakiet instalacyjny na docelowy punkt końcowy.

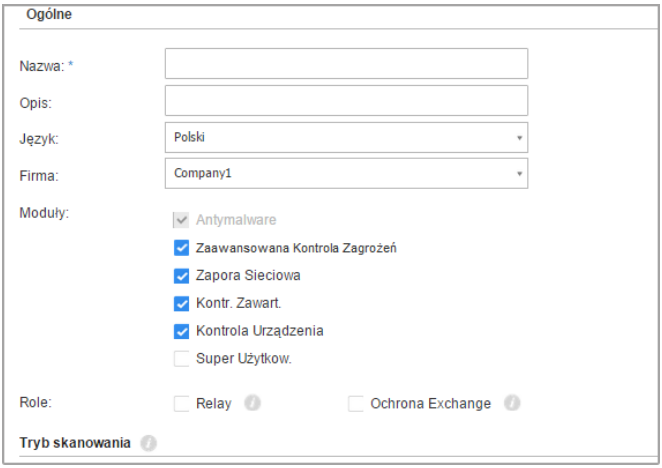
   Alternatywnie możesz wysłać linki do pobrania pakietów instalacyjnych w wiadomości e-mail do kilku użytkowników sieci.
3. Uruchom pakiet instalacyjny na docelowym punkcie końcowym.

Tworzenie pakietów instalacyjnych

Każdy pakiet instalacyjny będzie widoczny w Control Center tylko dla partnera, który utworzył pakiet i dla użytkownika kont w firmie związanej z pakietem instalacyjnym.

Aby utworzyć pakiet instalacyjny:

1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć > Pakiety**.
3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlone zostanie okno konfiguracji.



Tworzenie Paczek - Opcje

4. Wpisz sugestywną nazwę i opis dla pakietów instalacyjnych, które chcesz stworzyć.
5. Z pola **Języki**, wybierz żądany język dla interfejsu klienta.

Notatka
Ta opcja jest dostępna tylko dla niektórych systemów operacyjnych Windows.

6. Wybierz moduły ochrony, które chcesz zainstalować.

Notatka
Zostaną zainstalowane tylko obsługiwane moduły dla każdego z systemów operacyjnych. Aby uzyskać więcej informacji, odwołaj się do „Agenci Bezpieczeństwa" (p. 9).

7. Wybierz docelową rolę punktu końcowego:
   - **Relay**, aby stworzyć pakiet dla punktu końcowego z rolą Relay. Aby uzyskać więcej informacji, odwołaj się do „Relay" (p. 11)
   - **Serwer Buforujący Zarządzania Aktualizacjami**, aby serwer Relay był serwerem wewnętrznym dla aktualizacji oprogramowania. Ta rola jest wyświetlana, gdy wybrana jest rola Relay. Aby uzyskać więcej informacji, odwołaj się do „Serwerów Buforowania Łatek " (p. 12)
   - **Ochrona Exchange**, aby zainstalować moduły zabezpieczeń dla Serwerów Microsoft Exchange, w tym antymalware, antyspam, filtrowanie treści i załączników dla ruchu pocztowego Exchange i skanowania antymalware na żądanie baz danych programu Exchange. Aby uzyskać więcej informacji, odwołaj się do „Instalowanie Ochrony Exchange" (p. 65).
8. Wybierz firmę w której pakiety instalacyjne będą używane.
9. **Usuń Konkurentów**. Zaleca się pozostawienie zaznaczenia tego pola wyboru, aby automatycznie usunąć niekompatybilne oprogramowanie zabezpieczające podczas gdy agent Bitdefender instaluje się na punkcie końcowym. Odznaczając tą opcję, agent Bitdefender agent zainstaluje się obok istniejącego rozwiązania bezpieczeństwa. Możesz ręcznie usunąć poprzednio zainstalowane rozwiązanie bezpieczeństwa później, na własne ryzyko.

WAŻNE
Uruchomienie agenta Bitdefender jednocześnie z innym oprogramowaniem zabezpieczającym na punkcie końcowym może wpływać na ich działanie i powodować poważne problemy z systemem.

10. **Tryb skanowania**. Wybierz technologię skanowania, która najlepiej pasuje do Twojego środowiska sieciowego i zasobów punktów końcowych. Możesz zdefiniować tryb skanowania, poprzez wybranie jednego z następujących typów:

- **Automatyczne**. W tym przypadku, agent bezpieczeństwa będzie automatycznie wykrywał konfigurację punktu końcowego i odpowiednio dostosuje technologię skanowania:
  - Centralne Skanowanie w Publicznej lub Prywatnej Chmurze (z Security Server) z awaryjnym Skanowaniem Hybrydowym (Lekkie Silniki) dla fizycznych komputerów o niskiej wydajności sprzętu oraz maszyn wirtualnych. Sprawa ta wymaga co najmniej jednego wdrożonego Security Server w sieci.
  - Lokalne Skanowanie (z Pełnymi Silnikami) na fizycznych komputerach z wysokimi wymaganiami sprzętowymi.

  Notatka
  Komputery ze słabą wydajnością posiadające częstotliwość procesora niższą niż 1.5 Ghz, lub pamięć RAM niższą niż 1GB.

- **Użytkownika**. W tym przypadku, można skonfigurować tryb skanowania, wybierając spośród kilku technologii skanowania dla maszyn fizycznych i wirtualnych:
  - Centralne Skanowanie w Publicznej lub Prywatnej chmurze (z Security Server) z awaryjnym Skanowaniem Hybrydowym (z Lekkimi Silnikami) lub Lokalnym Skanowaniem (z Pełnymi Silnikami)
  - Hybrydowe Skanowanie (z Lekkimi Silnikami)
  - Lokalne Skanowanie (z Pełnymi Silnikami)

  Dla instancji EC2, można wybrać pomiędzy następującymi trybami niestandardowego skanowania:

  Domyślnym trybem skanowania dla instancji EC2 jest Skanowanie Lokalne (zawartość bezpieczeństwa jest przechowywana na zainstalowanym agencie

zabezpieczeń, a skanowanie jest uruchamiane lokalnie na komputerze). Jeśli chcesz skanować instancje EC2 za pomocą Security Server, musisz odpowiednio skonfigurować pakiet instalacyjny agenta bezpieczeństwa i zastosowane zasady.

Domyślnym trybem skanowania dla maszyn wirtualnych Microsoft Azure jest skanowanie lokalne (zawartość bezpieczeństwa jest przechowywana w zainstalowanym agencie bezpieczeństwa, a skanowanie jest uruchamiane lokalnie na komputerze). Jeśli chcesz skanować maszyny wirtualne Microsoft Azure za pomocą Security Server, musisz odpowiednio skonfigurować pakiet instalacyjny agenta bezpieczeństwa i zastosowane polityki.

– Centralne Skanowanie w Publicznej lub Prywatnej chmurze (z Security Server) z awaryjnym Skanowaniem Hybrydowym (z Lekkimi Silnikami) lub Lokalnym Skanowaniem (z Pełnymi Silnikami)

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

Aby uzyskać więcej informacji na temat dostępnych technologii skanowania, zapoznaj się z „Silniki Skanowania” (p. 3)

11. Podczas dostosowywania silników skanowania przy użyciu skanowania Publicznej lu Prywatnej Chmury (Security Server), musimy wybrać lokalnie zainstalowane Security Server, które chcemy wykorzystać i skonfigurować ich priorytetowanie w sekcji **Przypisane Security Server**:

    a. Kliknij listę Security Server w nagłówku tabeli. Wyświetlono listę wykrytych Security Server.

    b. Wybierz jednostkę.

    c. Naciśnij przycisk ⊕ **Dodaj** z nagłówka kolumny **Akcje**.

    Security Server został dodany do listy.

    d. Zrób te same kroki, aby dodać kilka serwerów bezpieczeństwa, jeżeli jest to możliwe. W tym przypadku, możesz skonfigurować priorytet używając strzałek ⌃ góra i ⌄ dół dostępnych po prawej stronie każdego wpisu. Gdy pierwszy Security Server nie jest dostępny, następny zostanie wykorzystany i tak dalej.

    e. Aby usunąć wpis z listy, naciśnij przycisk ⊗ **Usuń** w górnej części tabeli.

Możesz wybrać opcję szyfrowania połączenia z Security Server wybierając opcję **Użyj SSL**.

12. Wybierz **Skanuj przed instalacją** jeżeli chcesz się upewnić, że maszyny są czyste przed instalacją na nich klienta. Szybkie skanowanie w chmurze zostanie przeprowadzone na docelowych maszynach przed rozpoczęciem instalacji.
13. Bitdefender Endpoint Security Tools jest zainstalowany w domyślnym katalogu instalacyjnym. Zaznacz **Użyj niestandardowej ścieżki instalacji** jeśli chcesz zainstalować agenta Bitdefender w innej lokacji. Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
    - Na Windows, domyślna ścieżka to `C:\Program Files\`. By zainstalować Bitdefender Endpoint Security Tools w niestandardowej lokacji użyj schematu Windows podczas wprowadzania ścieżki. Na przykład, `D:\folder`.
    - Na systemach Linux, Bitdefender Endpoint Security Tools jest zainstalowany domyślnie w folderze `/opt`. By zainstalować agenta Bitdefender w niestandardowej lokacji użyj schematu Linux podczas wprowadzania ścieżki. Na przykład, `/folder`.

      Bitdefender Endpoint Security Tools nie wspiera instalacji w następujących niestandardowych ścieżkach:
      – Każda ścieżka, która nie rozpoczyna się slashem (/). Jedynym wyjątkiem jest lokacja Windows `%PROGRAMFILES%`, którą agent interpretuje jako domyślny folder Linux `/opt`.
      – Każda ścieżka, która jest w `/tmp` lub `/proc`.
      – Każda ścieżka, która zawiera następujące symbole specjalne: `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
      – Specyfikator `systemd` (%)

      Na systemach Linux instalacja do niestandardowej ścieżki wymaga glibc 2.21 lub wyżej.

      WAŻNE
      Gdy używasz niestandardowej ścieżki, upewnij się, że masz odpowiedni pakiet instalacyjny dla każdego systemu operacyjnego.

14. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.

15. Jeśli docelowe punkty końcowe są w Inwentaryzacji Sieci w **Grupy Niestandardowe**, możesz wybrać, aby przenieść je do określonego folderu od razu po zakończeniu wdrażania agenta bezpieczeństwa.

    Zaznacz **Użyj foldera niestandardowego** i wybierz folder w odpowiedniej tabeli.

16. W sekcji **Wdrożeniowiec**, wybierz podmiot, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:

    - **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:

      W tym przypadku, można również zdefiniować ustawienia serwera proxy, jeśli docelowe punkty końcowe są połączone z Internetem za pośrednictwem serwera proxy. 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 wdrożeń przez Bitdefender Endpoint Security Tools Relay do pracy.

17. Kliknij **Zapisz**.

Nowoutworzony pakiet zostanie dodany do listy pakietów firmy docelowej.

Notatka
Ustawienia skonfigurowane w ramach pakietu instalacyjnego będą stosowane do punktów końcowych natychmiast po instalacji. Tak szybko, jak polityka jest stosowana do klienta, ustawienia skonfigurowane w ramach polityki będą egzekwowane, zastępując niektóre ustawienia pakietu instalacyjnego (takie jak serwery komunikacyjne lub ustawienia proxy).

Pobieranie pakietów instalacyjnych

Aby pobrać pakiety instalacyjne agentów bezpieczeństwa:

1. Zaloguj się do Control Center z punktu końcowego, na którym chcesz zainstalować ochronę.

2. Przejdź do strony **Sieć > Pakiety**.
3. Wybierz firmę, w której znajduje się punkt końcowy z nagłówka kolumny **Firma**. Tylko pakiety dostępne dla wybranej firmy będą wyświetlane.
4. Wybierz pakiety instalacyjne , które chcesz pobrać.
5. Naciśnij przycisk **Pobierz** w górnej części tabeli i wybierz typ instalacji, który chcesz. Dwa typy plików instalacyjnych są dostępne.
   - **Pobieranie**. Downloader najpierw pobiera pełny zestaw instalacyjny z serwerów w chmurze Bitdefender, a następnie rozpoczyna instalacje. Plik ma mały rozmiar i może być uruchomiony w systemach 32-bit i 64-bit (co czyni to łatwym w dystrybucji). Z drugiej strony, wymaga aktywnego połączenia z Internetem.
   - **Pełen Zestaw**. Pełne zestawy instalacyjne są większe i muszą być uruchomione na odpowiedniej wersji systemu operacyjnego.

     Pełny zestaw jest używany do instalacji ochrony na punktach końcowych z wolnym łączem lub brakiem połączenia z Internetem. Pobierz ten plik na połączony z Internetem punkt końcowy, następnie rozprowadź go na innych punktach końcowych używając zewnętrznych nośników pamięci lub udostępniając w sieci.

     Notatka
     Dostępne pełne wersje narzędzi:
     - **Windows OS:** systemy 32-bit i 64-bit
     - **System Operacyjny Linux:** dla systemów 32-bit i 64-bit
     - **macOS:** tylko 64-bitowe systemy

     Upewnij się, że instalujesz poprawną dla systemu wersję.

6. Zapisz plik na punkcie końcowym.

   Ostrzeżenie
   - Nie należy zmieniać nazwy wykonywalnego pliku downloadera, w przeciwnym wypadku nie będzie on w stanie porać plików instalacyjnych z serwera Bitdefender.

7. Dodatkowo, jeśli wybrałeś Downloader, możesz stworzyć pakiet MSI dla punktów końcowych Windows. Więcej informacji, szukaj w artykule KB

Wyślij linki do pobrania pakietów instalacyjnych w wiadomości e-mail.

Będziesz musiał szybko poinformować administratorów firmy, że pakiet instalacyjny jest dostępny dla nich do pobrania. W tym przypadku, wykonaj kroki opisane poniżej:

Możesz potrzebować szybko poinformować innych użytkowników o dostępności pakietów instalacyjnych do pobrania. W tym przypadku, wykonaj kroki opisane poniżej:

1. Przejdź do strony **Sieć > Pakiety**.
2. Wybierz pakiety instalacyjne, które potrzebujesz.
3. Kliknij przycisk **Wyślij linki pobierania** z górnej strony tabeli. Wyświetlone zostanie okno konfiguracji.
4. Wpisz adres e-mail dla każdego użytkownika, który chce otrzymać link do pobrania pakietu instalacyjnego. Naciśnij `Enter` po każdym adresu e-mail.

   Upewnij się, że każdy wpisany adres e-mail jest prawidłowy.
5. Jeżeli chcesz zobaczyć linki pobierania przed wysłaniem ich w wiadomości e-mail, naciśnij na przycisk **Linki instalacyjne**.
6. Kliknij **Wyślij**. E-mail zawierający link instalacyjny jest wysyłany do każdego podanego adresu e-mail.

Uruchamianie Pakietów Instalacyjnych

Aby instalacja została uruchomiona, pakiet instalacyjny musi być uruchamiany przy użyciu uprawnień administratora.

Pakiet instaluje się inaczej na każdym systemie operacyjnym, jak następuje:

- Na systemach operacyjnych Windows i macOS:
  1. Na docelowy punkt końcowy, pobierz plik instalacyjny z Control Center lub skopiuj go z udziału sieciowego.
  2. Jeżeli pobrałeś pełny zestaw, wyodrębnij pliki z archiwum.
  3. Uruchom plik wykonywalny.
  4. Postępuj według instrukcji na ekranie.

Notatka
W systemie MacOS po zainstalowaniu Endpoint Security for Mac użytkownicy są proszeni o zatwierdzenie rozszerzeń jądra Bitdefender na swoich komputerach.

Dopóki użytkownicy nie zaakceptują rozszerzeń jądra Bitdefender, niektóre funkcje agenta zabezpieczeń nie będą działać. Więcej szczegółów znajdziesz w tym artykule KB.

- Na systemach operacyjnych Linux:
  1. Połącz się i zaloguj do Control Center.
  2. Pobierz lub kopiuj plik instalacyjny do docelowego punktu końcowego.
  3. Jeżeli pobrałeś pełny zestaw, wyodrębnij pliki z archiwum.
  4. Uzyskaj uprawnienia roota przez uruchomienie polecenia `sudo su`.
  5. Zmień uprawnienia do pliku instalacyjnego, aby można było go wykonać:

     ```
     # chmod +x installer
     ```

  6. Uruchom plik instalacyjny:

     ```
     # ./installer
     ```

  7. Aby sprawdzić, czy agent został zainstalowany na punkcie końcowym, uruchom polecenie:

     ```
     $ service bd status
     ```

Gdy agent bezpieczeństwa zostanie zainstalowany, punkt końcowy pokaże się w zarządzaniu w Control Center (Strona **Sieć**) w ciągu kilku minut.

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.

Instalacja Zdalna

Control Center dopuszcza zdalną instalację agenta bezpieczeństwa na punktach końcowych wykrytych w sieci przez użycie zadań instalacji.

Kiedy już zainstalowano lokalnie pierwszego klienta z rolą Relay, może upłynąć kilka minut, zanim reszta punktów końcowych sieci, stanie się widoczna w Control Center. Od tego momentu, możesz zdalnie zainstalować agenta bezpieczeństwa na punktach końcowych zarządzanych przez Ciebie przy użyciu zadania instalacji z Control Center.

Bitdefender Endpoint Security Tools zawiera mechanizm automatycznego wykrywania sieci, która umożliwia wykrywanie innych punktów końcowych, w tej samej sieci. Wykryte punkty końcowe są wyświetlane jako **niezarządzane** na stronie **Sieci**.

Aby włączyć wyszukiwanie sieci, musisz mieć zainstalowany Bitdefender Endpoint Security Tools przynajmniej na jednym punkcie końcowym w sieci. Ten punkt końcowy będzie używany do skanowania sieci i instalacji Bitdefender Endpoint Security Tools na niechronionych punktach końcowych.

Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „Jak działa wyszukiwanie sieci” (p. 59).

Wymagania zdalnej instalacji

Aby zdalna instalacja działała:

- Bitdefender Endpoint Security Tools Relay musi być zainstalowany w Twojej sieci.
- Dla Windows:
  - Udziały administracyjne `admin$` muszą być włączone. Skonfiguruj każdą docelową stacje roboczą do nie używania zaawansowanej wymiany plików.

– Skonfiguruj Kontrolę Konta Użytkownika (UAC) w zależności od systemu operacyjnego uruchomionego na docelowych punktach końcowych. Jeśli punkty końcowe znajdują się w domenie Active Directory, można użyć zasad grupy do skonfigurowania Kontroli Konta Użytkownika. Więcej szczegółów znajdziesz w tym artykule KB.

– Wyłącz Windows Firewall lub skonfiguruj ją tak, aby zezwalała na ruch przez protokół udostępniania plików i drukarek.

Notatka
Zdalne wdrażanie działa tylko w nowoczesnych systemach operacyjnych, zaczynając od Windows 7 / Windows Server 2008 R2, dla których Bitdefender zapewnia pełne wsparcie. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 20).

- Na Linux: SSH musi być włączone.
- Na MacOS: zdalne logowanie i udostępnianie plików musi być włączone.

Uruchamianie Zadania Zdalnej Instalacji

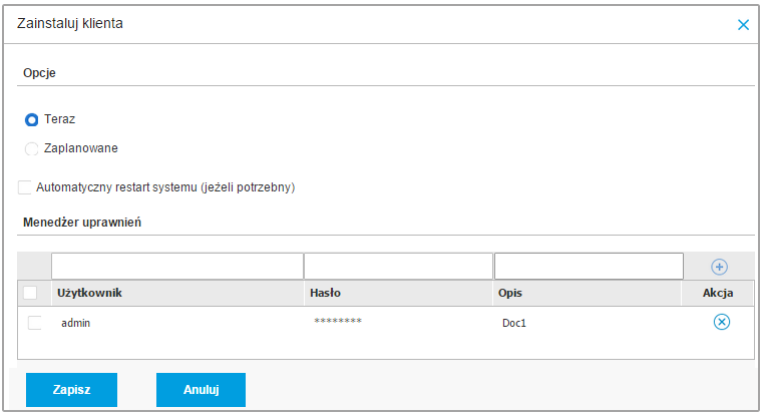
Aby uruchomić zdalną instalacje:

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

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

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

   Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Bitdefender Endpoint Security Tools z menu zadań

6. 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.

7. Jeśli chcesz, by docelowe punkty końcowe samoczynnie się uruchamiały, aby zakończyć instalację, wybierz **Automatyczny restart (w razie potrzeby)**.
8. 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.

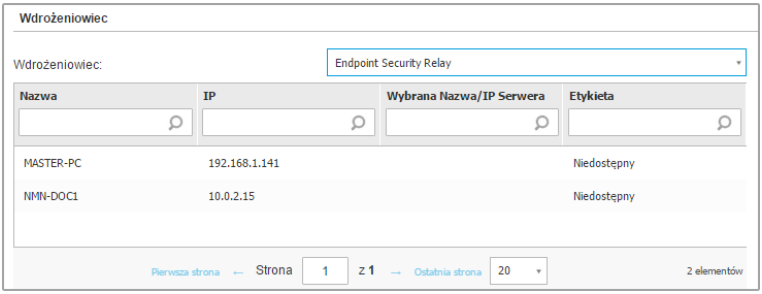
WAŻNE
Jeżeli dostarczone poświadczenia są nieważne, instalacja klienta nie powiedzie się na odpowiednich punktach końcowych. Upewnij się, że zaktualizowałeś wprowadzone poświadczenia OS w Menedżerze Poświadczeń, gdy są one zmieniane na docelowych punktach końcowych.

9. 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.

10. W sekcji **Wdrożeniowiec**, skonfiguruj Relay, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:
    - Wszystkie maszyny z rolą Relay wykryte w twojej sieci pojawią się w tabeli dostępnej w sekcji **Wdrożeniowca**. Każdy nowy klient musi być połączony z przynajmniej jednym klientem Relay z tej samej sieci, który będzie służyć do komunikacji i aktualizacji serwera. Wybierz Relay, który chcesz połączyć z docelowym punktem końcowym. 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.



11. 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.
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, patrz „Tworzenie pakietów instalacyjnych" (p. 43).

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.

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.

Przygotowywanie Systemów Linux do Skanowania Dostępowego

Wersja Bitdefender Endpoint Security Tools dla Linux zawiera możliwości skanowania dostępowego, które pracują z określoną dystrybucją Linux i wersjami jądra. Więcej informacji można znaleźć w wymaganiach systemu.

Następnie musisz nauczyć się jak ręcznie skompilować moduł DazukoFS.

Ręcznie skompiluj moduł DazukoFS.

Postępuj według poniższych kroków aby skompilować DazukoFS dla wersji jądra systemy i załaduj moduły:

1. Pobierz odpowiednie nagłówki jądra.
   - W systemie **Ubuntu**, uruchom komendę:

```
$ sudo apt-get install linux-headers-`uname -r`
```

- W systemach **UbuntuRHEL/CentOS**, uruchom komendę:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. W systemach **Ubuntu**. potrzebujesz `build-essential`:

```
$ sudo apt-get install build-essential
```

3. kopiuj i wyodrębnij kod źródłowy DazukoFS w wybranym katalogu:

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzvf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Skompiluj moduł:

```
# make
```

5. Zainstaluj i załaduj moduł:

```
# make dazukofs_install
```

Wymagania dotyczące korzystania ze skanowania dostępowego z DazukoFS

Aby DazukoFS i skanowaniu zależne od dostępu mogły razem pracować musi być spełniony szereg warunków. Proszę sprawdzić, czy którekolwiek z oświadczeń poniżej stosuje się do systemu Linux i postępuj zgodnie ze wskazówkami, aby uniknąć problemów.

- polityka SELinux musi być włączona i ustawiona na **zezwolono**. Sprawdź i dopasuj ustawienia polityki SELinux, edytując plik `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools jest wyłącznie zgodny z wersją DazukoFS zawartą w pakiecie instalacyjnym. Jeżeli DazukoFS jest zainstalowany w systemie, usuń go przed instalacja Bitdefender Endpoint Security Tools.

- DazukoFS wspiera niektóre wersje jądra. Jeżeli pakiety DazukoFS dostarczone z Bitdefender Endpoint Security Tools nie są kompatybilne z wersją jądra systemu, moduł się nie załaduje. W danym przypadku, możesz zaktualizować jądro do obsługiwanej wersji lub przekompilować moduł DazukoFS do twojej wersji jądra. Możesz znaleźć pakiet DazukoFS w katalogu instalacyjnym Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`

- Kiedy udostępniasz pliki używając dedykowanych serwerów takich jak NFS, UNFSv3 lub Samba, musisz uruchomić usługi w poniższej kolejności:

  1. Włącz skanowanie na wejściu przy pomocy polityki z Control Center.

     Po więcej informacje odnieś się do Przewodnika Partnerskiego GravityZone lub Administratorskiego.

  2. Uruchom usługę udostępniania w sieci.

     Dla NFS:

     ```
     # service nfs start
     ```

     Dla UNFSv3:

     ```
     # service unfs3 start
     ```

     Dla Samba:

     ```
     # service smbd start
     ```

WAŻNE
Dla usługi NFS, DazukoFS jest kompatybilny tylko z Użytkownikiem Serwera NFS.

Jak działa wyszukiwanie sieci

Oprócz integracji z usługa Active Directory, GravityZone zawiera również mechanizm automatycznego wykrywania sieci, przeznaczony do wykrywania komputerów grupy roboczej.

GravityZone opiera się na usłudze **Microsoft Computer Browser** oraz narzędziu **NBTscan** aby wykryć urządzenie w sieci.

Usługa przeglądania komputera jest technologia sieciową, która jest używana przez komputery z systemem operacyjnym Windows do aktualizacji listy domen, grup roboczych i komputerów w ich obrębie i dostarcza te listy do komputerów klienta na żądanie. Komputery wykryte w sieci przez usługę przeglądania komputerów można zobaczyć uruchamiając komendę **zobacz sieć** w oknie wiersza poleceń.

Polecenie zobacz sieć

Narządzie NBTscan skanuje sieci komputerowe korzystając z NetBIOS'a. Służy do sprawdzania każdego punktu końcowego w sieci i pobierania informacji, takich jak adres IP, nazwa komputera NetBIOS i adres MAC.

Aby włączyć automatyczne wyszukiwanie sieci, musisz mieć zainstalowany Bitdefender Endpoint Security Tools Relay przynajmniej na jednym komputerze w sieci. Ten komputer będzie używany do skanowania sieci.

WAŻNE

Control Center nie wykorzystuje informacji sieciowych z Active Directory lub funkcji mapy sieci. Mapa sieci zależy od innych technologi wykrywania sieci: protokołu Link Layer Topology Discovery (LLTD).

Control Center nie jest aktywnie zaangażowany w operację serwisową Computer Browser. Bitdefender Endpoint Security Tools wysyła jedynie zapytanie do usługi Computer Browser w celu uzyskania listy stacji roboczych i serwerów widocznych aktualnie w sieci (znanych jako lista przeglądania) następnie wysyła je do Control Center. Control Center przetwarza listy przeglądania, dołączając nowo wykryte komputery do listy **Niezarządzane Komputery**. Wcześniej wykryte komputery nie są usunięte po ponownym zapytaniu wykrywania sieci, musisz wyłączyć & ręcznie; usuń komputery, które nie są już w sieci.

Początkowe zapytanie na liście przeglądania przeprowadzane jest po raz pierwszy podczas instalacji Bitdefender Endpoint Security Tools w sieci.

- Jeżeli Relay jest zainstalowany na komputerze grupy roboczej, tylko komputery z grupy roboczej będą widoczne w Control Center.
- Jeżeli Relay jest zainstalowany na komputerze domeny, tylko komputery z domeny będą widoczne w Control Center. Komputery z innej domeny zostaną wykryte jeżeli mają zaufane połączenie z domeną, na której jest zainstalowany Relay.

Kolejne pytania wyszukiwania sieci są wykonywane regularnie co godzinę. Dla każdego nowego zapytania, Control Center dzieli zarządzanie przestrzenią komputerów w widocznym obszarze i następnie wyznacza jeden Relay w każdym obszarze, aby wykonać zadanie. Widocznym obszarem jest grupa komputerów, które wykrywają siebie nawzajem. Zazwyczaj, widoczny obszar jest definiowany przez grupę robocza lub domenę, ale to zależy od topologii sieci i konfiguracji. W niektórych przypadkach, widoczność obszaru może zależeć od wielu domen i grup roboczych.

Jeżeli wybrany Relay wyświetli błąd podczas wykonywania zapytania, Control Center poczeka do następnego zaplanowanego zapytania, aby spróbować ponownie, bez wybierania innego Relaya.

Dla pełnej widoczności sieci Relay musi być zainstalowany na przynajmniej jednym komputerze każdej grupy roboczej lub domeny w twojej sieci. W idealnym przypadku Bitdefender Endpoint Security Tools powinien być zainstalowany co najmniej na jednym komputerze w każdej podsieci.

Więcej o usłudze przeglądania komputerów Microsoft

Szybka charakterystyka usługi przeglądania komputerów:

- Działa niezależnie od usługi Active Directory.
- Działa wyłącznie w sieci IPv4 i działa niezależnie w granicach grupy LAN (grupy roboczej lub domeny). Przeglądanie listy jest opracowane i utrzymywane dla każdej grupy LAN.
- Zazwyczaj używa bezpołączeniowych transmisji Serwera do komunikacji między węzłami.
- Używa NetBIOS nad TCP/IP (NetBT).

- Wymaga nazwy rozdzielczości NetBIOS. Jest zalecane posiadanie infrastruktury Windows Internet Name Service (WINS) i działanie w sieci.
- Domyślnie nie jest włączone w Windows Serwer 2008 i 2008 R2.

Dla szczegółowych informacji usługa Przeglądania Komputera, sprawdź Dane Techniczne usługi Przeglądania komputerów w Microsoft Technet.

Wymagania wyszukiwania sieci

Aby poprawnie wykryć wszystkie komputery (serwery i stacje robocze) które będą zarządzane przez Control Center, wymagane są:

- Komputery muszą być przyłączone do grupy roboczej lub domeny i połączone przez lokalną sieć IPv4. Usługa Przeglądarki komputerowej nie działa w sieci IPv6.
- Kilka komputerów w każdej grupie LAM (stacje robocze lub domeny) muszą uruchamiać usługę Przeglądarki Komputerów. Podstawowe kontrolery domeny muszą również uruchomić usługę.
- NetBIOS nad TCP/IP (NetBT) musi być włączony na komputerach. Lokalny firewall musi dopuszczać ruch NetBT.
- 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.
- Udostępnianie plików musi być włączone na komputerach. Lokalny firewall musi dopuszczać udostępnianie plików.
- Infrastruktura Windows Internet Name Service (WINS) musi zostać ustawiona i działać poprawnie.
- Odnajdywanie Sieci musi być uruchomione (**Panel Sterownia > Centrum Sieci i Udostępniania > Zmień Zaawansowane Ustawienia udostępniania**).

  By uruchomić tę funkcję muszą być uruchomiony następujące usługi:
  - Klient DNS
  - Funkcja wykrywania zasobów publikacji
  - Wykrywanie SSDP
  - Host UPnP Urządzenia

- W środowiskach z wieloma domenami, jest rekomendowane aby ustawić zaufaną relację pomiędzy domenami, dzięki czemu komputery będą miały dostęp do przeglądania listy z innych domen.

Komputery, z których Bitdefender Endpoint Security Tools wysyła zapytania do usługi Przeglądarki Komputerowej muszą mieć możliwość rozpoznawania nazw NetBIOS.

Notatka
Mechanizm wyszukiwania sieci działa dla wszystkich obsługiwanych systemów operacyjnych, włączając wersję wbudowaną w Windows, pod warunkiem, że wymagania są spełnione.

5.3. Instalowanie EDR

Moduł ten jest domyślnie instalowany przy użyciu zestawu instalacyjnego Bitdefender Endpoint Security Tools i wymaga aktywacji Sensora Incydentów po pierwszym wpisaniu klucza licencyjnego.

Przed instalacją upewnij się, że docelowe punkty końcowe spełniają minimalne wymagania. Minimalne wymagania Incydentów są zgodne z Wymaganiami Agenta Bezpieczeństwa.

Aby zabezpieczyć punkty końcowe za pomocą EDR, możesz wybrać jedną z dwóch opcji:

- Zainstaluj agentów bezpieczeństwa przy użyciu czujnika EDR po wprowadzeniu klucza licencyjnego. Odnieś się do Aktywowanie licencji.
- Użyj zadania **Zrekonfiguruj**.

WAŻNE
The Incidents Sensor no longer provides support for Internet Explorer.

Aby uzyskać więcej informacji, zapoznaj się z Podręcznikiem Administratora GravityZone.

5.4. Instalacja Pełnego Szyfrowania Dysku

Pełne Szyfrowanie Dysku jest uruchamiane inaczej dla firm klienta z licencją roczną, a inaczej dla tych z licencją miesięczną.

- Dla firm klienta z licencją roczną, Pełne Szyfrowanie Dysku jest dostarczane jako dodatek wymagający aktywacji w oparciu o klucz licencyjny.

- Dla firm klienta z licencją miesięczną, możesz zezwolić na zarządzanie Pełnym Szyfrowaniem Dysku dla każdej firmy, bez klucza licencyjnego.

Firmy Klienta z Roczną Licencją

Aby aktywować Pełne Szyfrowanie Dysku dla firm klienta z roczną licencją:

1. Zaloguj do Control Center.
2. Idź do **Firmy**.
3. Kliknij nazwę firmy, dla której chcesz włączyć Pełne Szyfrowanie Dysku.
4. W sekcji **Licencja**, w polu **Dodatkowy klucz** wpisz klucz licencyjny Pełnego Szyfrowania Dysku.
5. Kliknij **Dodaj**. Szczegóły dodatku pojawią się w tabeli: typ, klucz licencyjny i opcja usunięcia klucza.
6. Naciśnij **Zapisz** aby zastosować zmiany.

Firmy klienta z Miesięczną Licencją

Aby zezwolić na zarządzanie Pełnym Szyfrowaniem Dysku dla firm klienta z miesięczną licencją:

1. Zaloguj do Control Center.
2. Idź do **Firmy**.
3. Naciśnij przycisk ⊕ **Dodaj** na pasku narzędzi.
4. Wypełnij wymagane dane, wybierz **Klient** dla typu firmy i **Subskrypcja Miesięczna** dla typu licencji.
5. Wybierz pole **Pozwól firmie zarządzać Szyfrowaniem**.
6. Naciśnij **Zapisz** aby zastosować zmiany.

Firmy partnerskie posiadają domyślne ustawienia Pełnego Szyfrowania Dysku i nie mogą włączyć lub wyłączyć tej funkcji.

Aby uzyskać więcej informacji o kluczu licencyjnym, przejdź do „Zarządzanie Licencjami” (p. 34).

Agenci bezpieczeństwa Bitdefender obsługują Pełne Szyfrowanie Dysku, zaczynając od wersji Windows 6.2.22.916 i Mac 4.0.0173876. Masz dwie opcje, aby upewnić się, że agenci są kompatybilni z tym modułem:

- Zainstaluj agentów bezpieczeństwa za pomocą dołączonego modułu Szyfrowania.
- Uruchom zadanie **Rekonfiguruj**.

Aby uzyskać szczegółowe informacje na temat korzystania z Pełnego Szyfrowania Dysku, zapoznaj się z rozdziałem **Polityki Bezpieczeństwa > Szyfrowanie** w Przewodniku Administratora GravityZone.

5.5. Instalowanie Ochrony Exchange

Security for Exchange automatycznie integruje się z Serwerami Exchange, w zależności od roli serwera. Dla każdej z ról tylko kompatybilne funkcje są instalowane, co opisano tutaj:

Funkcje	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Krawędź	Skrzynka pocztowa	Krawędź	Hub	Skrzynka pocztowa
Poziom Transport					
Filtrowanie Antymalware	x	x	x	x	
Filtrowanie Antyspam	x	x	x	x	
Filtrowanie zawartości	x	x	x	x	
Filtrowanie załączników	x	x	x	x	
Exchange Store					
Skanowanie na żądanie przeciw malware		x			x

5.5.1. Przygotowywanie do Instalacji

Zanim zainstalujesz Security for Exchange, upewnij się, że wszystkie wymagania są spełnione, inaczej Bitdefender Endpoint Security Tools może zostać zainstalowany bez modułu ochrony Exchange.

Dla płynnego działania modułu Ochrony Exchange i zapobiegania konfliktom oraz niepożądanym efektom, usuń agentów antymalware i filtrowania wiadomości e-mail.

Bitdefender Endpoint Security Tools automatycznie wykrywa i usuwa większość produktów antymalware i wyłącza wbudowanego agenta antymalware w Exchange

Server od wersji 2013. Szczegółowe informacje dotyczące listy wykrytych oprogramowań zabezpieczających, patrz ten artykuł KB.

Możesz ręcznie ponownie włączyć wbudowanego agenta antymalware Exchange w dowolnym czasie, jednak nie jest to zalecane, aby to robić.

5.5.2. Instalowanie Ochrony na Serwerach Exchange

Aby chronić swoje Serwery Exchange, musisz zainstalować Bitdefender Endpoint Security Tools z rolą Ochrona Exchange na każdym z nich.

Masz kilka opcji wdrożenia Bitdefender Endpoint Security Tools na Serwerach Exchange:

- Instalacja lokalna, przez pobranie i uruchomienie pakietu instalacyjnego na serwerze.
- Zdalna instalacja, uruchamiając zadanie **Zainstaluj**.
- Zdalnie, uruchamiając zadanie **Rekonfiguruj Klienta**, jeśli Bitdefender Endpoint Security Tools oferuje już ochronę systemu na serwerze.

Szczegółowe kroki instalacji, odwołaj się do „Instalowanie Agentów Bezpieczeństwa" (p. 39).

5.6. Manager uprawnień

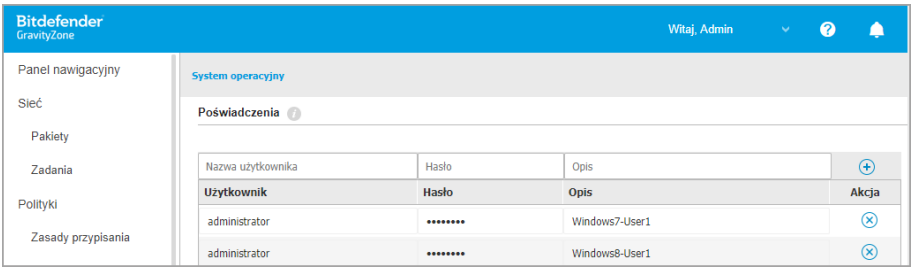
Menadżer Poświadczeń pomaga zdefiniować poświadczenia wymagane dla zdalnego uwierzytelniania na różnych systemach operacyjnych w twojej sieci.

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

5.6.1. Dodaj Poświadczenia to Menadżera Poświadczeń

Za poocą Menadżera Poświadczeń możesz zarządzać poświadczeniami administratora wymaganymi do zdalnego uwierzytelniania podczas instalacji zadań 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.

5.6.2. Usuwanie Poświadczeń z Menadżera Poświadczeń

aby usunąć nieaktualne poświadczenia z Menadżera Poświadczeń:

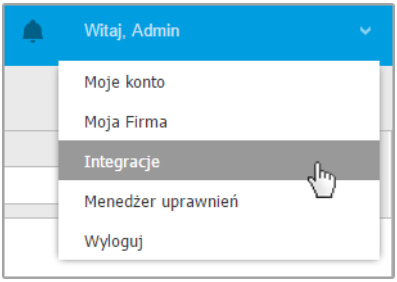
1. Wskaż wiersz w tabeli zawierający dane uwierzytelniające, które chcesz usunąć.

2. Kliknij przycisk ⊗**Usuń** po prawej stronie odpowiedniego wiersza w tabeli. Wybrane konto zostanie usunięte.

6. INTEGRACJE

GravityZone zapewnia możliwość integracji Control Center z rozwiązaniami stron trzecich.

Możesz skonfigurować integrację rozwiązań firm trzecich na stronie **Integracje**, do której dostęp można uzyskać poprzez wskazanie swojej nawy użytkownika w prawym górnym rogu konsoli i wybierając **Integracje**.



Na tej stronie możesz dodawać, edytować lub usuwać integracje zgodnie z własnymi potrzebami.

6.1. Integracja z ConnectWise Automate

Dzięki tej integracji masz dostęp do funkcji GravityZone takich jak wdrożenie, zarządzanie kwarantanną, alerty i powiadomienia wewnątrz Centrum Kontroli Automate. Po więcej informacji odnieś się do Poradnika Intergracji ConnectWise Automate.

6.2. Integracja z ConnectWise Manage

Control Center stanowi specyficzną funkcjonalność integracji dla partnerów z kontami ConnectWise, umożliwiając sprawne monitorowanie usług bezpieczeństwa Bitdefender dostarczonych do firm klienckich za pośrednictwem platformy ConnectWise, na podstawie zautomatyzowanych procedur biletowych i rozliczeniowych.

Aby uzyskać pełne informacje na temat integracji GravityZone Control Center z ConnectWise Manage, odnieś się do Przewodnika Integracji ConnectWise Manage.

6.3. Integracja z Amazon EC2

Jako Managed Service Provider (MSP) z kontem partnera w GravityZone Control Center, masz możliwość integracji Control Center z Amazon EC2 i centralnego wdrażania, zarządzania i monitorowania zabezpieczeń Bitdefender na inwentaryzacji instancji. Posiadane serwery skanowania są hostowane przez Bitdefender wewnątrz chmury AWS Cloud w celu zapewnienia optymalnego odcisku na chronionych przypadkach by wyeliminować skanowanie napowietrznego występującego w tradycyjnym oprogramowaniu ochrony.

Aby uzyskać pełne informacje o architekturze Bitdefender Security for AWS, wymaganiach wstępnych, trybie subskrypcji, tworzeniu i zarządzaniu integracją z Amazon EC2, zapoznaj się z przewodnikiem po integracji Amazon EC2.

6.4. Integracja z Splunk

Partnerzy z kontami Splunk mogą wysyłać dane z GravityZone do Splunk przez HTTP Event Collector. Ta integracja wykorzystuje interfejsy API GravityZone, a do konfiguracji wymaga równoczesnego dostępu do platformy Control Center i Splunk.

Pełne wskazówki dotyczące integracji GravityZone ze Splunk znajdują się w tym artykule KB.

6.5. Intergracja z Kaseya VSA

Dzięki tej integracji możesz zarządzać zabezpieczeniami GravityZone wewnątrz Kaseya VSA. Po więcej informacji odnieś się do Poradnika Integracji Kaseya VSA Bitdefender.

6.6. Integracja z Datto RMM

Dzięki tej integracji możesz wdrożyć agenta bezpieczeństwa Bitdefender dla pojedynczego lub wielu obiektów. Po więcej informacji, odnieś się do Podręcznika użytkownika komponentów Datto RMM.

7. ODINSTALOWYWANIE OCHRONY

Możesz odinstalować i zainstalować komponenty GravityZone w takich przypadkach, gdy trzeba użyć klucza licencyjnego na innej maszynie, aby naprawić błędy lub podczas aktualizacji.

Aby poprawnie odinstalować ochronę Bitdefender z punktów końcowych w Twojej sieci, podążaj za opisanymi instrukcjami w tym rozdziale.

- Odinstalowywanie Ochrony Endpoint
- Odinstalowywanie Ochrony Exchange

7.1. Odinstalowywanie Ochrony Endpoint

Aby bezpiecznie usunąć ochronę Bitdefender, musisz najpierw odinstalować agenty bezpieczeństwa, a następnie Security Server, jeśli jest to potrzebne. Jeśli chcesz odinstalować tylko Security Server, upewnij się, że najpierw połączyłeś jego agenty do innego Security Server.

- Odinstalowywanie Agentów Bezpieczeństwa
- Odinstalowywanie Security Server

7.1.1. Odinstalowywanie Agentów Bezpieczeństwa

Masz dwie opcje na odinstalowanie agentów bezpieczeństwa:

- Zdalnie w Control Center
- Manualnie na maszynie docelowej

Zdalne Odinstalowywanie

Aby zdalnie odinstalować ochronę Bitdefender z jakiegokolwiek zarządzanego punktu końcowego:

1. Przejdź do strony **Sieć**.
2. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
3. Zaznacz punkty końcowe, z których chcesz dokonać odinstalowania agenta bezpieczeństwa Bitdefender.

4. Kliknij **Zadania** w górnej części tabeli i wybierz **Odinstaluj klienta**. Wyświetlono okno konfiguracji.
5. W oknie zadania **Odinstaluj agenta** możesz wybrać czy zachować pliki poddane kwarantannie na punkcie końcowym czy je usunąć.
6. Naciśnij **Zapisz** aby utworzyć zadanie. Pojawia się wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem w **Sieć > Zadania**.

Deinstalacja Lokalna

Aby ręcznie odinstalować agenta bezpieczeństwa Bitdefender z maszyny Windows:

1. W zależności od Twojego systemu operacyjnego:
   - W Windows 7, idź do **Start > Panel Kontrolny > Odinstaluj program** w kategorii **Programy**.
   - W Windows 8, idź do **Ustawienia > Panel Kontrolny > Odinstaluj program** w kategorii **Program**.
   - W Windows 8.1, kliknij prawym przyciskiem myszy na przycisk **Start**, a następnie wybierz **Panel Kontrolny > Programy & funkcje**.
   - W Windows 10, idź do **Start > Ustawienia > System > Aplikacje & funkcje**.
2. Wybierz agenta Bitdefender z listy programów.
3. Kliknij **Odinstaluj**.
4. Wprowadź hasło Bitdefender, jeśli jest włączone w polityce bezpieczeństwa. Podczas deinstalacji, możesz zobaczyć postęp zadania.

Aby ręcznie odinstalować agenta bezpieczeństwa Bitdefender z maszyny Linux:

1. Otwórz terminal.
2. Zdobądź dostęp do roota poprzez komendy `su` lub `sudo su`
3. Nawigacja za pomocą polecenia `cd` do następującej ścieżki: `/opt/BitDefender/bin`
4. Uruchom skrypt:

```
# ./remove-sve-client
```

5. Wprowadź hasło Bitdefender, aby kontynuować, jeśli jest włączone w polityce bezpieczeństwa.

Aby manualnie odinstalować agenta Bitdefender z Mac:

1. PRzejdź do **Finder > Aplikacje**.
2. Otwórz folder Bitdefender.
3. Kliknij dwukrotnie **Bitdefender Mac Uninstall**.
4. W oknie potwierdzającym, kliknij oba **Sprawdź** i **Odinstaluj**, aby kontynuować.

7.1.2. Odinstalowywanie Security Server

Aby usunąć Security Server:

1. Wyłącz i usuń maszynę wirtualną Security Server ze swojego środowiska wirtualizacji.
2. Zaloguj się do GravityZone Control Center.
3. Przejdź do **Sieci** i znajdź Security Server w inwentarzu. Po chwili usunięcia maszyny wirtualnej Security Server zostanie zgłoszony jako offline.
4. Zaznacz pole odpowiadające Security Server.
5. Naciśnij przycisk ⊖ **Usuń** na pasku narzędzi.

   Security Server zostanie przeniesiony do folderu **Usunięte**, gdzie możesz go całkowicie usunąć, klikając ponownie ⊖ **Usuń** na pasku narzędzi akcji.

7.2. Odinstalowywanie Ochrony Exchange

Możesz usunąć Ochronę Exchange z jakiegokolwiek Serwera Microsoft Exchange mając Bitdefender Endpoint Security Tools z tą rolą zainstalowaną. Możesz wykonać odinstalowywanie w Control Center.

1. Przejdź do strony **Sieć**.
2. Wybierz pożądany kontener z lewego panelu bocznego. Wpisy będą wyświetlane po prawej stronie panelu tabeli.
3. Wybierz punkt końcowy, z którego chcesz odinstalować Ochronę Exchange.
4. Kliknij **Rekonfiguruj Klienta** w menu **Zadania**, w górnym panelu tabeli. Wyświetlono okno konfiguracji.
5. W sekcji **Ogólne** wyczyść pole wyboru **Ochrona Exchange**.

Ostrzeżenie
W oknie konfiguracji, upewnij się, że wybrałeś wszystkie inne role, które są aktywne na punkcie końcowym. W przeciwnym razie będą one także odinstalowane.

6. Naciśnij **Zapisz** aby utworzyć zadanie.

Możesz zobaczyć i zarządzać zadaniem w **Sieć > Zadania**.

Jeśli chcesz przeinstalować Ochronę Exchange, przejdź do „Instalowanie Ochrony Exchange" (p. 65).

8. OTRZYMYWANIE POMOCY

Bitdefender stara się zapewnić swoim klientom najwyższy poziom szybkiej i dokładnej pomocy technicznej. Jeżeli męczy cię jakiś problem lub masz pytania dotyczące produktu Bitdefender, przejdź do naszego Centrum Wsparcia Online. Oferuje kilka zasobów, które możesz użyć do szybkiego znalezienia rozwiązania lub odpowiedzi. Jeśli wolisz, możesz skontaktować się z Obsługą Klienta Bitdefender. Nasi przedstawiciele ds. pomocy technicznej szybko odpowiedzą na twoje pytania oraz zapewnią ci niezbędną pomoc.

Notatka
Możesz dowiedzieć się więcej na temat usług wsparcia jakie oferujemy i sposobów jej udzielania w Centrum pomocy.

8.1. Bitdefender Wsparcie Techniczne

Bitdefender Centrum Pomocy, to miejsce gdzie uzyskasz wszelką pomoc dla Twoich produktów Bitdefender.

Możesz użyć kilku źródeł, aby szybko znaleźć rozwiązanie problemu lub odpowiedź:

- Znana baza artykułów
- Bitdefender forum pomocy
- Dokumentacja produktu

Możesz również użyć ulubionej wyszukiwarki, aby znaleźć więcej informacji o ochronie komputera, produktach Bitdefender i firmie.

Znana baza artykułów

Bazą wiedzy Bitdefender jest dostępne w internecie repozytorium informacji na temat produktów Bitdefender produktów. Przechowuje czytelne raporty z trwających działań zespołu Bitdefender odnośnie pomocy technicznej i naprawiania błędów oraz bardziej ogólne artykuły dotyczące ochrony antywirusowej, szczegółowego zarządzania rozwiązaniami produktu Bitdefender oraz wielu innych zagadnień.

Baza wiedzy Bitdefender jest publiczna i bezpłatna. Informacje, które zawiera, stanowią kolejny sposób na dostarczenie klientom Bitdefender, potrzebnej wiedzy technicznej i wsparcia. Prawidłowe żądania informacji lub raportów o błędach, pochodzące od klientów Bitdefender, w końcu znajdują drogę do Bazy Wiedzy

Bitdefender. jako raporty informujące o poprawkach, sposoby ominięcia problemów czy pliki pomocy produktu i teksty informacyjne.

Baza Wiedzy Bitdefender dla produktów biznesowych jest dostepna w każdej chwili na http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne.

Bitdefender forum pomocy

Forum pomocy technicznej Bitdefender pozwala użytkownikom Bitdefender uzyskać pomoc oraz pomagać innym osobom korzystającym z produktu. Możesz tu opublikować dowolny problem lub pytanie dotyczące twoich produktów Bitdefender.

Pracownicy ds. pomocy technicznej Bitdefender monitorują forum sprawdzając nowe wpisy i zapewniając pomoc. Odpowiedź lub rozwiązanie można także uzyskać od bardziej zaawansowanego użytkownika programu Bitdefender.

Przed zamieszczeniem problemu lub pytania przeszukaj forum w celu znalezienia podobnych lub powiązanych tematów.

Forum pomocy technicznej Bitdefender jest dostępne pod adresem http://forum.bitdefender.com w 5 językach: angielskim, niemieckim, francuskim, hiszpańskim i rumuńskim. Aby uzyskać dostęp do sekcji poświęconej produktom biznesowym, kliknij łącze **Ochrona dla biznesu**.

Dokumentacja produktu

Dokumentacja produktu jest najbardziej kompletnym źródłem informacji o produkcie.

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.

8.2. Prośba o pomoc

Możesz poprosić o pomoc za pośrednictwem naszego Centrum Wsparcia Online. Wypełnij formularz kontaktowy i wyślij go do nas.

8.3. 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.

8.3.1. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Windows

Uruchamianie aplikacji Support Tool

Aby wygenerować dziennik na zagrożonym komputerze, użyj jednej z następujących metod:

- Wiersz poleceń

  Dla problemów z BEST, zainstalowanego na komputerze.

- Problem z instalacją

  Dla sytuacji gdzie BEST nie jest zainstalowany na komputerze i instalacja kończy się niepowodzeniem.

Metoda wiersza poleceń

Używając wiersza poleceń możesz zbierać logi bezpośrednio z zainfekowanego komputera. Metoda ta przydaje się w sytuacjach gdy nie masz dostępu do Centrum Kontroli GravityZone lub komputer nie komunikuje się z konsolą.

1. Otwórz wiersz polecenia z uprawnieniami administratora.
2. Przejdź do folderu instalacji produktu. Domyślna ścieżka to:

   `C:\Program Files\Bitdefender\Endpoint Security`

3. Zbieraj i zapisuj logi, uruchamiając to polecenie:

   ```
   Product.Support.Tool.exe collect
   ```

   Dzienniki są domyślnie zapisywane w `C:\Windows\Temp`.

   Opcjonalnie, jeśli chcesz zapisać dziennik Support Tool w niestandardowej lokalizacji, użyj ścieżki opcji:

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Przykład:

   ```
   Product.Support.Tool.exe collect path="D:\Test"
   ```

Podczas wykonywania polecenia można zauważyć na ekranie pasek postępu. Po zakończeniu procesu dane wyjściowe wyświetlają nazwę archiwum zawierającego dzienniki i ich lokalizację.

By wysłać logi do Biznesowej Pomocy Bitdefender przejdź do `C:\Windows\Temp` lub do niestandardowej lokacji i znajdź archiwum o nazwie `ST_[computername]_[currentdate]`. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

Problem z instalacją

1. By pobrać BEST Support Tool kliknij tutaj.
2. Uruchom plik wykonywalny jako administrator. Zostanie wyświetlone okno.
3. Wybierz lokację by zapisać archiwum logów.

   Podczas zbierania logów zauważysz pasek postępu na ekranie. Po zakończeniu procesu dane wyjściowe wyświetlają nazwę archiwum i ich lokalizację.

By wysłać logi do Biznesowej Pomocy Bitdefender przejdź do wybranej lokacji i znajdź archiwum o nazwie `ST_[computername]_[currentdate]`. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

8.3.2. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Linux

Dla systemów operacyjnych Linux, Narzędzie Wsparcia jest zintegrowane wraz z agentem bezpieczeństwa Bitdefender.

Aby zebrać informacje na temat systemu Linux przy pomocy Narzędzia Wsparcia, uruchom następujące polecenia:

```
# /opt/BitDefender/bin/bdconfigure
```

korzystając z następujących dostępnych opcji:

- `--help` aby wyświetlić listę wszystkich poleceń Narzędzia Wsparcia
- `enablelogs` aby włączyć produkt i dziennik modułu komunikacyjnego (wszystkie usługi zostaną automatycznie uruchomione ponownie)

- `disablelogs` aby wyłączyć produkt i dzienniki modułu komunikacyjnego (wszystkie usługi zostaną automatycznie uruchomione ponownie)
- `deliverall`, aby utworzyć:
  - Archiwum zawierające logi produktu i modułu komunikacyjnego dostarczone do folderu `/tmp` w następującym formacie: `bitdefender_machineName_timeStamp.tar.gz`.

  Po utworzeniu archiwum:

  1. Zostanie wyświetlony monit, jeżeli zachcesz wyłączyć dzienniki. W razie potrzeby, usługi są automatycznie ponownie uruchamiane.
  2. Zostanie wyświetlony monit, czy chcesz usunąć dzienniki.
- `deliverall -default` dostarcza pewne informacje jak w poprzedniej opcji, lecz domyślne akcje nie będą uwzględniane w dzienniku bez potwierdzenia ze strony użytkownika (dzienniki zostają wyłączone i skasowane).

Możesz także uruchomić polecenie `/bdconfigure` bezpośrednio z pakietu BEST (pełny lub downloader) bez zainstalowanego produktu.

Aby zaraportować zdarzenie GravityZone dotyczące twojego systemu Linux, przejdź do kolejnego kroku, wykorzystując wcześniej opisane opcje:

1. Uruchom produkt oraz dziennik modułu komunikacyjnego.
2. Spróbuj odtworzyć problem.
3. Wyłącz dzienniki.
4. Utwórz archiwum dzienników.
5. Odbierz bilet mailowego wsparcia używając formularza dostępnego na stronie **Pomoc & Wsparcie** Control Center, wraz z opisem zdarzenia i załączonym archiwum dziennika.

Narzędzie Wsparcia dla Linux dostarcza następujące informacje:

- `etc`, `var/log`, `/var/crash` (jeśli dostępne) oraz foldery `var/epag` z `/opt/BitDefender`, zawierają dzienniki i ustawienia Bitdefender
- Plik `/tmpvar/log/BitDefender/bdinstall.log` zawierający informacje dotyczące instalacji
- Plik `network.txt`, zawierający ustawienia sieci / informacje połączenia maszyny

- Plik `product.txt`, zawierający zawartość wszystkich plików `update.txt` z `/opt/BitDefender/var/lib/scan` i rekursywna pełna lista wszystkich plików z `/opt/BitDefender`
- Plik `system.txt` zawiera ogólne informacje systemowe (dystrybucja, wersja jądra, dostępna pamięć RAM, wolna przestrzeń dyskowa)
- Plik `users.txt`, zawierający informacje o użytkowniku
- Pozostałe informacje dotyczące produktu związane z systemem, takie jak zewnętrzne połączenia procesów i wykorzystanie procesora
- Logi systemowe

8.3.3. 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.

8.4. Informacje o produkcie

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 18 lat Bitdefender uzyskał niekwestionowaną reputację dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiekolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

8.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com
Centrum pomocy:http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne
Dokumentacja: gravityzone-docs@bitdefender.com
Lokalni Dystrybutorzy:http://www.bitdefender.com/partners
Program partnerski: partners@bitdefender.com
Rzecznik prasowy: pr@bitdefender.com
Wysyłanie Próbek Wirusów: virus_submission@bitdefender.com
Wysyłanie Próbek Spamu: spam_submission@bitdefender.com
Raportowanie Abuse: abuse@bitdefender.com
Strona: http://www.bitdefender.com

8.4.2. 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.

8.4.3. Biura Bitdefender

Biura Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych. Ich adresy oraz dane kontaktowe są wypisane poniżej.

Stany Zjednoczone

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (sprzedaż&pomoc techniczna): 1-954-776-6262
Sprzedaż: sales@bitdefender.com
Internet: http://www.bitdefender.com
Centrum pomocy: http://www.bitdefender.com/support/business.html

Francja

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Faks: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
Adres e-mail: b2b@bitdefender.fr
Strona internetowa: http://www.bitdefender.fr
Centrum pomocy: http://www.bitdefender.fr/support/business.html

Hiszpania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona

España
Faks: (+34) 93 217 91 28
Telefon (biuro i sprzedaż): (+34) 93 218 96 15
Telefon (pomoc techniczna): (+34) 93 502 69 10
Sprzedaż: comercial@bitdefender.es
Strona internetowa: http://www.bitdefender.es
Centrum pomocy: http://www.bitdefender.es/support/business.html

Niemcy

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (biuro i sprzedaż): +49 (0) 2304 94 51 60
Telefon (pomoc techniczna): +49 (0) 2304 99 93 004
Sprzedaż: firmenkunden@bitdefender.de
Strona internetowa: http://www.bitdefender.de
Centrum pomocy: http://www.bitdefender.de/support/business.html

Anglia i Irlandia

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (sprzedaż&pomoc techniczna): (+44) 203 695 3415
Adres e-mail: info@bitdefender.co.uk
Sprzedaż: sales@bitdefender.co.uk
Strona internetowa: http://www.bitdefender.co.uk
Centrum pomocy: http://www.bitdefender.co.uk/support/business.html

Rumunia

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Faks: +40 21 2641799

Telefon (sprzedaż&pomoc techniczna): +40 21 2063470
Sprzedaż: sales@bitdefender.ro
Strona internetowa: http://www.bitdefender.ro
Centrum pomocy: http://www.bitdefender.ro/support/business.html

Zjednoczone Emiraty Arabskie

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (sprzedaż&pomoc techniczna): 00971-4-4588935 / 00971-4-4589186
Faks: 00971-4-44565047
Sprzedaż: sales@bitdefender.com
Internet: http://www.bitdefender.com
Centrum pomocy: http://www.bitdefender.com/support/business.html

A. Aneksy

A.1. Wspierane Typy Plików

Antymalwarowe silniki skanowania załączone w rozwiązaniu ochrony Bitdefender mogą skanować wszystkie typy plików, które mogą zawierać zagrożenia. Lista poniżej zawiera najbardziej pospolite typy plików, które są analizowane.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

A.2. Obiekty Sandbox Analyzer

A.2.1. 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.2.2. Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania

Wstępne filtrowanie zawartości określi konkretny typ pliku za pomocą kombinacji, która implikuje treść i rozszerzenie obiektu. Oznacza to, że plik wykonywalny z rozszerzeniem `.tmp` zostanie rozpoznany jako aplikacja i jeśli okaże się podejrzany, zostanie wysłany do Sandbox Analyzer.

- Aplikacje - pliki o formacie PE32, w tym między innymi następujące rozszerzenia: exe, dll, com .
- Dokumenty - pliki o formacie dokumentu, w tym między innymi następujące rozszerzenia: xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm

, Dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf .

- Skrypty: ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- Archiwa: zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- E-maile (zapisane w systemie plików): eml, tnef .

A.2.3. Domyślne Wykluczenia przy Automatycznym Wysyłaniu

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

A.3. Jądra obsługiwane przez Sensor Incydentów

Sensor Incydentów obsługuje następujące jądra: