

Bitdefender® ENTERPRISE

BITDEFENDER SMALL OFFICE SECURITY

Przewodnik administratora



Bitdefender Small Office Security

Przewodnik administratora

Data publikacji 2015.01.21

Copyright© 2015 Bitdefender

Uwagi prawne

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

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

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

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



Spis treści

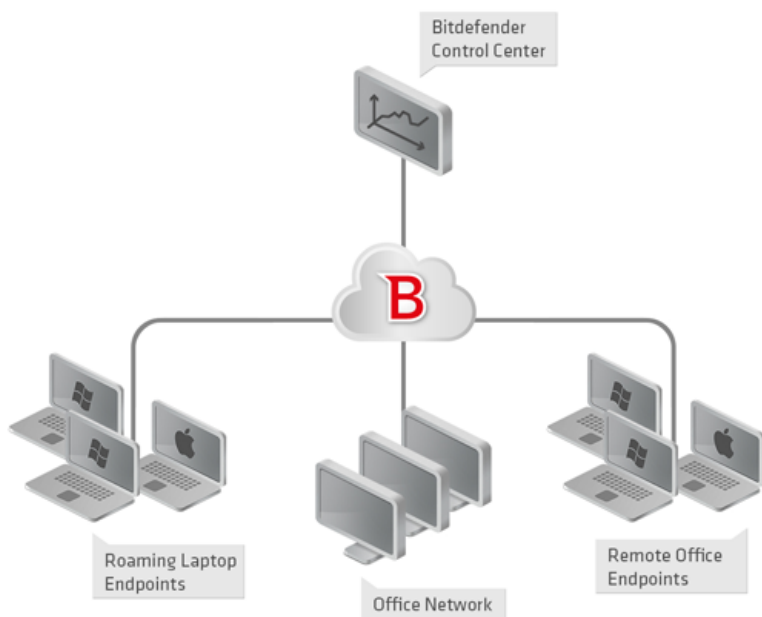
1. O Small Office Security	1
2. Pierwsze Kroki	3
2.1. Łączenie z Control Center	3
2.2. Control Center w skrócie	4
2.2.1. Control Center Przegląda	4
2.2.2. Tabela Danych	5
2.2.3. Paski narzędzi działań	6
2.2.4. Menu Kontekstowe	7
2.3. Zarządzanie kontem	7
2.4. Zarządzanie swoją firmą	8
2.5. Zmiana hasła logowania	10
3. Zarządzanie kontami użytkownika	12
3.1. Role użytkownika	13
3.2. Prawa użytkownika	14
3.3. Tworzenie Kont Użytkowników	14
3.4. Edytowanie Kont	15
3.5. Usuwanie kont	16
3.6. Resetowanie haseł logowania	16
4. Instalowanie Security for Endpoints	17
4.1. Wymagania systemowe	18
4.1.1. Wspierane systemy operacyjne	18
4.1.2. Wymagania Sprzętowe	19
4.1.3. Obsługiwane przeglądarki	19
4.1.4. Porty Komunikacji Small Office Security	19
4.2. Przygotowywanie do Instalacji	20
4.3. Instalacja lokalna	20
4.3.1. Tworzenie Endpoint Security pakietów instalacyjnych	21
4.3.2. Pobieranie pakietów instalacyjnych	24
4.3.3. Uruchamianie Pakietów Instalacyjnych	24
4.4. Instalacja Zdalna	25
4.4.1. Zdalna instalacja wymagań Endpoint Security	25
4.4.2. Działanie zadań zdalnej instalacji Endpoint Security	25
4.5. Jak działa wyszukiwanie sieci	29
4.5.1. Więcej o usłudze przeglądania komputerów Microsoft	30
4.5.2. Wymagania wyszukiwania sieci	31
5. Zarządzanie Komputerami	32
5.1. Sprawdź Stan Komputera	33
5.1.1. Zarządzane, Niezarządzane i Usunięte Komputery	34
5.1.2. Komputery Online i Offline	34

5.1.3. Komputery z problemami bezpieczeństwa	35
5.2. Organizowanie Komputerów w Grupy	35
5.3. Przeglądanie szczegóły komputera.	37
5.4. Sortowanie, filtrowanie i wyszukiwanie komputerów.	40
5.4.1. Sortowanie komputerów	40
5.4.2. Filtrowanie komputerów	40
5.4.3. Wyszukiwanie komputerów	43
5.5. Uruchamianie zadań na komputerach	44
5.5.1. Skanowanie	44
5.5.2. Zainstaluj klienta	51
5.5.3. Modyfikuj instalator	54
5.5.4. Odinstaluj Klienta	55
5.5.5. Aktualizacja	56
5.5.6. Uruchom ponownie komputer.	56
5.5.7. Przeszukiwanie sieci	57
5.6. Tworzenie szybkich raportów	57
5.7. Przypisywanie polityk	58
5.8. Usuwanie komputerów z zasobów sieci	59
5.8.1. Wykluczanie komputerów z zasobów sieci	59
5.8.2. Trwałe usuwanie komputerów	60
5.9. Pakiety Instalacyjne	61
5.9.1. Tworzenie pakietów instalacyjnych	61
5.9.2. Pobieranie pakietów instalacyjnych	63
5.9.3. Wyślij linki do pobrania pakietów instalacyjnych w wiadomości e-mail.	64
5.10. Przeglądanie i zarządzanie zadaniami	64
5.10.1. Sprawdzanie statusu zadania	65
5.10.2. Przeglądanie raportów zadania	66
5.10.3. Ponowne uruchomienie zadań	67
5.10.4. Usuwanie zadań	67
5.11. Menedżer uprawnień	67
5.11.1. Dodawanie poświadczeń do Menadżera poświadczeń	68
5.11.2. Usuwanie Poświadczeń z Menadżera Poświadczeń	68
6. Polityki Bezpieczeństwa	69
6.1. Zarządzanie politykami	70
6.1.1. Tworzenie polityk	70
6.1.2. Zmiany ustawień polityk.	71
6.1.3. Zmianie nazw polityk	71
6.1.4. Usuwanie polityki	72
6.1.5. Przypisywanie Polityk do obiektów sieci	72
6.2. Polityki Komputera	74
6.2.1. Ogólne	74
6.2.2. Antimalware	82
6.2.3. Zapora sieciowa	98
6.2.4. Kontrola zawartości	108
7. Monitorowanie Panelu	118
7.1. Odświeżanie Danych Portletów	119
7.2. Edytowanie ustawień portletów	119
7.3. Dodawanie nowego portletu	119

7.4. usuwanie Portletu	120
7.5. Zmiana Układu Portletów	120
8. Używanie raportów	121
8.1. Dostępne rodzaje raportów	121
8.2. Tworzenie raportów	124
8.3. Przeglądania i zarządzanie zaplanowanych raportów	126
8.3.1. Przeglądanie raportów	127
8.3.2. Edytowanie zaplanowanego raportu.	128
8.3.3. Usuwanie zaplanowanych raportów	129
8.4. Zapisywanie raportów	129
8.4.1. Eksportowanie raportów	129
8.4.2. Raporty pobierania	130
8.5. Raporty E-mailów	130
8.6. Drukowanie raportów	131
9. Kwarantanna	132
9.1. Nawigacja i Wyszukiwanie	133
9.2. Przywracanie plików kwarantanny	133
9.3. Automatyczne usunięcie plików kwarantanny	134
9.4. Usuwanie plików kwarantanny	134
10. Dziennik Aktywności Użytkownika	136
11. Powiadomienia	138
11.1. Rodzaje powiadomień	138
11.2. Zobacz powiadomienia	139
11.3. Usuwanie powiadomień	140
11.4. Konfiguracja ustawień powiadomień	141
12. Otrzymywanie pomocy	143
12.1. Bitdefender Wsparcie Techniczne	143
12.2. Prośba o pomoc	144
12.3. Używanie Narzędzi Pomocy	144
12.4. Informacje o produkcie	145
12.4.1. Adresy Internetowe	146
12.4.2. Biura Bitdefender	146
A. Aneksy	149
A.1. Lista Typów Plików Aplikacji	149
A.2. Używa zmiennych systemowych	149
Słownik	151

1. 0 Small Office Security

Small Office Security to usługa ochrony przeciw malware bazująca na chmurze opracowana przez Bitdefender dla komputerów działających w systemach operacyjnych Microsoft Windows i Macintosh. Używa scentralizowanego Oprogramowania jako Usługi wielokrotnego modelu wdrażania nadającego się dla klientów biznesowych, przy jednoczesnym wykorzystaniu sprawdzonej pod każdym kątem technologii ochrony przed złośliwym oprogramowaniem opracowanym przez Bitdefender dla rynku konsumenckiego.



Architektura Small Office Security

Usługa bezpieczeństwa jest hostowana przez publiczną chmurę Bitdefender. Subskrybenci mają dostęp do interfejsu zarządzania sieciowego zwanego **Control Center**. W interfejsie, administratorzy mogą zdalnie zainstalować i zarządzać ochroną przed złośliwym oprogramowaniem na wszystkich komputerach z systemami Windows i Macintosh takich jak: serwery i stacje robocze w sieci wewnętrznej, korzystające z roamingu laptopy lu zdalne biurowe punkty końcowe.

Lokalna aplikacja **Endpoint Security** jest zainstalowana na każdym chronionym komputerze. Lokalni użytkownicy mają ograniczoną widoczność i dostęp tylko do odczytu w ustawieniach

bezpieczeństwa, które są zarządzane przez administratora z Control Center; natomiast skanowanie, aktualizacja i zmiany konfiguracji są zazwyczaj wykonywane w tle.

2. Pierwsze Kroki

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

2.1. Łączenie z Control Center

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

Warunki wstępne:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Zalecana rozdzielczość ekranu: 1024x768 lub wyższa

Żeby połączyć się z Control Center:

1. Otwórz przeglądarkę.
2. Zobacz pod adresem: <https://gravityzone.bitdefender.com>
3. Podaj adres e-mail i hasło twojego konta.
4. Kliknij „Zaloguj”.

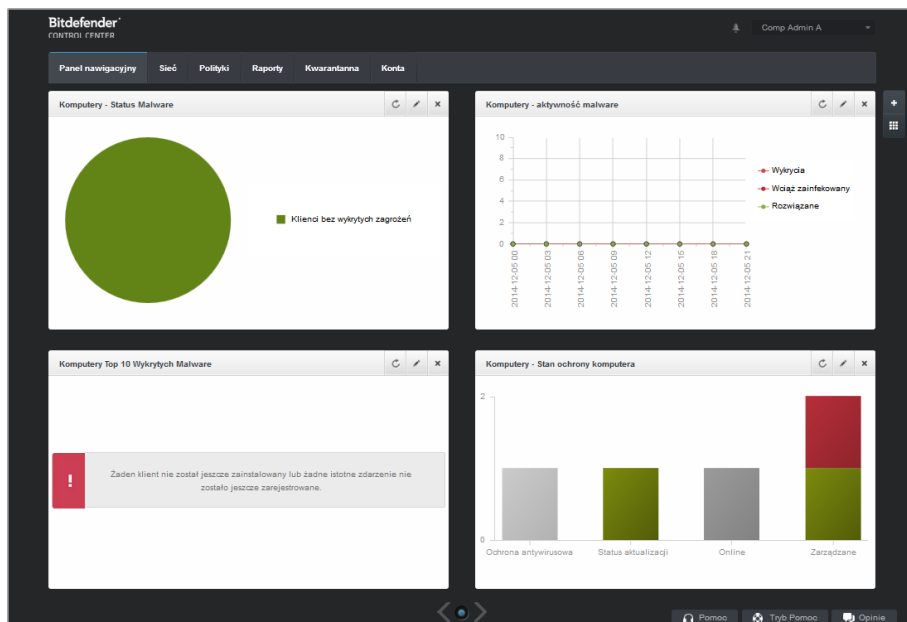


Notatka

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

2.2. Control Center w skrócie

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



Panel

2.2.1. Control Center Przegląda

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

W zależności od roli, administratorzy Small Office Security mogą uzyskać dostęp do następujących sekcji z paska menu:

Panel nawigacyjny

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

Sieć

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

Polityki

Utwórz i zarządzaj politykami bezpieczeństwa.

Raporty

Pobierz raporty bezpieczeństwa dotyczące zarządzania klientami.

Kwarantanna

Zdalne zarządzanie plikami kwarantanny.


Konta

Zarządzaj dostępem do Control Center dla innych pracowników firmy.



Notatka

To menu jest dostępne tylko dla użytkowników z prawami zarządzania użytkownikami.

Dodatkowo w górnym rogu konsoli ikona  **Powiadomienia** umożliwia łatwy dostęp do powiadomień i strony **powiadomienia**.

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

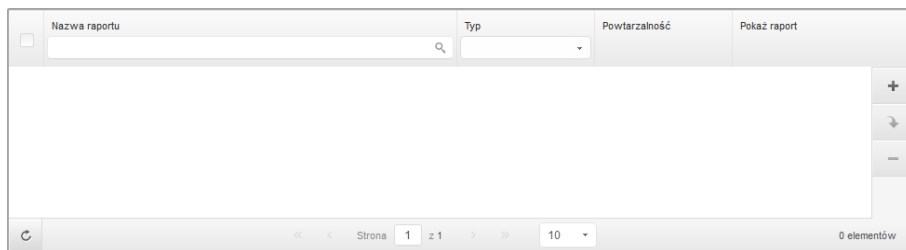
- **Moje konto.** Kliknij tę opcję, aby zarządzać danymi konta użytkownika i preferencjami.
- **Moja Firma.** Kliknij tę opcję, aby zarządzać danymi konta firmy i preferencjami.
- **Menedżer uprawnień.** Naciśnij tę opcję aby dodać i zarządzać poświadczeniami uwierzytelniania potrzebnymi do zdalnej instalacji zadań.
- **Wyloguj.** Kliknij tę opcję, aby wylogować się z konta.

W prawym dolnym rogu konsoli dostępne są linki:

- **Pomoc.** Naciśnij ten przycisk aby znaleźć informacje o wsparciu.
- **Tryb Pomoc.** Naciśnij ten przycisk aby włączyć funkcję pomocy dostarczającą podpowiedzi w Control Center. Łatwo znajdziesz przydatne informacje dotyczące funkcji Control Center.
- **Opinie.** Naciśnij ten przycisk żeby wyświetlić pole umożliwiające edycję i wysyłanie wiadomości zwrotnych dotyczących twoich doświadczeń z Small Office Security.

2.2.2. Tabela Danych

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



Nazwa raportu	Typ	Powtarzalność	Pokaż raport
---------------	-----	---------------	--------------

Strona 1 z 1 | 10 | 0 elementów

Strona raportów - Tabele raportów

Poruszanie się po stronach

Tabele z ponad 10 zgłoszeniami rozciągają się na kilka stron. Domyślnie tylko 10 wpisów jest wyświetlanych na stronie. Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Możesz zmienić liczbę wpisów wyświetlanych na stronie, wybierając inną opcję z menu obok przycisków nawigacyjnych.

Szukanie określonych wpisów


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

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

Sortowanie danych

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

Odświeżanie Danych Tabeli

Abby upewnić się, że konsola wyświetla najnowsze informacje, naciśnij przycisk  **Odśwież** w dolnym lewym rogu tabeli.


2.2.3. Paski narzędzi działań

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

- Stwórz nowy raport.
- Pobierz raporty wygenerowane przez zaplanowany raport.

- Usuń zaplanowany raport.

Raporty				
<input type="checkbox"/>	Nazwa raportu	Typ	Powtarzalność	Pokaż raport
<input type="checkbox"/>	Status aktualizacji	Status aktualizacji	cogodzinny	17 Lis 2014 - 10:39

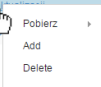


Strona raportów - Paski Narzędzi działań

2.2.4. Menu Kontekstowe

Komendy pasków narzędzi działań są również dostępne z menu kontekstowego. Naciśnij prawy przycisk w sekcji Centrum Kontroli, której aktualnie używaj i wybierz polecenie, które potrzebujesz z dostępnej listy.

Raporty				
<input type="checkbox"/>	Nazwa raportu	Typ	Powtarzalność	Pokaż raport
<input checked="" type="checkbox"/>	Status aktualizacji	Status aktualizacji	cogodzinny	17 Lis 2014 - 13:44
<input type="checkbox"/>	Aktywność malware	Aktywność malware	cogodzinny	Raport nie został jeszcze ...

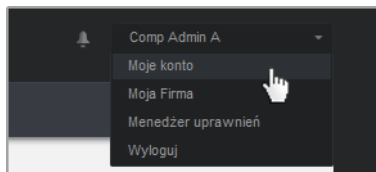


Strona Raportów - menu kontekstowe

2.3. Zarządzanie kontem

Żeby sprawdzić albo zmienić szczegółowe dane konta lub ustawić:

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



Menu konta użytkownika

2. W **Szczegóły konta**, popraw lub aktualizuje szczegóły twojego konta.
 - **Pełna nazwa.** Wprowadź swoje imię i nazwisko.

- **E-mail.** To jest twój login i kontaktowy adres e-mail. Raporty i ważne powiadomienia bezpieczeństwa będą wysyłane na ten adres. Powiadomienia e-mail są wysyłane automatycznie, gdy zostaną wykryte istotne ryzykowne warunki w sieci.
 - **Hasło.** Link **Zmień hasło** pozwala Ci na zmianę hasła logowania.
3. W **Ustawienia**, konfiguruj ustawienia konta zgodnie z własnymi preferencjami.
- **Strefa czasowa.** Wybierz z menu strefę czasową konta. Konsola wyświetli informację o czasie, w zależności od wybranej strefy czasowej.
 - **Język.** Wybierz z menu język wyświetlania w konsoli.
 - **Sesja wygasła.** Wybierz czas nieaktywności sesji zanim wygaśnie.
4. Naciśnij **Zapisz** aby zastosować zmiany.



Notatka

Nie możesz usunąć swojego własnego konta.

2.4. Zarządzanie twoją firmą

Jako użytkownik z rolą Administratora Firmy, możesz sprawdzić i zmienić szczegóły swojej firmy i ustawienia licencji:

1. Wskaż nazwę użytkownika w prawym górnym rogu konsoli i wybierz **Moja Firma**.

Szczegółowe informacje o firmie

Nazwa firmy:

Adresy:

ID:

Telefon:

Logo:

Logo musi mieć wielkość 200x30 px, oraz być w formacie png lub jpg

Pozwól innym firmom zarządzać bezpieczeństwem tej firmy

Licencja

Klucz licencyjny:

Data wygaśnięcia: 06 Paź 2018
Używany: 9
Dostępne do instalacji: 1
Całkowity: 10

Bitdefender Partner [Zmień](#)

Nazwa firmy:

ID:

Adresy:

Telefon:

Połącz tą firmę z MyBitdefender (opcjonalnie)

Strona Mojej Firmy

2. W **Szczegóły Firmy**, uzupełnij w informacjach twoich firmy, takie jak nazwa firmy, adres i telefon.
3. Możesz zmienić logo wyświetlane w Control Center jak również w raporcie twojej firmy i powiadomieniach e-mail, według poniższych:
 - Naciśnij **Zmiana** aby przeglądać obrazy logo na twoim komputerze. Obraz musi być w formacie .png lub .jpg i wielkość obrazu musi wynosić 200x30 pikseli.
 - Naciśnij **Domyślne** aby usunąć obraz i zresetować obraz do domyślnie dostarczonego przez Bitdefender.
4. Domyślnie, Twoja firma może być zarządzana przez konta partnerskie innych firm, które mogą mieć Twoją firmę wymienioną w swojej Bitdefender Control Center. Możesz blokować dostęp tych firm do swojej sieci przez wyłączenie opcji **Zezwól innym firmom na zarządzanie bezpieczeństwem firmy**. W rezultacie, Twoja sieć nie będzie już widoczna w innych Control Center przedsiębiorstw i nie będą one już w stanie zarządzać Twoją subskrypcją.
5. W sekcji **Licencja** możesz zobaczyć i zmodyfikować szczegóły Twojej licencji.

- Aby dodać nowy klucz licencyjny:
 - a. Z **Menu typ**, wybierz typ subskrypcji **Licencja**.
 - b. Podaj klucz licencyjny w polu **Klucz Licencyjny**.
 - c. Naciśnij przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o wpisanym kluczu licencyjnym.
 - Aby sprawdzić szczegóły twojego klucza licencyjnego, zobacz wyświetlone informacje poniżej klucza licencyjnego:
 - **Data wygaśnięcia** data do kiedy klucz licencyjny może być używany.
 - **Używane**: liczba używanych miejsc z ogólnej ilości miejsc w kluczu licencyjnym. Miejsce licencji używane w kliencie Bitdefender zainstalowane w punktach końcowych w zarządzanej sieci.
 - **Dostępne do zainstalowania**: liczba wolnych miejsc z ogólnej liczby miejsc z miesięcznej puli licencji (z wyjątkiem stosowanych miejsc).
 - **Całkowicie**: całkowita liczba dostępnych licencji dla twojej subskrypcji.
6. W **Partner Bitdefender** możesz znaleźć informacje na temat Twojego usługodawcy. Aby zmienić dostawcę usług zarządzalnych:
- a. Kliknij przycisk **Zmień**.
 - b. Wprowadź kod ID firmy partnerskiej w polu **ID Partnera**.



Notatka

Każda firma może znaleźć swoje ID na stronie **Moja Firma**. Po dokonaniu umowy z firmą partnerską, jej przedstawiciel musi dostarczyć Ci swój Control Center ID.

- c. Kliknij **Zapisz**.

W rezultacie, Twoja firma jest automatycznie przeniesiona z poprzedniej partnerskiej do nowej partnerskiej Control Center.
7. Opcjonalnie, możesz połączyć swoją firmę z kontem MyBitdefender używając odpowiednich pól.
8. Naciśnij **Zapisz** aby zastosować zmiany.

2.5. Zmiana hasła logowania

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

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

Aby zmienić hasło logowania:

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

3. Zarządzanie kontami użytkownika

Usługa Security for Endpoints może być ustawiona lub zarządzana z Control Center używając konta otrzymanego po subskrypcji usługi.

Wszystko co musisz wiedzieć o kontach użytkowników Small Office Security:

- Aby umożliwić innym pracownikom twojej firmy dostęp do Control Center, możesz stworzyć wewnętrzne konta użytkowników. Możesz przypisać konta użytkowników z różnymi rolami, zależnie od ich poziomu dostępu w firmie.
- Dla każdego konta użytkownika, możesz dostosować dostęp do funkcji Small Office Security lub do określonych części sieci, do których należy.
- Wszystkie konta z prawami **Zarządzanie Użytkownikami** można stworzyć, edytować lub usunąć inny użytkownik.
- Możesz zarządzać tylko kontami z równymi lub mniejszymi przywilejami dla konta.
- Możesz stworzyć lub zarządzać kontami użytkownika na stronie **Konta**.

Pełna nazwa	E-mail	Rola
Net Admin A	netadmina@bd.com	Administrator sieci
Reporter A	reportera@bd.com	Sprawozdawca

Strona Kont

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

- Nazwa użytkownika konta (używana do logowania do Control Center).
- Adres e-mail konta (używany jako adres kontaktowy). Raporty i ważne powiadomienia bezpieczeństwa będą wysyłane na ten adres. Powiadomienia e-mail są wysyłane automatycznie, gdy zostaną wykryte istotne ryzykowne warunki w sieci.
- Rola użytkownika (partner / administrator firmy / administrator sieci / reporter / inna).

3.1. Rola użytkownika

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



Notatka

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

Dostępne są następujące role użytkowników:

1. **Administrator Firmy** - Nadaje się dla menedżerów firm klientów, którzy zakupili Small Office Security licencję od partnera. Administrator firmy zarządza licencjami, profilami firmowymi i całym wdrożeniem Small Office Security, zezwalając na najwyższy poziom kontroli nad wszystkimi ustawieniami bezpieczeństwa (chyba, że zostaje zastąpiony przez dominujące konto partnera w scenariuszu dostawcy usług bezpieczeństwa). Administrator firmy może podzielić się lub przekazać swoje obowiązki operacyjne podległym kontu administracyjnym i reporterowi kont użytkowników.
2. **Administrator Sieci** - Kilka kont z rola Administratora może zostać stworzonych dla firmy, z przywilejami administracyjnymi na całą wdrożoną firmę Security for Endpoints lub dla określonych grup komputerów, zawierających zarządzanie użytkownikami. Administratorzy Sieci są odpowiedzialni za aktywne zarządzanie ustawieniami bezpieczeństwa sieci.
3. **Reporter** - Konto reportera jest kontem wewnętrznym tylko do odczytu. Pozwalają jedynie na dostęp do raportów i dzienników. Takie konta mogą być przydzielone dla pracowników z kontrolowaniem obowiązków lub dla innych pracowników którzy muszą utrzymywać wysoki stan bezpieczeństwa.
4. **Niestandardowe** - Wstępnie zdefiniowane role użytkowników obejmują pewna kombinacje praw użytkowników. Jeżeli wcześniej zdefiniowana rola użytkownika nie spełnia twoich oczekiwań, możesz stworzyć niestandardowe konto poprzez wybranie tylko tych praw, które cie interesują.

Poniższa tabela podsumowuje relacje między różnymi rolami kont i ich prawami. Aby uzyskać szczegółowe informacje, odwołaj się do „[Prawa użytkownika](#)” (p. 14).

Rola konta	Dopuszcza konta dzieci	Prawa użytkownika
Administrator firmy	Administratorzy firm, administratorzy sieci, Reporterzy	Zarządzaj Firmą Zarządzaj Użytkownikami Zarządzaj sieciami Zarządzaj Raportami
Administrator sieci	Administratorzy sieci, Reporterzy	Zarządzaj Użytkownikami

Rola konta	Dopuszcza konta dzieci	Prawa użytkownika
		Zarządzaj sieciami
		Zarządzaj Raportami
Sprawozdawca	-	Zarządzaj Raportami

3.2. Prawa użytkownika

Możesz przypisać prawa dla poniższych użytkowników do kont użytkowników Small Office Security:

- **Zarządzaj Użytkownikami.** Twórz, edytuj lub usuwaj konta użytkowników.
- **Zarządzaj Firmą.** Użytkownicy mogą zarządzać ich własnymi kluczami licencyjnymi Small Office Security i edytować ich ustawienia profilu firmy. Przywileje są określone dla kont administracyjnych firmy.
- **Zarządzaj sieciami.** Zapewnia uprawnienia administracyjne dla ustawień zabezpieczenia sieci (zasoby sieci, pakiety instalacyjne, kwarantanna). Przywilej ten jest specyficzny dla kont administratorów sieci.
- **Zarządzaj Raportami.** Twórz, edytuj, usuń raporty i zarządzaj panelem.

3.3. Tworzenie Kont Użytkowników

Przed stworzeniem konta użytkownika, upewnij się, że masz odpowiedni adres email pod ręką. Ten adres jest obowiązkowy aby utworzyć konto użytkownika Small Office Security. Użytkownicy dostaną szczegółowe dane logowania z Small Office Security na podany adres e-mail. Użytkownicy będą używać adresu e-mail również do logowania do Small Office Security

Aby utworzyć konto użytkownika:

1. Przejdź do strony **Konta**.
2. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
3. W sekcji **Szczegóły**, uzupełnij szczegółowe dane konta.
 - **E-mail.** Podaj adres e-mail użytkownika. Informacje logowania zostaną wysłane na ten adres niezwłocznie po utworzeniu konta.



Notatka

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

- **Pełna nazwa.** Podaj pełną nazwę dla właściciela konta.
4. W sekcji **Ustawienia i Przywileje**, skonfiguruj poniższe ustawienia:

- **Strefa czasowa.** wybierz z menu strefę czasową konta. Konsola wyświetli informację o czasie, w zależności od wybranej strefy czasowej.
 - **Język.** Wybierz z menu język wyświetlania w konsoli.
 - **Rola.** Wybierz rolę użytkownika. Aby uzyskać informacje o rolach użytkownika, odwołaj się do „[Role użytkownika](#)” (p. 13).
 - **Prawa.** Każda predefiniowana rola użytkownika ma pewną konfigurację praw. Jednak, powinieneś wybrać jedynie prawa, które potrzebujesz. W tym przypadku, rola użytkownika zmienia się na **Niestandardowe**. Aby uzyskać informacje o prawach użytkownika, odwołaj się do „[Prawa użytkownika](#)” (p. 14).
 - **Wybierz Cele.** Przewiń w dół okno konfiguracji aby wyświetlić potrzebną sekcję. wybierz grupę sieciową do której użytkownik będzie miał dostęp. Możesz zastrzec dostęp do określonych obszarów sieci.
5. Naciśnij **Zapisz** aby dodać użytkownika. Nowe konto pokaże się na liście kont użytkowników.



Notatka

Hasło dla każdego konta użytkownika jest automatycznie generowane podczas tworzenia konta i wysyłane do użytkownika wiadomością e-mail z innymi szczegółami dotyczącymi konta.

Możesz zmienić hasło po utworzeniu konta. Naciśnij nazwę konta na stronie **Konta** aby edytować hasło. Gdy hasło zostanie zmodyfikowane, użytkownik natychmiast zostanie powiadomiony przez e-mail.

Użytkownicy mogą zmieniać swoje hasło logowania z Control Center, uzyskując dostęp przez stronę **Moje konto**.

3.4. Edytowanie Kont

Edytuj konta aby zachować dane na bieżąco lub zmienić ustawienia konta.

Aby edytować konto użytkownika:

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



Notatka

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

3.5. Usuwanie kont

Usuwanie kont, gdy nie są już potrzebne. Na przykład, jeżeli właściciel konta nie pracuje już w firmie.

Aby usunąć konto:

1. Zaloguj do Control Center.
2. Przejdź do strony **Konta**.
3. Wybierz konto z listy.
4. Kliknij przycisk **Usuń** po prawej stronie tabeli.

3.6. Resetowanie haseł logowania

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

aby zresetować hasło logowania dla użytkownika:

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

4. Instalowanie Security for Endpoints

Security for Endpoints jest przeznaczony do komputerów i laptopów działających na systemach operacyjnych Windows i Mac OS X i serwerami Windows. Aby chronić komputery fizyczne z Security for Endpoints, musisz zainstalować Endpoint Security (oprogramowanie klienta) na któryś z nich. Endpoint Security zarządza ochroną na lokalnym komputerze. Komunikuje się również z Control Center aby otrzymać komendy administratora i wysłać wyniki przeprowadzonych działań.

Możesz zainstalować Endpoint Security z jedną z poniższych ról (dostępne w kreatorze instalacji):

1. **Punkt końcowy**, gdy odpowiadający komputer jest punktem końcowym.
2. **Endpoint Security Relay** gdy odpowiadający komputer jest używany przez inne punkty końcowe w sieci do komunikacji z Control Center. Rola Endpoint Security Relay instaluje Endpoint Security razem z aktualizacjami serwera, które mogą być użyte do aktualizacji wszystkich innych klientów w sieci. Punkty Końcowe w tej samej sieci mogą być konfigurowane przez polityki do komunikacji z Control Center poprzez jeden albo kilka komputerów z rolą Endpoint Security Relay. Gdy Endpoint Security Relay jest niedostępny, następny jest brany pod uwagę w celu zapewnienia komunikacji komputera z Control Center.



Ostrzeżenie

- Pierwszy komputer, na którym zainstalujesz zabezpieczenie musi mieć rolę Endpoint Security Relay, w przeciwnym razie nie będziesz w stanie wdrożyć Endpoint Security na innych komputerach w sieci.
- Komputer z rolą Endpoint Security Relay musi być włączony i widoczny online aby klienci mieli połączenie z Control Center.

Możesz zainstalować Endpoint Security na komputerze [poprzez uruchomienie pakietów lokalnie](#) lub [poprzez uruchomienie zadania zdalnie](#) z Control Center.

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

Endpoint Security ma minimalny interfejs użytkownika. Dopuszcza tylko użytkowników aby sprawdzić status ochrony i uruchomić podstawowe zadania bezpieczeństwa (aktualizacje i skanowanie), bez zapewnienia dostępu do ustawień.

Domyślnie, wyświetl język interfejsu użytkownika na chronionych komputerach jest ustawiony w czasie instalacji na język twojego konta.

Aby zainstalować interfejs użytkownika w innym języku na wybranych komputerach, możesz stworzyć pakiet instalacyjny i ustawić preferowany język w opcjach konfiguracyjnych pakietu.

Aby uzyskać więcej informacji o tworzeniu paczek instalacyjnych, odwołaj się do „[Tworzenie Endpoint Security pakietów instalacyjnych](#)” (p. 21).

4.1. Wymagania systemowe

4.1.1. Wspierane systemy operacyjne

Security for Endpoints aktualnie chroni następujące systemy operacyjne:

Systemy operacyjne stacji roboczych:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista z dodatkiem Service Pack 1
- Windows XP z dodatkiem Service Pack 2 64-bit
- Windows XP z Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Tablet i wbudowane systemy operacyjne:

- 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 Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP z wbudowanym Service Pack 2
- Windows XP Tablet PC Edition*

*Konkretne moduły systemu operacyjnego muszą być zainstalowane na Security for Endpoints, aby pracował.

Systemy operacyjne serwera:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 z Service Pack 1

- Windows Home Server

4.1.2. Wymagania Sprzętowe

- Procesor kompatybilny z Intel® Pentium:

Systemy operacyjne stacji roboczych

- 1 GHz lub szybszy dla Microsoft Windows XP SP3, Windows XP SP2 64 bit i Windows 7 Enterprise (32 i 64 bit)
- 2 GHz lub szybszy dla Microsoft Windows Vista SP1 lub wyższy (32 i 64 bit), Microsoft Windows 7 (32 i 64 bit), Microsoft Windows 7 SP1 (32 i 64bit), Windows 8
- 800 MHz lub szybszy dla Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded z Service Pack 2, Microsoft Windows XP Tablet PC Edition

Systemy operacyjne serwera

- Minimalnie: 2.4 GHz jednordzeniowy CPU
- Rekomendowane: 1.86 GHz lub szybszy Intel Xeon wielordzeniowy CPU

- **Wolna pamięć RAM:**

- Dla Windows: minimum 512 MB, rekomendowane 1 GB
- Dla MAC: minimum 1 GB

- **miejsce HDD:**

- 1.5 GB wolnego miejsca na dysku twardym



Notatka

Wymagane jest co najmniej 6 GB wolnego miejsca na dysku dla podmiotów z rolą Endpoint Security Relay, gdzie będą przechowywać wszystkie aktualizacje i pakiety instalacyjne.

4.1.3. Obsługiwane przeglądarki

Przeglądarka bezpieczeństwa Endpoint jest weryfikowana do pracy z następującymi przeglądarkami:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

4.1.4. Porty Komunikacji Small Office Security

Poniższa tabela zawiera informacje na temat portów używanych przez składniki Small Office Security:

Port	Użycie
80 (HTTP) / 443 (HTTPS)	Port używany do uzyskania dostępu do konsoli webowej Control Center.
80	Port serwera aktualizacji.
8443 (HTTPS)	port używany przez klienta/agenta oprogramowania do połączenia z Serwerem komunikacji.
7074 (HTTP)	Komunikacja z Endpoint Security Relay (jeżeli dostępne)

Aby otrzymać więcej informacji na temat portów Small Office Security, patrz [ten artykuł KB](#).

4.2. Przygotowywanie do Instalacji

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

1. Upewnij się, że komputery spełniają [minimalne wymagania sprzętowe](#). Dla niektórych komputerów, możesz potrzebować zainstalować ostatni dostępny service pack dla systemu operacyjnego lub wolne miejsce na dysku. Sprawdź listę komputerów, które nie spełniają niezbędnych wymogów, aby można było je wykluczyć z zarządzania.
2. Odinstaluj (nie tylko wyłącz) każde oprogramowanie antywirusowe, firewall lub ochronę Internetu z komputerów. Uruchomienie Endpoint Security jednocześnie z innym oprogramowaniem ochronnym na komputerze, może wpływać na ich działanie i spowodować problemy z systemem.

Wiele programów ochronnych jest niekompatybilne z Endpoint Security są automatycznie wykrywane i usuwane podczas instalacji. Aby nauczyć się więcej i sprawdzić listę wykrytych programów ochronnych, odwołaj się do [tego artykułu KB](#).



WAŻNE

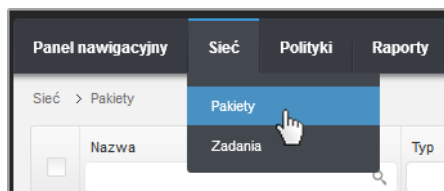
Nie musisz się bać o funkcje bezpieczeństwa Windows (Windows Defender, Windows Firewall), zostaną one wyłączone automatycznie przez rozpoczęciem instalacji.

3. Instalacja wymaga praw administracyjnych i dostępu do internetu. Upewnij się, że posiadasz niezbędne poświadczenia dla wszystkich komputerów.
4. Komputery muszą mieć połączenie z Control Center.

4.3. Instalacja lokalna

Jednym sposobem na instalację Endpoint Security na komputerze jest uruchomienie lokalnie pakietów instalacyjnych.

Możesz utworzyć pakiety instalacyjne według swoich potrzeb na stronie **Sieć > Pakiety**.



Sieć > Menu Pakietów



Ostrzeżenie

- Pierwszy komputer, na którym zainstalujesz zabezpieczenie musi mieć rolę Endpoint Security Relay, w przeciwnym razie nie będziesz w stanie wdrożyć Endpoint Security na innych komputerach w sieci.
- Komputer z rolą Endpoint Security Relay musi być włączony i widoczny online aby klienci mieli połączenie z Control Center.



Notatka

Gdy pierwszy klient zostanie zainstalowany, zostanie on wykorzystany do wykrycia innych komputerów w tej samej sieci, bazując na mechanizmie wykrywania sieci. Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „[Jak działa wyszukiwanie sieci](#)” (p. 29).

Aby zainstalować lokalnie Endpoint Security na komputerze, wykonaj 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 komputer.
3. [Uruchom pakiet instalacyjny](#) na komputerze.

4.3.1. Tworzenie Endpoint Security pakietów instalacyjnych

Stwórz paczkę instalacyjną Endpoint Security

1. Połącz się i zaloguj do Control Center używając twojego konta.
2. Przejdź do strony **Sieć > Pakiety**.

Nazwa	Język	Opis	Status
Relay	Polski		Gotowe do pobrania
Endpoint	Polski		Gotowe do pobrania

Strona Pakietów

3. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlone zostanie okno konfiguracji.

Endpoint Security

Szczegóły

Nazwa: *

Opis:

Ogólne

Rola:

Firma:

Moduły, które będą zainstalowane:

Antimalware ⓘ

Zapora sieciowa ⓘ

Kontrola zawartości

Ustawienia

Język:

Skanowanie przed instalacją

Użyj niestandardowej ścieżki instalacyjnej

Automatyczny restart systemu (jeżeli potrzebny)

Ustaw hasło deinstalacji

Hasło:

Potwierdź hasło:

Utwórz Paczki Endpoint Security - Opcje

4. Wpisz sugestywną nazwę i opis dla pakietów instalacyjnych, które chcesz stworzyć.

5. Wybierz docelową rolę komputera:
 - **Punkt końcowy.** Wybierz opcje do stworzenia pakietu dla stałego punktu końcowego.
 - **Endpoint Security Relay.** Wybierz tę opcję aby stworzyć pakiet dla punktu końcowego z rolą Endpoint Security Relay. Endpoint Security Relay jest specjalną rolą która instaluje uaktualnienia serwera na maszynach docelowych z Endpoint Security, który może być użyty do aktualizacji wszystkich innych klientów w sieci, obniżając zużycie pasma między maszynami klientów a Control Center.
6. Wybierz firmę w której pakiety instalacyjne będą używane.
7. Wybierz moduły ochrony, które chcesz zainstalować.
8. Z pola **Języki**, wybierz żądany język dla interfejsu klienta.
9. Wybierz **Skanuj przed instalacją** jeżeli jesteś pewny, że komputery są czyste przed instalacją Endpoint Security. Szybkie skanowanie w chmurze zostanie przeprowadzone na odpowiednich komputerach przed rozpoczęciem instalacji.
10. Endpoint Security jest zainstalowany w domyślnym katalogu instalacyjnym na wybranych komputerach. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** Jeżeli chcesz zainstalować Endpoint Security w innej lokalizacji. W tym przypadku, podaj ścieżkę docelową w odpowiednim polu. Użyj konwencji Windows podczas wprowadzania ścieżki (np. D:\folder. Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
11. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
12. Kliknij **Dalej**.
13. W zależności od roli pakietu instalacyjnego (Endpoint lub Endpoint Security Relay), wybierz wpis do tych komputerów docelowych, które będą okresowo łączyć się z klientach w celu aktualizacji:
 - **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:
 - **Endpoint Security Relay**, jeżeli chcesz połączyć punkt końcowy z Endpoint Security Relay zainstalowanych w twojej sieci. Wszystkie komputery z rolą Endpoint Security Relay wykryte w twojej sieci pokażą się w tabeli poniżej. Wybierz Endpoint Security Relay który chcesz. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego Endpoint Security Relay.

**WAŻNE**


Port 7074 musi być otwarty dla wdrożeń przez Endpoint Security Relay do pracy.

14. Kliknij **Zapisz**.

Nowe pakiety instalacyjne pojawią się na liście pakietów docelowej firmy.

4.3.2. Pobieranie pakietów instalacyjnych

Aby pobrać pakiety instalacyjne Endpoint Security:

1. Zaloguj się do Control Center z komputera na którym chcesz zainstalować ochronę.
2. Przejdź do strony **Sieć > Pakiety**.
3. Wybierz pakiety instalacyjne Endpoint Security, które chcesz pobrać.
4. Naciśnij przycisk  **Pobierz** po prawej stronie 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 instalację. 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.** Pełny zestaw jest używany do instalacji ochrony na komputerach z wolnym połączeniem z internetem. Pobierz ten plik na połączony z internetem komputer, następnie rozprosz go na innych komputerach używając zewnętrznych nośników pamięci lub udostępniając w sieci.



Notatka

Dostępne pełne wersje narzędzi:

- **Windows OS:** systemy 32-bit i 64-bit
- **Mac OS X:** tylko systemy 64-bit

Upewnij się, że instalujesz poprawną wersję oprogramowania.

5. Zapisz plik na komputerze.

4.3.3. Uruchamianie Pakietów Instalacyjnych

Aby instalacja działała, pakiety instalacyjne muszą działać używając uprawnień administratora lub na koncie administracyjnym.

1. Połącz się i zaloguj do Control Center.
2. Pobierz i skopiuj plik instalacyjny na komputer docelowy lub udostępnij w sieci z tego komputera.
3. Uruchom pakiet instalacyjny.
4. Postępuj według instrukcji na ekranie.

Gdy Endpoint Security zostanie zainstalowany, komputer pokaże się w zarządzaniu w Control Center (Strona **Sieć**) w ciągu kilku minut.

4.4. Instalacja Zdalna

Możesz lokalnie zainstalować pierwszego klienta dzięki roli Endpoint Security Relay, może to zająć kilka minut zanim inne komputery sieciowe zobaczą go w Control Center. Od tego momentu, możesz zdalnie zainstalować Endpoint Security na komputerach zarządzanych przez Ciebie przy użyciu zadania instalacji z Control Center.

Endpoint Security zawiera mechanizm automatycznego wykrywania sieci, która umożliwia wykrywanie innych komputerów, w tej samej sieci. Wykryte komputery są wyświetlane jako **niezarządzane komputery** na stronie **Sieci**.

Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „[Jak działa wyszukiwanie sieci](#)” (p. 29).

4.4.1. Zdalna instalacja wymagań Endpoint Security

Aby zdalna instalacja działała:

- Endpoint Security Relay musi być zainstalowany w Twojej sieci.
- Każdy komputer docelowy musi mieć włączone udostępnianie administracyjne. Skonfiguruj każdą docelową stację roboczą do używania zaawansowanej wymiany plików.
- Tymczasowo wyłącz Kontrolę Konta użytkownika na wszystkich komputerach z systemami operacyjnymi Windows, które zawierają tę funkcję zabezpieczeń (Windows Vista, Windows 7, Windows Server 2008, itp.). Jeśli komputery wchodzą w skład domeny, za pomocą polityki możesz wyłączyć kontrolę użytkownika zdalnie.
- Wyłącz lub zamknij zapore sieciową na komputerach. Jeśli komputery wchodzą w skład domeny, za pomocą polityki możesz wyłączyć zaporę sieciową Windows zdalnie.

4.4.2. Działanie zadań zdalnej instalacji Endpoint Security


Aby uruchomić zdalną instalację:

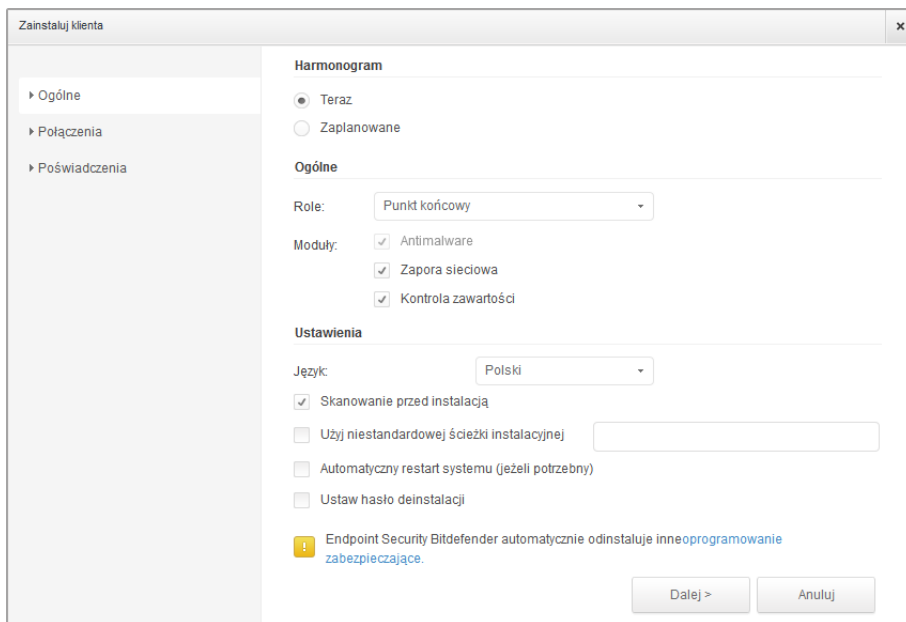
1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz żadaną grupę sieciową z lewego panelu bocznego. Jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.



Notatka

Opcjonalnie, możesz zastosować filtry, aby wyświetlić tylko komputery nie zarządzane. Naciśnij przycisk **Filtry** i wybierz poniższe opcje: **Niezarządzane** z kategorii **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z kategorii **Głębokość**.

4. Wybierz wpisy (komputery lub grupy komputerów), na których chcesz zainstalować ochronę.
5. Kliknij przycisk  **Zadania** po prawej stronie tabeli i wybierz **Instaluj klienta**. Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Endpoint Security z menu zadań

6. Skonfiguruj opcje instalacji:

- Harmonogram 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.

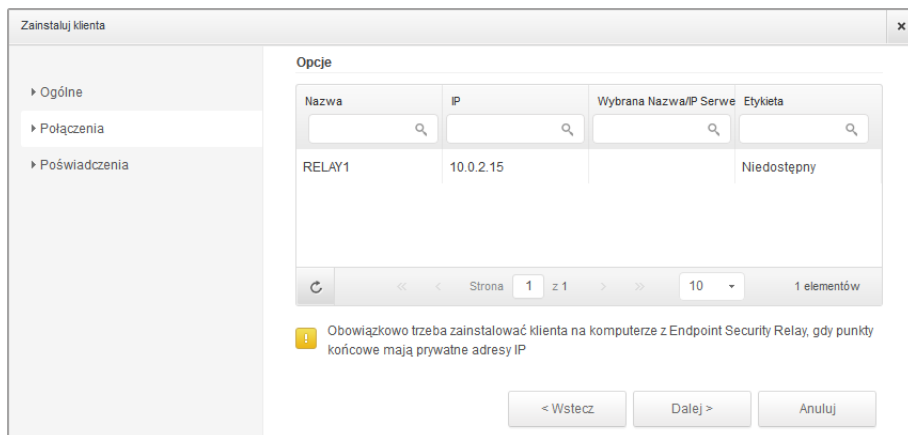


Notatka

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.

- Wybierz moduły ochrony, które chcesz zainstalować. Należy pamiętać, że tylko ochrona antymalware jest dostępna dla systemów operacyjnych serwera.
- Z pola **Języki**, wybierz żądany język dla interfejsu klienta.

- Wybierz **Skanuj przed instalacją** jeżeli jesteś pewny, że komputery są czyste przed instalacją Endpoint Security. Szybkie skanowanie w chmurze zostanie przeprowadzone na odpowiednich komputerach przed rozpoczęciem instalacji.
- Endpoint Security jest zainstalowany w domyślnym katalogu instalacyjnym na wybranych komputerach. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** Jeżeli chcesz zainstalować Endpoint Security w innej lokalizacji. W tym przypadku, podaj ścieżkę docelową w odpowiednim polu. Użyj konwencji Windows podczas wprowadzania ścieżki (np. D:\folder. Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
- Podczas cichej instalacji, komputer jest skanowany w poszukiwaniu malware. Czasami, system może potrzebować restartu aby ukończyć usuwanie malware.
Wybierz **Automatyczny restart (jeżeli potrzebny)** aby upewnić się, że wykryte malware zostało w pełni usunięte przed instalacją. W przeciwnym razie instalacja może się nie powieść.
- Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
- Kliknij **Dalej**.
- Na karcie **Połączenie** znajduje się lista punktów końcowych z rolą Endpoint Security Relay zainstalowanych w sieci. Każdy nowy klient musi być połączony z przynajmniej jednym Endpoint Security Relay z tej samej sieci, który będzie służyć do komunikacji i aktualizacji serwera. Wybierz Endpoint Security Relay jeżeli chcesz połączyć się z nowym klientem.



7. Kliknij **Dalej**.

8. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na wybranych punktach końcowych. Możesz dodać potrzebne poświadczenia przez wpisanie użytkownika i hasła dla docelowego systemu operacyjnego.



WAŻNE

Dla Windows 8.1 musisz podać poświadczenia wbudowanego konta administratora lub konta administratora domeny. Aby nauczyć się więcej, odwołaj się do [tego artykułu KB](#).



Notatka

Ostrzeżenie jest wyświetlane tak długo jak nie wybierzesz żadnych poświadczeń. Ten krok jest obowiązkowy dla instalacji zdalnych Endpoint Security na komputerach.

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

Użytkownik powinien użyć formy DOMENAWAZWA UŻYTKOWNIKA, gdzie DOMENA jest nazwą NetBios domeny.

< Wstecz Zapisz Anuluj

Aby dodać wymagane poświadczenia OS:

- a. Podaj nazwę użytkownika i hasło dla konta administracyjnego dla docelowego systemu operacyjnego w odpowiednich polach. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto. Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

Użyj konwencji systemu Windows podczas wprowadzania nazwy konta użytkownika domeny np. `user@domain.com` lub `domain\user`. Aby upewnić się, że podane poświadczenia będą działać, dodaj je w obu formach (`user@domain.com` i `domain\user`).



Notatka

Określone poświadczenia, zostaną zapisane automatycznie w menadżerze poświadczeń, więc nie będziesz musiał wprowadzać ich ponownie następnym razem.

- b. Kliknij przycisk **+** **Dodaj** . Konto jest dodane do listy poświadczeń.
 - c. Zaznacz pola odpowiadające kontom które chcesz używać.
9. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

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

4.5. Jak działa wyszukiwanie sieci

Security for Endpoints zawiera mechanizm automatycznego wykrywania sieci przeznaczonej do wykrywania komputerów grupy roboczej.

Security for Endpoints opiera się na **Usłudze Microsoft Computer Browser** do wyszukiwania sieci. Usługa przeglądania komputera jest technologią 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.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

Polecenie zobacz sieć

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



WAŻNE

Control Center nie używa informacji sieciowych z Active Directory ani z funkcji mapy sieci dostępnej w Windows Vista i późniejszych. Mapa sieci zależy od innych technologii wykrywania sieci: protokołu Link Layer Topology Discovery (LLTD).

Control Center nie jest aktywnie zaangażowana w działanie operacji usługi Przeglądania Komputerów Endpoint Security wysyła zapytanie tylko do usługi Przeglądarki Komputera dla listy stacji roboczych i serwisów obecnie widocznych w sieci i 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 Endpoint Security w sieci.

- Jeżeli Endpoint Security jest zainstalowany na komputerze grupy roboczej, tylko komputery z grupy roboczej będą widoczne w Control Center.
- Jeżeli Endpoint Security 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 Endpoint Security jest zainstalowany.

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 Endpoint Security 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 Endpoint Security wyświetli błąd podczas wykonywania zapytania, Control Center poczeka do następnego zaplanowanego zapytania, aby spróbować ponownie, bez wybierania innego Endpoint Security.

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

4.5.1. 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.

4.5.2. 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.
- 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.
- Dla Windows Vista lub wyższych wersji, wykrywanie sieci musi być włączone (**Panel Kontrolny > Centrum Wykrywania i Udostępniania > Zmień Zaawansowane Ustawienia udostępniania**).

Aby móc włączyć tę funkcję, musisz najpierw uruchomić poniższe 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 Endpoint Security wysyła zapytania do usługi Przeglądarki Komputerów muszą mieć możliwość rozpoznawania nazw NetBIOS.

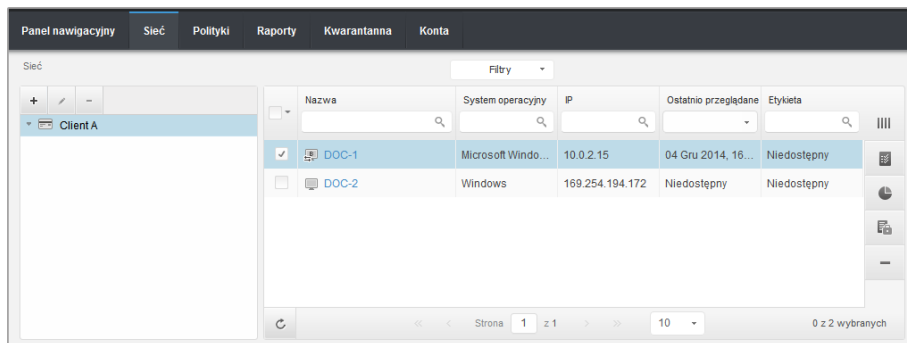


Notatka

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

5. Zarządzanie Komputerami

Strona **Sieć** udostępnia kilka funkcji do odkrywania i zarządzania dostępnymi komputerami. Zobacz **Sieć** składającą się z dwóch paneli interfejsu wyświetlających w czasie rzeczywistym statusu wszystkich obiektów sieciowych:



Strona Sieci

1. Lewy panel wyświetla dostępną strukturę drzewa sieci.



Notatka

Możesz przeglądać i zarządzać tylko grupami, które mają prawa administracyjne.

2. Prawy panel wyświetla zawartość grupy jaką wybrałeś na drzewie sieciowym. Ten panel składa się z siatki, w której wiersze zawierają obiekty sieciowe, a kolumny wyświetlają szczegółowe informacje dla każdego obiektu. Ten panel składa się z sieci, w której wiersze zawierają obiekty sieci i kolumny wyświetlania szczegółowych informacji dla każdego typu obiektu.

W tym panelu, możesz zrobić poniższe punkty:


- Zobacz szczegółowe informacje o każdym obiekcie sieciowym na twoim koncie. Możesz zobaczyć status każdego obiektu sprawdzając ikonę obok nazwy. Naciśnij nazwę obiektu aby wyświetlić okno zawierające więcej informacji.
- Użyj **Toolbar Akcji** po prawej stronie tabeli do wykonywania określonych czynności dla poszczególnych obiektów sieciowych (takich jak uruchamianie zadań, tworzenie raportów, przypisywanie polityk i usuwanie).
- [Odśwież Dane Tabeli.](#)

W sekcji **Sieć** możesz zarządzać [pakietami instalacyjnymi](#) i [listą zadań](#) dla każdego obiektu sieciowego.

Aby wyświetlić komputery przypisane do konta, przejdź do strony **Sieć** i wybierz żądaną grupę roboczą z lewej części strony.

Możesz przeglądać dostępne sieci komputerowe w lewym panelu i szczegóły każdego komputera w prawym panelu.

Aby dostosować szczegóły komputera wyświetlone w tabeli:







1. Naciśnij przycisk  **Kolumny** po prawej stronie nagłówka tabeli.
2. Wybierz nazwy kolumny jaką chcesz zobaczyć
3. Naciśnij przycisk **Reset** aby przywrócić domyślny widok kolumn.

W sekcji **Sieć**, możesz zarządzać komputerami, według poniższych:

- [Sprawdź Stan Komputera.](#)
- [Organizowanie Komputerów w Grupy](#)
- [Zobacz szczegóły komputera.](#)
- [Sortuj, filtruj i wyszukuj komputery.](#)
- [Uruchom zadania na komputerach.](#)
- [Twórz szybkie raporty.](#)
- [Przydziel polityki.](#)
- [Usuń komputery z zasobów sieci.](#)

5.1. Sprawdź Stan Komputera

Na stronie sieci, każdy komputer reprezentuje ikona określająca stan komputera. Zobacz statusy komputerów i odpowiednie ikony w poniższej tabeli:

Ikona Status	
	Komputer, Zarządzany, Bez problemów, Online
	Zarządzany komputer, z problemami bezpieczeństwa, online,
	Komputer, Zarządzany, Bez problemów, Offline
	Zarządzany komputer, z problemami bezpieczeństwa, Offline
	Niezarządzane
	Usunięto




Aby uzyskać szczegółowe informacje, odwołaj się do:

- [„Zarządzane, Niezarządzane i Usunięte Komputery”](#) (p. 34)
- [„Komputery Online i Offline”](#) (p. 34)

- „Komputery z problemami bezpieczeństwa” (p. 35)



5.1.1. Zarządzane, Niezarządzane i Usunięte Komputery

Komputery mogą mieć różne stany zarządzania:

-  **Zarządzane** - komputery których ochrona Endpoint Security jest zainstalowana.
-  **Niezarządzane** - wykryte komputery których ochrona Endpoint Security nie została jeszcze zainstalowana.
-  **Usunięte** - komputery które usunięto z Control Center. Aby uzyskać więcej informacji, odwołaj się do „Usuwanie komputerów z zasobów sieci” (p. 59).

5.1.2. Komputery Online i Offline

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

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

Komputer jest offline jeżeli Endpoint Security jest nieaktywny przez więcej niż 5 minut. Możliwe powody dlaczego komputery są offline:

- Komputer jest wyłączony, uśpiony albo w hibernacji.



Notatka

Komputery wirtualne pokazują się jako online, nawet gdy są one zablokowane lub użytkownik jest wylogowany.

- Endpoint Security nie ma połączenia z Bitdefender Control Center albo z przypisanym Endpoint Security Relay:
 - Komputer może być odłączony od sieci.
 - Zapora sieciowa lub router może blokować komunikację pomiędzy Endpoint Security i Bitdefender Control Center lub przypisany Endpoint Security Relay.
- Endpoint Security może zostać ręcznie odinstalowany z komputera, jeżeli komputer nie ma połączenia z Bitdefender Control Center lub z przypisanym Endpoint Security Relay. Normalnie, kiedy Endpoint Security jest ręcznie odinstalowywany z komputera, Control Center zostaje powiadomiona o tym zdarzeniu i komputer zostaje oznaczony jako niezarządzany.
- Endpoint Security może nie działać poprawnie.

Aby dowiedzieć się, jak długo komputery były nieaktywne:



1. Wyświetl tylko zarządzane komputery. Naciśnij menu **Filtry** znajdujące się poniżej tabeli, wybierz **Zarządzane (Punkty końcowe)** i **Zarządzane (Endpoint Security Relay)** w kategorii **Bezpieczeństwo** i naciśnij **Zapisz**.
2. Naciśnij nagłówek kolumny **Ostatnio Widziane** aby posortować komputery według okresu bezczynności.

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

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


5.1.3. Komputery z problemami bezpieczeństwa

Dotyczy stanu bezpieczeństwa tylko na zarządzanych komputerach. Sprawdź ikonę stanu wyświetlającą symbol ostrzeżenia, aby zidentyfikować komputery z problemami bezpieczeństwa.

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

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

- Ochrona antymalware jest wyłączona.
- Licencja Endpoint Security wygasła.
- Endpoint Security jest nieaktualny.
- Sygnatury są nieaktualne.
- Wykryto złośliwe oprogramowanie.

Jeśli zauważysz, komputer z problemami bezpieczeństwa, należy kliknąć jego nazwę, aby wyświetlić stronę **Szczegóły Komputera**. Możesz zidentyfikować problemy bezpieczeństwa poprzez ikonę . Sprawdź ikony podpowiedzi aby znaleźć więcej szczegółów. Mogą być potrzebne dalsze badania lokalne.

5.2. Organizowanie Komputerów w Grupy

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

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

W grupie **Siec** należącej do twojej firmy, możesz **utworzyć**, **usunąć**, **zmienić nazwę** i **przesunąć** grupy komputerów z niestandardowo zdefiniowaną strukturą drzewa.



WAŻNE

Proszę zwrócić uwagę na następujące:

- Grupa może zawierać zarówno komputery jak i inne grupy.
- Kiedy wybierasz grupę w lewym panelu, możesz zobaczyć wszystkie komputery z wyjątkiem tych umieszczonych w podgrupach. Aby zobaczyć komputery zawarte w grupie i jej podgrupy, naciśnij na menu **Filtry** znajdujące się poniżej tabeli i wybierz **Wszystkie elementy rekurencyjne** w sekcji **Głębokość**.

Tworzenie grup

Przed rozpoczęciem tworzenia grup, pomyśl dlaczego ich potrzebujesz i wymyśl schemat grup. Na przykład, możesz grupować komputery opierając się na jednej lub na kombinacji następujących kryteriów:


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

Aby zorganizować swoją sieć w grupy:

1. Wybierz grupę **Sieć** w lewym panelu bocznym.
2. Naciśnij przycisk **+** **Dodaj grupę** u góry lewego panelu bocznego.
3. Podaj sugestywną nazwę dla grupy i naciśnij **OK**.

Zmianianie nazw grup

Aby zmienić nazwę grupy:

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

Przenoszenie Grup i Komputerów

Możesz przesunąć grupy i użytkowników gdziekolwiek w hierarchii grupy **Sieć**. Aby przesunąć grupę lub użytkownika, przeciągnij i upuść go do nowej lokacji.




Notatka

Jednostka, która jest przenoszona odziedziczy ustawienia polityki nowej grupy macierzystej, chyba że inna polityka zostanie do niej przypisana. Aby uzyskać więcej informacji o dziedziczeniu polityk, odwołaj się do „Przypisywanie Polityk do obiektów sieci” (p. 72).

Usuwanie grup

Grupa nie może zostać usunięta jeżeli należy do niej przynajmniej jeden komputer. Przenieś wszystkie komputery z grupy, którą chcesz usunąć do innej grupy. Jeżeli grupa zawiera podgrupy, możesz przenieść wszystkie podgrupy, a nie indywidualne komputery.

Aby usunąć grupę:

1. Wybierz pusta grupę w prawym panelu **Strona Sieci**.
2. Naciśnij przycisk  **Usuń grupę** u góry lewego panelu bocznego. Czynności należy potwierdzić, klikając **Tak**.

5.3. Przeglądanie szczegółów komputera.

Możesz uzyskać szczegółowe informacje o każdym komputerze na stronie **Sieć**, takie jak OS, IP, data i czas ostatniej widoczności, itp.

Aby znaleźć szczegóły o komputerze:

1. Przejdź do strony **Sieć**.
2. Wybierz żądaną grupę sieciową z lewego panelu bocznego.
Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Możesz w łatwy sposób zidentyfikować stan komputera przez sprawdzenie odpowiedniej ikony. Aby uzyskać szczegółowe informacje, odwołaj się do „Sprawdź Stan Komputera” (p. 33).
4. Sprawdź informacje wyświetlane w kolumnach tabeli dla każdego komputera:
 - **Nazwa**: nazwa komputera.
 - **FQDN**: w pełni kwalifikowana nazwa domeny zawierająca nazwę hosta i nazwę domeny.
 - **OS**: system operacyjny zainstalowany na komputerze.
 - **IP**: adres IP komputera.
 - **Ostatnio Widziano**: szczegóły o stanie połączenia komputera.



Notatka

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


- **Etykieta:** etykieta dodana do komputera w oknie **Szczegóły Komputera**.
5. Naciśnij nazwę zarządzanego komputera, który Cię interesuje. Wyświetlono okno **Szczegóły komputera**.

- Przejdź do zakładki **Przegląd** aby znaleźć poniższe szczegóły:
 - Ogólne informacje o komputerze, takie jak nazwa, adres IP, system operacyjny, grupa nadrzędna i obecny stan. Możesz dodatkowo przypisać komputer z etykietą. Możesz szukać komputery za pomocą filtrowania etykiet używając kolumny **Etykieta** pola wyszukiwania z prawej strony kolumny strony **Sieć**.
 - Szczegóły bezpieczeństwa powiązane z Endpoint Security zainstalowanym na wybranym komputerze, takie jak zainstalowane moduły, przypisana polityka, status antymalware, status licencji, ostatnia aktualizacja, wersja produktu i sygnatur oraz złośliwe oprogramowanie wykryte w ciągu ostatnich 24 godzin. Możesz również uzyskać szybki przegląd ilości malware wykrytych na komputerze danego dnia.
 - Naciśnij **Generuj raport stanu malware** aby uzyskać dostęp do opcji raportu malware na wybranym komputerze.

Aby uzyskać więcej informacji, odwołaj się do „[Tworzenie raportów](#)” (p. 124)



Notatka

Każde wygenerowany problem bezpieczeństwa jest oznaczony ikoną . Sprawdź ikony podpowiedzi aby znaleźć więcej szczegółów. Mogą być potrzebne dalsze badania lokalne.

Szczegóły Komputera

Przegląd | Dzienniki | Połączeni Klienci

Ogólne

Nazwa: DOC-XP
 IP: 10.0.2.15
 Etykieta:
 System operacyjny: Microsoft Windows XP
 Grupa: Grupy niestandardowe
 Status: Online, ostatnio widziany w 14 Listopad 2014, 17:23:24

Bezpieczeństwo [Generuj raport o statusie malware](#)

Zainstalowane moduły: Antimalware, Zapora sieciowa, Kontrola zawartości
 Polityka: grupa1
 Antimalware: Włączony
 Status licencji: Zarejestrowany
 Ostatnia aktualizacja: 14 Listopad 2014, 16:42:14
 Wersja Produktu: 5.3.13.492
 Wersja sygnatur: 7.56116(10282854)
 Aktywność Malware (ostatnie 24h): Nie wykryto wirusów
 Wykryte Malware (ostatnie 24h): Niedostępny


Dane bezpieczeństwa oparte są na danych zebranych, gdy komputer był ostatnio online.

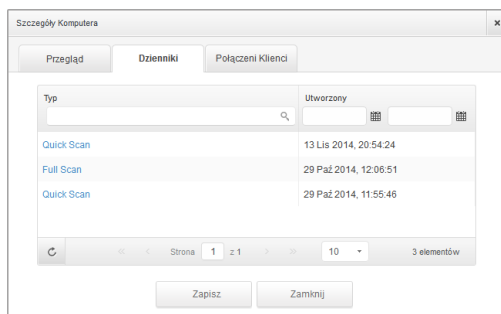
Zapisz | Zamknij

Szczegóły Komputera - Przegląd

- Sekcja **Endpoint Security Relay** (dostępna dla stałych klientów endpoint) wyświetla informacje o Endpoint Security Relay z którymi połączony jest komputer.
- Naciśnij zakładkę **Dzienniki Skanowania** aby zobaczyć szczegółowe informacje o wszystkich zadaniach skanowania przeprowadzone na komputerze. Naciśnij raport skanowania jaki Cię interesuje aby otworzyć nową stronę w przeglądarce.

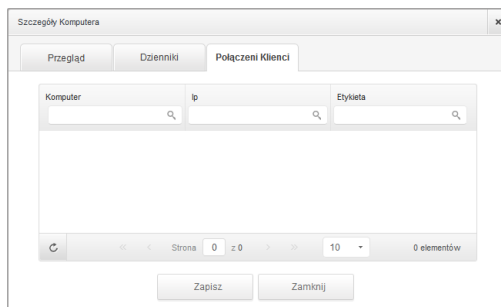
Do poruszania się po kolejnych stronach służą opcje nawigacji znajdujące się na dole tabeli. Jeżeli jest tam za dużo wpisów, możesz użyć opcji filtra dostępnych na górze tabeli.

Naciśnij przycisk  **Odśwież** w lewym dolnym rogu tabeli aby zaktualizować listę dziennika skanowania.



Szczegóły Komputera - Dzienniki Skanowania

- Dla komputerów z rolą Endpoint Security Relay, zakładka **Połączeni Klienci** jest dostępna, możesz w niej zobaczyć listę podłączonych punktów końcowych.



Szczegóły Komputera - Połączeni Klienci

5.4. Sortowanie, filtrowanie i wyszukiwanie komputerów.

W zależności od liczby komputerów, tabela komputerów może obejmować kilka stron (domyślnie tylko 10 wpisów jest wyświetlanych na jednej stronie). Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

Jeżeli jest za mało wpisów, możesz użyć pola wyszukiwania pod nagłówkiem kolumny w menu **Filtry** na górze tabeli, aby odfiltrować wyniki według daty. Na przykład, możesz szukać konkretnego komputera lub chcesz zobaczyć tylko zarządzane komputery.

5.4.1. Sortowanie komputerów

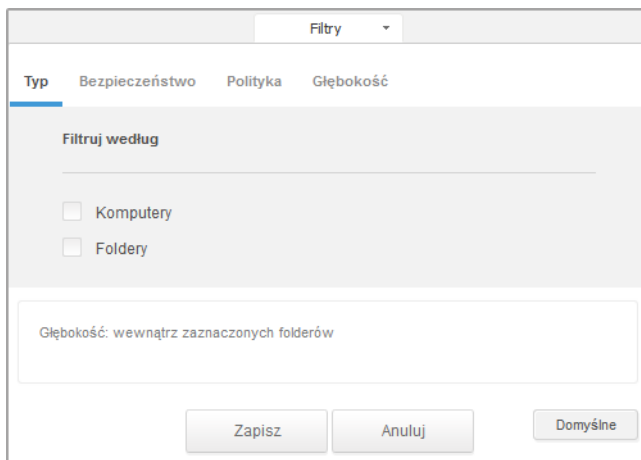
Aby posortować dane według określonych kolumn, naciśnij na nagłówek kolumny. Przykładowo, jeśli chcesz posortować komputery według nazwy, kliknij nagłówek **Nazwa**. Po ponownym kliknięciu komputery zostaną posortowane w odwrotnej kolejności.



Sortowanie komputerów

5.4.2. Filtrowanie komputerów

1. Wybierz żądaną grupę w lewym panelu bocznym.
2. Naciśnij menu **Filtry** znajdujące się w tabeli poniżej.
3. Wybierz kryteria filtrowania według:
 - **Typ**. Wybierz rodzaj wpisów jakie chcesz wyświetlić (komputery, foldery lub oba).



Filtry

Typ Bezpieczeństwo Polityka Głębokość

Filtruj według

Komputery

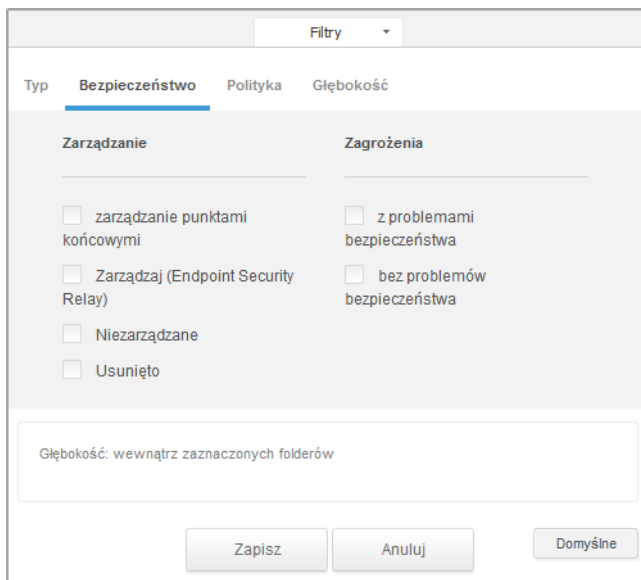
Foldery

Głębokość: wewnątrz zaznaczonych folderów

Zapisz Anuluj Domyślne

Komputery - Filtrowanie po Rodzaju

- **Bezpieczeństwo.** Wybierz aby wyświetlić komputery zarządzane i stan bezpieczeństwa.



Filtry

Typ **Bezpieczeństwo** Polityka Głębokość

Zarządzanie **Zagrożenia**

zarządzanie punktami
kończącymi

Zarządzaj (Endpoint Security
Relay)

Niezarządzane

Usunięto

z problemami
bezpieczeństwa

bez problemów
bezpieczeństwa

Głębokość: wewnątrz zaznaczonych folderów

Zapisz Anuluj Domyślne

Komputery - Filtrowanie po Bezpieczeństwie

- **Polityka.** Wybierz szablon polityki jakim chcesz filtrować komputery, rodzaj przypisania polityki (bezpośrednia lub dziedziczona), status przypisanej polityki (przypisana lub w toku).

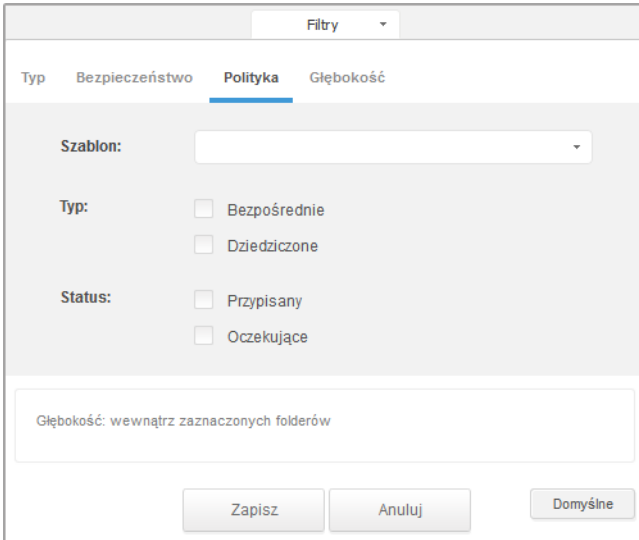


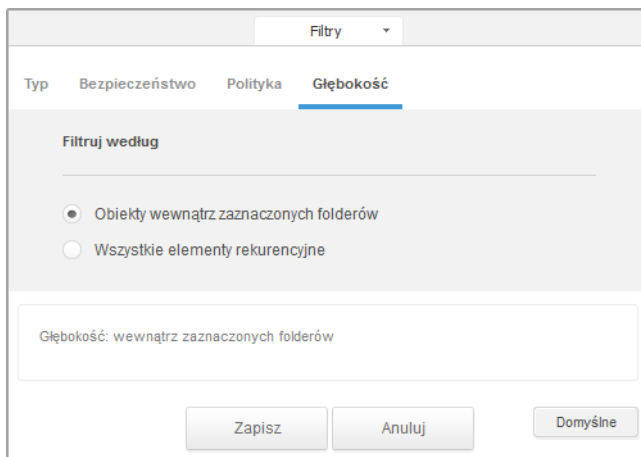
Diagram showing the 'Polityka' (Policy) filter settings in the Bitdefender interface. The interface includes a 'Filtry' (Filters) dropdown menu, tabs for 'Typ' (Type), 'Bezpieczeństwo' (Security), 'Polityka' (Policy), and 'Głębokość' (Depth). The 'Polityka' tab is active. The settings include:

- Szablon:** A dropdown menu.
- Typ:** Radio buttons for 'Bezpośrednie' (Direct) and 'Dziedziczone' (Inherited).
- Status:** Radio buttons for 'Przypisany' (Assigned) and 'Oczekujące' (Pending).
- Głębokość:** A text input field with the placeholder 'Głębokość: wewnątrz zaznaczonych folderów'.

Buttons at the bottom: 'Zapisz' (Save), 'Anuluj' (Cancel), and 'Domyślne' (Default).

Komputery - Filtrowanie po Polityce

- **Głębokość.** Kiedy zarządzasz strukturą drzewa komputerów sieciowych, komputery znajdujące się w podgrupach nie są wyświetlane gdy są wybrane grupy administracyjne. Wybierz **Wszystkie elementy rekurencyjnie** aby zobaczyć wszystkie komputery zawarte w obecnej grupie i podgrupach.



Komputery - Filtrowanie po Głębokości



Notatka


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

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

5.4.3. Wyszukiwanie komputerów

- Wybierz żądaną grupę w lewym panelu bocznym.
- Podaj wyszukiwaną frazę w odpowiednim polu pod nagłówkami kolumn (nazwa, OS lub IP) z prawego panelu bocznego. Na przykład, w polu **IP** podaj adres IP komputera, którego szukasz. Tylko pasujące komputery pokażą się w tabeli.

Wyczyść pole wyszukiwania aby wyświetlić pełną listę komputerów.

	Nazwa	System operacyjny	IP	Ostatnio przeglądane	Etykieta
<input type="checkbox"/>	bi				
<input type="checkbox"/>	 BI			Niedostępny	Niedostępny

Wyszukiwanie komputerów

5.5. Uruchamianie zadań na komputerach

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

Oto co możesz zrobić:

- „Skanowanie” (p. 44)
- „Zainstaluj klienta” (p. 51)
- „Modyfikuj instalator” (p. 54)
- „Odinstaluj Klienta” (p. 55)
- „Aktualizacja” (p. 56)
- „Uruchom ponownie komputer.” (p. 56)
- „Przeszukiwanie sieci” (p. 57)

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

Dla każdego komputera możesz rozpocząć kompatybilne zadania. Na przykład, jeżeli wybierzesz niezarządzany komputer, możesz tylko wybrać **Instalacja Klienta**, inne zadania będą nieaktywne.


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

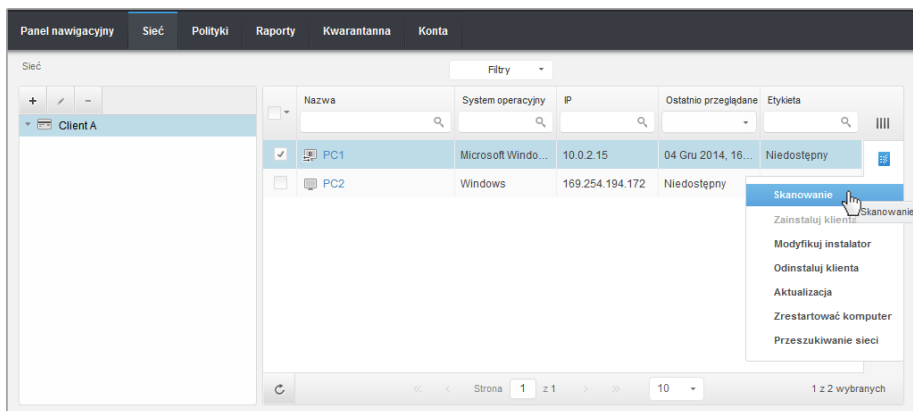
Po utworzeniu zadania, od razu uruchomi się na komputerach będących online w sieci. Jeżeli komputer jest offline, zadanie rozpocznie się zaraz po podłączeniu online.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).

5.5.1. Skanowanie

Aby uruchomić zadanie skanowania na kilku komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz żądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz pola odpowiadające komponentom które mają być zeskanowane.
4. Naciśnij przycisk  **Zadanie** po prawej stronie tabeli i wybierz **Skanowanie**.

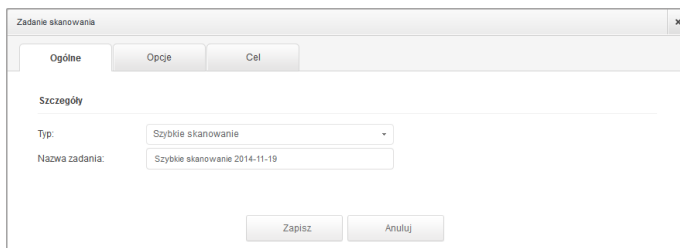


Zadanie skanowania komputerów

Wyświetlone zostanie okno konfiguracji.

5. Skonfiguruj opcje skanowania:

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



Zadanie skanowania komputerów - Konfigurowanie ustawień ogólnych

Wybierz rodzaj skanowania z menu **Rodzaj**:

- **Szybkie skanowanie** Do wykrywania w systemie złośliwego oprogramowania Szybkie Skanowanie wykorzystuje skanowanie w chmurze. Wykonanie Szybkiego Skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.

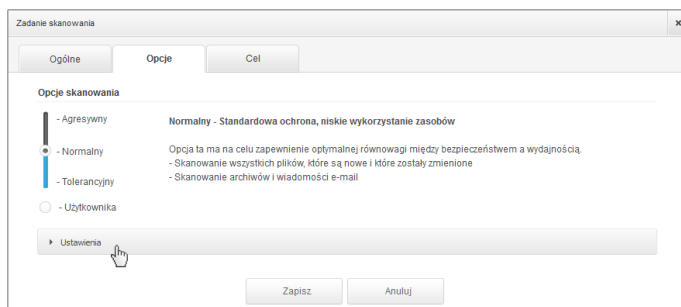


Notatka

Szybkie skanowanie wygrywa tylko istniejące malware, nie wykonuje innych akcji. Jeżeli malware zostało znalezione podczas Szybkiego Skanowania, musisz uruchomić Pełne Skanowanie Systemu aby usunąć wykryte malware.

- **Pełne Skanowanie** sprawdza cały komputer w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu, takiego jak wirusy, oprogramowanie typu spyware/adware, rootkity i inne.
- **Niestandardowe skanowanie** dopuszcza wybranie lokacji, które mają zostać przeskanowane i skonfigurować opcje skanowania. Zdefiniuj niestandardowe skanowanie:
 - Przejdź do zakładki **Opcje** aby ustawić opcje skanowania. Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

Bazując na wybranym profilu, opcje skanowania w sekcji **Ustawienia** zostaną automatycznie skonfigurowane. Jednak, jeżeli chcesz, możesz skonfigurować je szczegółowo. Aby to zrobić, zaznacz pole wyboru **Niestandardowe** i przejdź do sekcji **ustawienia**.



Zadanie skanowania komputerów

Dostępne są następujące opcje:

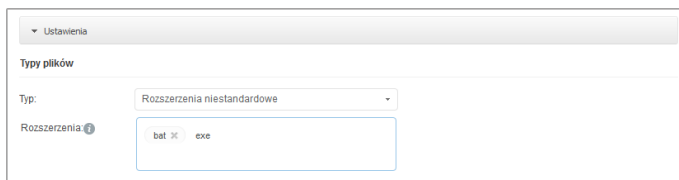
- **Typy plików.** Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Możesz ustawić Endpoint Security aby skanował pliki (niezależnie od rozszerzenia pliku), tylko pliki aplikacji lub określone rozszerzenia plików, które uważasz, że mogą być niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.



Notatka

Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „Lista Typów Plików Aplikacji” (p. 149).

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



Opcje zadania skanowania komputerów - Dodawanie niestandardowych rozszerzeń

- **Archiwa.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym. Zaleca się użycie tej opcji, w celu wykrycia i usunięcia wszelkich potencjalnych zagrożeń, nawet jeśli nie jest to zagrożenie bezpośrednie.



Notatka

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

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



Notatka

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

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

- **Skanowanie sektorów startowych.** Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu bootowania. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
- **Skanowanie rejestru.** Włącz tę opcję, aby skanować klucze rejestru. Rejestr Windows jest bazą danych przechowującą ustawienia konfiguracji i opcje dla komponentów systemu operacyjnego Windows oraz dla zainstalowanych aplikacji.
- **Skanowanie w poszukiwaniu rootkitów.** Zaznacz tę opcję, aby skanować w poszukiwaniu [rootkitów](#) ukrytych obiektów, które korzystają z tego rodzaju oprogramowania.
- **Skanuj w poszukiwaniu keyloggerów.** Zaznacz opcje skanowania dla oprogramowania [keylogger](#).
- **Skanowanie pamięci.** Wybierz tę opcję, aby przeskanować programy działające w pamięci systemu.
- **Skanowanie ciasteczek.** Wybierz tę opcję, aby przeskanować ciasteczka zapisane w przeglądarce.
- **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanuj w poszukiwaniu niepożądanych aplikacji (PUA).** Potencjalnie niechciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-supported). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.
- **Działania.** W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:
 - **Gdy zostanie wykryty zainfekowany plik.** Pliki, w których wykryto infekcje, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania Bitdefender. Endpoint Security można normalnie usunąć kod malware z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

W przypadku wykrycia zainfekowanego pliku Endpoint Security podejmie automatyczną próbę jego dezynfekcji. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.



WAŻNE

W przypadku określonych typów złośliwego oprogramowania dezynfekcja jest niemożliwa, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Przy wykryciu podejrzanego pliku**. Pliki są wykrywane jako podejrzone przez analizę heurystyczną. Ponieważ B-HAVE to technologia oparta na analizie heurystycznej, Endpoint Security nie może być pewny, że plik jest rzeczywiście zainfekowany przez szkodliwe oprogramowanie. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

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

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

Wykrywanie rootkitów i ukrywanie plików jest domyślnie ignorowane.

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

Wylecz

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

Przenieś do kwarantanny

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

Usuń

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

Ignoruj

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

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

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

- a. Wybierz wcześniej zdefiniowaną lokalizację z rozwijanego menu lub wprowadź **Określoną ścieżkę**, którą chciałbyś przeskanować.
- b. W polu edycji określ ścieżkę do obiektów, które mają zostać przeskanowane.
 - Jeżeli wybrałeś wcześniej zdefiniowaną lokalizację, wypełnij ścieżkę jeśli potrzebujesz. Na przykład, aby przeskanować folder `Program Files` wystarczy wybrać odpowiednią ścieżkę z rozwijanego menu. Aby przeskanować konkretny folder z `Program Files`, musisz uzupełnić ścieżkę dodając backslash (\) i nazwę folderu.
 - Jeżeli wybrałeś **Określona ścieżka**, podaj pełną ścieżkę do obiektu, który chcesz przeskanować. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych. Aby uzyskać więcej informacji dotyczących zmiennych systemowych, odwołaj się do „[Używa zmiennych systemowych](#)” (p. 149)
- c. Naciśnij przycisk **+ Dodaj**.

Aby edytować istniejącą lokalizację, kliknij ją. Aby usunąć lokalizację z listy, przesuń kursor nad nią, a następnie kliknij odpowiedni przycisk **- Usuń**.

Naciśnij sekcje **Wyjątki** jeżeli chcesz zdefiniować wyjątki w celach.

Typ Wyjątków	Pliki, foldery lub rozszerzenia	Akcja
Plik	Szczegółowe ścieżki	+

Zadanie skanowania komputerów - Definiowanie wyjątków.

Możesz korzystać z wykluczeń określonych przez politykę lub określić wyraźne wykluczenia dla bieżącego zadania skanowania. Aby uzyskać więcej informacji dotyczących wykluczeń, odwołaj się do „Wyjątki” (p. 96).

6. Kliknij **Zapisz**, aby utworzyć zadanie skanowania. Pojawi się nowa wiadomość potwierdzająca.
7. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).

5.5.2. Zainstaluj klienta

Aby chronić komputery dzięki Security for Endpoints, należy zainstalować Endpoint Security na każdym z nich.



Ostrzeżenie

- Pierwszy komputer, na którym zainstalujesz zabezpieczenie musi mieć rolę Endpoint Security Relay, w przeciwnym razie nie będziesz w stanie wdrożyć Endpoint Security na innych komputerach w sieci.
- Komputer z rolą Endpoint Security Relay musi być włączony i widoczny online aby klienci mieli połączenie z Control Center.

Po instalacji klienta Endpoint Security z rolą Endpoint Security Relay w sieci, automatycznie zostaną wykryte niechronione komputery w tej sieci.

Ochrona Security for Endpoints może być zainstalowana na tych komputerach zdalnie z Control Center.

Zdalna instalacja jest wykonywana w tle, bez wiedzy użytkownika.



Ostrzeżenie

Przed instalacją, należy odinstalować istniejące oprogramowanie antymalware i zapory sieciowej z komputerów. Instalując Security for Endpoints przy istniejącym oprogramowaniu bezpieczeństwa może wpływać na jego działanie i spowodować problemy z systemem. Windows Defender i Windows Firewall zostaną automatycznie wyłączone, gdy rozpocznie się instalacja.


Aby zdalnie zainstalować ochronę Security for Endpoints na jednym lub kilku komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę sieciową z lewego panelu bocznego. Jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.



Notatka

Opcjonalnie, możesz zastosować filtry, aby wyświetlić tylko komputery nie zarządzane. Naciśnij przycisk **Filtry** i wybierz poniższe opcje: **Niezarządzane** z kategorii **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z kategorii **Głębokość**.

3. Wybierz wpisy (komputery lub grupy komputerów), na których chcesz zainstalować ochronę.
4. Kliknij przycisk  **Zadania** po prawej stronie tabeli i wybierz **Instaluj klienta**. Kreator **Klienta Instalacji** został wyświetlony.
5. Skonfiguruj opcje instalacji:
 - Harmonogram 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.

- Wybierz role jakie chcesz by miał klient:
 - **Punkt końcowy**. Wybierz tę opcję jeżeli chcesz zainstalować klienta w stałym punkcie końcowym.
 - **Endpoint Security Relay**. Wybierz tę opcję aby zainstalować klienta z rolą Endpoint Security Relay na docelowym komputerze. Endpoint Security Relay jest specjalną rolą która instaluje uaktualnienia serwera na maszynach docelowych z Endpoint

Security, który może być użyty do aktualizacji wszystkich innych klientów w sieci, obniżając zużycie pasma między maszynami klientów a Control Center.

- Wybierz moduły ochrony, które chcesz zainstalować. Należy pamiętać, że tylko ochrona antymalware jest dostępna dla systemów operacyjnych serwera.
- Z pola **Języki**, wybierz żądany język dla interfejsu klienta.
- Wybierz **Skanuj przed instalacją** jeżeli jesteś pewny, że komputery są czyste przed instalacją Endpoint Security. Szybkie skanowanie w chmurze zostanie przeprowadzone na odpowiednich komputerach przed rozpoczęciem instalacji.
- Endpoint Security jest zainstalowany w domyślnym katalogu instalacyjnym na wybranych komputerach. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** Jeżeli chcesz zainstalować Endpoint Security w innej lokalizacji. W tym przypadku, podaj ścieżkę docelową w odpowiednim polu. Użyj konwencji Windows podczas wprowadzania ścieżki (np. D:\folder. Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
- Podczas cichej instalacji, komputer jest skanowany w poszukiwaniu malware. Czasami, system może potrzebować restartu aby ukończyć usuwanie malware.

Wybierz **Automatyczny restart (jeżeli potrzebny)** aby upewnić się, że wykryte malware zostało w pełni usunięte przed instalacją. W przeciwnym razie instalacja może się nie powieść.

- Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
- Kliknij **Dalej**.
- W zależności od roli klienta (Endpoint lub Endpoint Security Relay), wybierz w jaki sposób klienci będą się komunikować:
 - **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:
 - **Endpoint Security Relay**, jeżeli chcesz połączyć punkt końcowy z Endpoint Security Relay zainstalowanych w twojej sieci. Wszystkie komputery z rolą Endpoint Security Relay wykryte w twojej sieci pokażą się w tabeli poniżej. Wybierz Endpoint Security Relay który chcesz. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego Endpoint Security Relay.



WAŻNE

Port 7074 musi być otwarty dla wdrożeń przez Endpoint Security Relay do pracy.

6. Kliknij **Dalej**.

7. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na wybranych punktach końcowych.

Możesz dodać potrzebne poświadczenia przez wpisanie użytkownika i hasła dla docelowego systemu operacyjnego.



Notatka

Ostrzeżenie jest wyświetlane tak długo jak nie wybierzesz żadnych poświadczeń. Ten krok jest obowiązkowy dla instalacji zdalnych Endpoint Security na komputerach.

Aby dodać wymagane poświadczenia OS:

- a. Podaj nazwę użytkownika i hasło dla konta administracyjnego dla docelowego systemu operacyjnego w odpowiednich polach. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto. Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

Użyj konwencji systemu Windows podczas wprowadzania nazwy konta użytkownika domeny np. `user@domain.com` lub `domain\user`. Aby upewnić się, że podane poświadczenia będą działać, dodaj je w obu formach (`user@domain.com` i `domain\user`).




Notatka

Określone poświadczenia, zostaną zapisane automatycznie w menadżerze poświadczeń, więc nie będziesz musiał wprowadzać ich ponownie następnym razem.

- b. Kliknij przycisk **+** **Dodaj** . Konto jest dodane do listy poświadczeń.
 - c. Zaznacz pola odpowiadające kontom które chcesz używać.
8. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.
- Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).

5.5.3. Modyfikuj instalator

Aby zmienić moduły zabezpieczeń zainstalowanych na jednym lub kilku komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz pola odpowiadające zarządzanym komputerom, w których chcesz zmienić zainstalowane moduły ochronne.
4. Kliknij przycisk  **Zadanie** po prawej stronie tabeli i wybierz **Modyfikuj instalator**.
5. Wybierz w sekcji **Moduły** tylko te moduły ochrony, które chcesz by były zainstalowane:

Antimalware

Moduł antymalware chroni system przed wszelkimi rodzajami złośliwego oprogramowania (wirusami, trojanami, oprogramowaniem typu spyware/adware, rootkitami i nie tylko).

Zapora sieciowa

Zapora sieciowa chroni twój komputer przed niechcianymi połączeniami z zewnątrz i od środka.

Kontrola zawartości

Moduł Kontrola Treści pomaga kontrolować dostęp użytkowników do Internetu i aplikacji. Zwróć uwagę, że po skonfigurowaniu ustawień kontroli Treści, pokaże się wszystkim użytkownikom dziennik na docelowych komputerach.



Notatka

Należy pamiętać, że tylko ochrona antymalware jest dostępna dla systemów operacyjnych serwera.


6. Sprawdź opcję **Uruchom ponownie w razie potrzeby**, aby umożliwić automatyczne ponowne uruchomienie komputera w celu dokończenia instalacji.

7. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).

5.5.4. Odinstaluj Klienta

Aby zdalnie odinstalować ochronę Security for Endpointsz jednego lub kilku komputerów:

1. Przejdź do strony **Sieć**.
2. Wybierz żądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz odpowiednie pola dla komputerów, z których chcesz odinstalować ochronę Security for Endpoints.
4. Kliknij przycisk  **Zadanie** po prawej stronie tabeli i wybierz **Odinstaluj klienta**.
5. Pojawi się okno konfiguracji, które pozwala pozostawić pliki kwarantanny na maszynach klienta.
6. Naciśnij **Zapisz** aby utworzyć zadanie. Pojawi się nowa wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).



Notatka


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

5.5.5. Aktualizacja

Sprawdź status zarządzanych komputerów okresowo. Jeśli zauważysz, komputer z problemami bezpieczeństwa, należy kliknąć jego nazwę, aby wyświetlić stronę **Szczegóły Komputera**. Aby uzyskać więcej informacji, odwołaj się do „Komputery z problemami bezpieczeństwa” (p. 35).

Nieaktualni klienci lub podpisy reprezentujące nieaktualne kwestie bezpieczeństwa. W tym przypadku, musisz uruchomić aktualizacje dla określonego komputera. To zadanie może zostać zrobione lokalnie z komputera lub zdanie z Control Center.

Aby zdanie zaktualizować klienta i sygnatury na zarządzanych komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz pola dla komputerów, na których chcesz uruchomić klienta aktualizacji.
4. Naciśnij przycisk  **Zadanie** po prawej stronie tabeli i wybierz **Aktualizacja**. Wyświetlone zostanie okno konfiguracji.
5. Możesz wybrać aktualizacje jedynie produktu, bazy wirusów lub obu.
6. Naciśnij **Aktualizuj** aby uruchomić zadanie. Pojawi się nowa wiadomość potwierdzająca. Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).


5.5.6. Uruchom ponownie komputer.

Możesz wybrać zdalne zarządzanie uruchamianiem komputerów.



Notatka

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


1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz pola odpowiadające komputerom które chcesz ponownie przeskanować.
4. Kliknij przycisk  **Zadane** po prawej stronie tabeli i wybierz **Ponowne uruchomienie komputera**.
5. Wybierz opcje harmonogramu restartu:
 - Zaznacz **Uruchom ponownie teraz** aby natychmiast uruchomić komputer ponownie.

- Wybierz **Ponowne Uruchamianie włączone** i użyj pola poniżej do zaplanowania restartu komputera danego dnia o określonej porze.
6. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.
- Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).

5.5.7. Przeszukiwanie sieci


Wykrywanie sieci jest automatycznie ustawione każdej godziny przez Endpoint Security z rola Endpoint Security Relay. Możesz ręcznie uruchomić zadanie wyszukiwania sieci z Control Center w każdym momencie, zaczynając od maszyny chronionej przez Endpoint Security.

Aby uruchomić zadanie wykrywania sieci:

1. Przejdź do strony **Sieć**.
 2. Wybierz żadaną grupę komputerów z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
 3. Zaznacz pola odpowiadające komputerom które chcesz wyszukać w sieci.
 4. Kliknij przycisk  **Zadane** po prawej stronie tabeli i wybierz **Wyszukiwanie Sieci**.
 5. Pojawi się nowa wiadomość potwierdzająca. Naciśnij **Tak**.
- Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**. Aby uzyskać więcej informacji, odwołaj się do [Viewing and Managing Tasks](#).

5.6. Tworzenie szybkich raportów

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

1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
Opcjonalnie, możesz filtrować zawartość wybranej grupy jedynie przez zarządzane komputery.
3. Zaznacz pola odpowiadające komputerom które chcesz żeby były zawarte w raporcie.
4. Kliknij przycisk  **Raport** po prawej stronie tabeli i wybierz rodzaj raportu z menu. Sprawozdania z działania będą zawierać jedynie dane z ostatniego tygodnia. Aby uzyskać więcej informacji, odwołaj się do „[Dostępne rodzaje raportów](#)” (p. 121).
5. Konfiguracja opcji raportu. Aby uzyskać więcej informacji, odwołaj się do „[Tworzenie raportów](#)” (p. 124)

6. Kliknij **Wygeneruj**. Raport jest natychmiast wyświetlony. Czas wymagany do utworzenia raportów uzależniony jest od liczby wybranych komputerów.

5.7. Przypisywanie polityk

Ustawienia bezpieczeństwa na komputerach jest zarządzane przez [polityki](#).

W sekcji **Sieć** możesz zobaczyć zmiany i przypisane polityki dla każdego komputera w grupie komputerów.



Notatka


Możesz wyświetlać lub zmieniać ustawienia zabezpieczeń dla zarządzanych komputerów lub grup. Aby ułatwić zadanie, możesz [odfiltrować](#) zawartość tabeli tylko dla zarządzanych komputerów.

Aby zobaczyć przypisane polityki dla konkretnego komputera:

1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Naciśnij nazwę zarządzanego komputera, który Cię interesuje. Pojawi się szczegółowe okno.
4. W sekcji **Bezpieczeństwo**, naciśnij nazwę obecnej polityki, aby zobaczyć ustawienia.
5. Możesz zmienić ustawienia bezpieczeństwa jakie potrzebujesz, pod warunkiem, że właściciel polityki zezwala użytkownikom na wprowadzenie zmian w tej polityce. Pamiętaj, że wszystkie wprowadzone zmiany będą miały wpływ na inne komputery przypisane do tej samej polityki.

Aby uzyskać więcej informacji o zmianie polityk komputera, odwołaj się do „[Polityki Komputera](#)” (p. 74).

Aby przypisać politykę do komputera lub grupy:


1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz pole dla żadanego komputera lub grupy. Możesz wybrać jeden z kilku obiektów tego samego rodzaju tylko tego samego poziomu.
4. Kliknij przycisk  **Polityka** z prawej strony tabeli.
5. Dokonaj niezbędnych ustawień w oknie **Przypisanie polityki**. Aby uzyskać więcej informacji, odwołaj się do „[Przypisywanie Polityk do obiektów sieci](#)” (p. 72).

5.8. Usuwanie komputerów z zasobów sieci

Jeżeli nie planujesz zarządzać niektórymi wykrytymi komputerami, możesz wybrać wykluczenie ich z zasobów sieci. Dodatkowo, możesz na stałe usunąć wykluczone komputery z zasobów sieci.

5.8.1. Wykluczanie komputerów z zasobów sieci

Aby wykluczyć komputery z zasobów sieci:

1. Przejdź do strony **Sieć**.
2. Wybierz żądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Zaznacz pola opowiadające komputerowi, jaki chcesz wykluczyć.
4. Naciśnij przycisk  **Usuń** po prawej stronie tabeli. Czynności należy potwierdzić, klikając **Tak**.



Notatka

Jeżeli usuniesz zarządzany komputer, Endpoint Security automatycznie odinstaluje go.

Po usunięciu z komputera, nie będzie można go zobaczyć w tabeli. Usunięte komputery pozostają w bazie danych Small Office Security, ale nie są widoczne.

Możesz chcieć ponownie zarządzać niektórymi usuniętymi komputerami. W tym przypadku, musisz wyświetlić usunięte komputery i zainstalować Endpoint Security na tym który Ciebie interesuje. Aby wyświetlić usunięte komputery, naciśnij menu **Filtry** znajdujące się pod tabelą, następnie idź do zakładki **Bezpieczeństwo**, zaznacz opcje **Usunięte** i naciśnij **Zapisz**.

Komputery - Filtrowanie po usuniętych punktach końcowych



Notatka

Jeżeli reinstalujesz ochronę na wykluczonym komputerze, zostanie on wykryty jako zarządzany i przywrócony w tabeli.

5.8.2. Trwale usuwanie komputerów

Aby trwale usunąć komputery z zasobów sieci:

1. Przejdź do strony **Sieć**.
2. Wybierz żadaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Filtrowanie zawartości tabeli po **Usunięte** komputery.
4. Zaznacz pola opowiadające komputerom, jakie chcesz usunąć.
5. Naciśnij przycisk **Usuń** po prawej stronie tabeli. Czynności należy potwierdzić, klikając **Tak**.

Odpowiednie komputery zostaną trwale usunięte z bazy danych Small Office Security.



Ostrzeżenie

Nie możesz przywrócić trwale usuniętego komputera z bazy Small Office Security.

5.9. Pakiety Instalacyjne

Składniki ochrony Small Office Security mogą być zainstalowane w docelowych obiektach sieciowych poprzez wdrożenie ich z Control Center lub przez pobranie potrzebnych pakietów instalacyjnych i uruchomienie ich ręcznie na docelowych obiektach sieciowych.

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

5.9.1. Tworzenie pakietów instalacyjnych

Możesz potrzebować dostosować pakiety instalacyjne, aby lepiej dopasować je do potrzeb bezpieczeństwa.

Tworzenie Endpoint Security pakietów instalacyjnych

Stwórz paczkę instalacyjną Endpoint Security

1. Połącz się i zaloguj do Control Center używając twojego konta.
2. Przejdź do strony **Sieć > Pakiety**.

<input type="checkbox"/>	Nazwa	Język	Opis	Status	
<input type="checkbox"/>	Relay	Polski		Gotowe do pobrania	+
<input type="checkbox"/>	Endpoint	Polski		Gotowe do pobrania	↓

Strona Pakietów

3. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlone zostanie okno konfiguracji.

The screenshot shows the 'Endpoint Security' configuration window. On the left, there is a sidebar with 'Opcje' and 'Zaawansowane' options. The main area is titled 'Szczegóły' and contains several sections:

- Szczegóły:** Fields for 'Nazwa: *' and 'Opis:'.
- Ogólne:** A dropdown for 'Rola:' set to 'Punkt końcowy' and a dropdown for 'Firma:'.
- Moduły, które będą zainstalowane:** Three checked checkboxes: 'Antimalware', 'Zapora sieciowa', and 'Kontrola zawartości'.
- Ustawienia:** A dropdown for 'Język:' set to 'Polski', and four checkboxes: 'Skanowanie przed instalacją' (checked), 'Użyj niestandardowej ścieżki instalacyjnej', 'Automatyczny restart systemu (jeżeli potrzebny)', and 'Ustaw hasło deinstalacji'.
- Below the checkboxes are fields for 'Hasło:' and 'Potwierdź hasło:', each with a button to change or re-enter the password.

Utwórz Paczki Endpoint Security - Opcje

4. Wpisz sugestywną nazwę i opis dla pakietów instalacyjnych, które chcesz stworzyć.
5. Wybierz docelową rolę komputera:
 - **Punkt końcowy.** Wybierz opcje do stworzenia pakietu dla stałego punktu końcowego.
 - **Endpoint Security Relay.** Wybierz tą opcję aby stworzyć pakiet dla punktu końcowego z rolą Endpoint Security Relay. Endpoint Security Relay jest specjalną rolą która instaluje uaktualnienia serwera na maszynach docelowych z Endpoint Security, który może być użyty do aktualizacji wszystkich innych klientów w sieci, obniżając zużycie pasma między maszynami klientów a Control Center.
6. Wybierz firmę w której pakiety instalacyjne będą używane.
7. Wybierz moduły ochrony, które chcesz zainstalować.
8. Z pola **Języki**, wybierz żądany język dla interfejsu klienta.

9. Wybierz **Skanuj przed instalacją** jeżeli jesteś pewny, że komputery są czyste przed instalacją Endpoint Security. Szybkie skanowanie w chmurze zostanie przeprowadzone na odpowiednich komputerach przed rozpoczęciem instalacji.
10. Endpoint Security jest zainstalowany w domyślnym katalogu instalacyjnym na wybranych komputerach. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** Jeżeli chcesz zainstalować Endpoint Security w innej lokalizacji. W tym przypadku, podaj ścieżkę docelową w odpowiednim polu. Użyj konwencji Windows podczas wprowadzania ścieżki (np. D:\folder. Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
11. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
12. Kliknij **Dalej**.
13. W zależności od roli pakietu instalacyjnego (Endpoint lub Endpoint Security Relay), wybierz wpis do tych komputerów docelowych, które będą okresowo łączyć się z klientach w celu aktualizacji:
 - **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:
 - **Endpoint Security Relay**, jeżeli chcesz połączyć punkt końcowy z Endpoint Security Relay zainstalowanych w twojej sieci. Wszystkie komputery z rolą Endpoint Security Relay wykryte w twojej sieci pokażą się w tabeli poniżej. Wybierz Endpoint Security Relay który chcesz. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego Endpoint Security Relay.



WAŻNE


Port 7074 musi być otwarty dla wdrożeń przez Endpoint Security Relay do pracy.

14. Kliknij **Zapisz**.

Nowe pakiety instalacyjne pojawią się na liście pakietów docelowej firmy.

5.9.2. Pobieranie pakietów instalacyjnych

Aby pobrać pakiety instalacyjne Endpoint Security:

1. Zaloguj się do Control Center z komputera na którym chcesz zainstalować ochronę.
2. Przejdź do strony **Sieć > Pakiety**.
3. Wybierz pakiety instalacyjne Endpoint Security, które chcesz pobrać.
4. Naciśnij przycisk  **Pobierz** po prawej stronie 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 instalację. 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.** Pełny zestaw jest używany do instalacji ochrony na komputerach z wolnym połączeniem z internetem. Pobierz ten plik na połączony z internetem komputer, następnie rozproś go na innych komputerach używając zewnętrznych nośników pamięci lub udostępniając w sieci.



Notatka


Dostępne pełne wersje narzędzi:

- **Windows OS:** systemy 32-bit i 64-bit
 - **Mac OS X:** tylko systemy 64-bit
- Upewnij się, że instalujesz poprawną wersję oprogramowania.

5. Zapisz plik na komputerze.

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

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** po prawej stronie 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 adresie 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 **Zobacz linki instalacyjne**.
6. Kliknij **Wyślij**. E-mail zawierający link instalacyjny jest wysyłany do każdego podanego adresu e-mail.

5.10. Przeglądanie i zarządzanie zadaniami

Strona **Sieć > Zadania** pozwoli Ci zobaczyć i zarządzać wszystkimi zadaniami jakie stworzyłeś.

Gdy stworzyłeś zadanie dla jednego lub kilku obiektów sieciowych, możesz zobaczyć je w tabeli zadań.

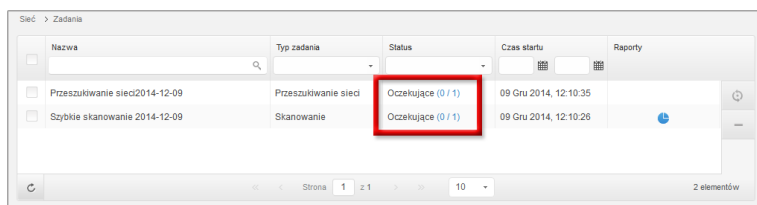
Możesz zrobić poniższe punkty ze strony **Sieć > Zadania**:

- [Sprawdź status zadania](#)
- [Zobacz raporty zadań](#)
- [Ponowne uruchomienie zadań](#)
- [Usuń zadania](#)

5.10.1. Sprawdzanie statusu zadania

Za każdym razem jak tworzysz zadanie dla kilku obiektów sieci, możesz chcieć sprawdzić postęp i dostać powiadomienie gdy wystąpi błąd.

Przejdź do strony **Sieć > Zadania** i sprawdź kolumnę **Status** dla każdego zadania jakie Cię interesuje. Możesz sprawdzić status głównego zadania i możesz uzyskać szczegółowe informacje o każdym pod zadaniu.



Strona Zadań

• Sprawdzenie statusu zadania głównego

Główne zadanie dotyczy działań rozpoczętych na obiektach sieciowych (takich jak instalacja klienta lub skanowanie) i zawiera pewną liczbę pod zadań, jedno dla każdego wybranego obiektu sieciowego. Na przykład, główne zadanie instalacyjne stworzone dla ośmiu komputerów zawiera osiem pod zadań. Liczby w nawiasach stanowią ilość zakończony pod zadań. Na przykład, (2/8) znaczy, że dwa z ośmiu pod zadań jest ukończonych.

Status głównego zadania może być:

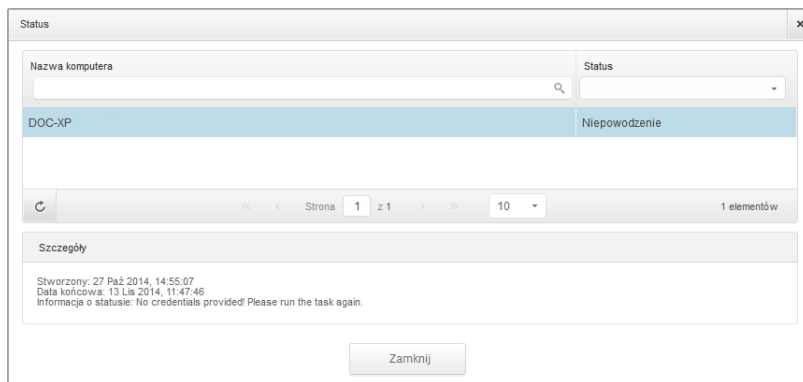
- **Oczekujące**, kiedy żadne z pod zadań jeszcze się nie rozpoczęło.
- **W trakcie**, kiedy wszystkie pod zadania są uruchomione. Status głównego zadania pozostaje jako W Trakcie tak długo aż nie skończy się ostatnie pod zadanie.
- **Zakończone**, kiedy wszystkie pod zadania są zakończone (powodzeniem lub niepowodzeniem). W przypadku nieudanych pod zadań, pojawi się symbol ostrzegawczy.

• Sprawdzenie statusu pod zadań

Przejdź do zadania, które Cię interesuje i wejdź w dostępny link w kolumnie **Status** aby otworzyć okno **Status**. Możesz zobaczyć listę obiektów sieci z przypisanymi zadaniami głównymi i statusem pod zadań. Status pod zadań może być:

- **W Trakcie**, kiedy pod zadania nadal działają.
- **Zakończone**, kiedy pod zadania są zakończone sukcesem.
- **Oczekujące**, kiedy pod zadania jeszcze się nie rozpoczęły. Może się to zdarzyć w następujących sytuacjach:
 - pod zadania czekają w kolejce.
 - Nie ma problemów z połączeniem Control Center i obiektów sieci docelowej.
- **Nie powiodło się**, kiedy pod zadania nie mogły się rozpocząć albo zostały zatrzymane przez błędy, takie jak niepoprawne uwierzytelnienie poświadczeń i za mała ilość pamięci.

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



Szczegóły statusu zadania


Możesz uzyskać informację na temat:

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

5.10.2. Przeglądanie raportów zadania


Na stronie **Sieć > Zadania** masz opcje żeby zobaczyć raporty zadań szybkiego skanowania.

1. Przejdź do strony **Sieć > Zadania**.
2. Zaznacz pole wyboru odpowiadające rodzajom skanowania zadań, którymi jesteś zainteresowany.

3. Naciśnij odpowiedni  przycisk z kolumny **Raporty**. Poczekaaj, aż zostanie wyświetlony raport. Aby uzyskać więcej informacji, odwołaj się do „[Używanie raportów](#)” (p. 121).

5.10.3. Ponowne uruchomienie zadań

Z różnych powodów, zadania instalacji klienta, dezinstalacji lub aktualizacji może nie zostać ukończona. Możesz wybrać czy uruchomić ponownie nieudane zadania zamiast tworzenia nowych, według następujących kroków:

1. Przejdź do strony **Sieć > Zadania**.
2. Wybierz pola wyboru odpowiadające nieudanym zadaniom.
3. Kliknij przycisk  **Uruchom ponownie** po prawej stronie tabeli. Wybrane zadania zostaną uruchomione ponownie i status zadań zostanie zmieniony na **Ponawianie**.




Notatka

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

5.10.4. Usuwanie zadań

Aby zapobiec zaśmieceniu listy zadań, zalecane jest usunąć zadania, które już nie będą potrzebne.

1. Przejdź do strony **Sieć > Zadania**.
2. Zaznacz pola odpowiadające zadaniom które mają zostać usunięte.
3. Kliknij przycisk  **Usuń** po prawej stronie tabeli. Czynności należy potwierdzić, klikając **Tak**.



Ostrzeżenie

Usuwanie oczekujących zadań, również anuluje zadanie.

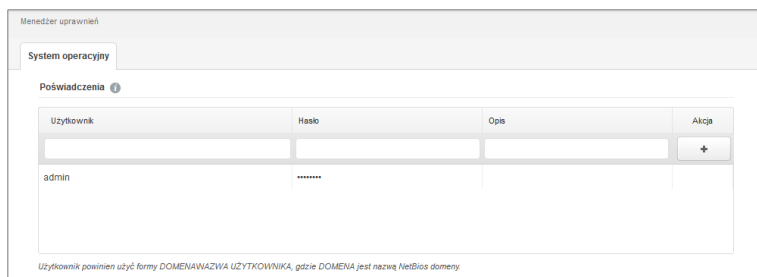
Jeżeli realizowane właśnie zadanie zostanie usunięte, wszystkie oczekujące podzadania zostaną anulowane. W tym przypadku, wszystkie podzadania nie zostaną ukończone.

5.11. Menedżer uprawnień

Menedżer poświadczeń pomaga zarządzać poświadczeniami wymaganymi do zdalnego uwierzytelniania różnych systemów operacyjnych w sieci.

Aby otworzyć Menedżera Poświadczeń, wskaż nazwę użytkownika w prawym górnym rogu konsoli i wybierz stronę **Zarządzanie Poświadczeniami**.

5.11.1. Dodawanie poświadczeń do Menadżera poświadczeń



Użytkownik	Hasło	Opis	Akcja
admin		+

Użytkownik powinien użyć formy DOMENAWAZWA UZYTEKOWNIKA, gdzie: DOMENA jest nazwą NetBios domeny.

Menedżer uprawnień

1. Podaj nazwę użytkownika i hasło dla konta administracyjnego dla docelowego systemu operacyjnego w odpowiednich polach. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto. Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

Użyj konwencji systemu Windows podczas wprowadzania nazwy konta użytkownika domeny np. `user@domain.com` lub `domain\user`. Aby upewnić się, że podane poświadczenia będą działać, dodaj je w obu formach (`user@domain.com` i `domain\user`).

2. Kliknij przycisk **+ Dodaj**. 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.

5.11.2. 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. Polityki Bezpieczeństwa

Po zainstalowaniu ochrony Bitdefender może być skonfigurowana i zarządzana z Control Center używając polityk bezpieczeństwa. Polityka dotycząca ustawień bezpieczeństwa zostanie zastosowana na komputerach.

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

Możesz stworzyć tak wiele polityk bazujących na wymaganiach bezpieczeństwa ile będziesz potrzebować.

To jest to co potrzebujesz, żeby wiedzieć o politykach:

- Polityki są tworzone na stronie **Polityki** i przypisane do obiektów sieciowych ze strony **Sieć**.
- Obiekty sieciowe mogą mieć tylko jedną aktywną politykę w tym samym czasie.
- Polityki są przekazywane do docelowych obiektów sieci natychmiast po utworzeniu lub modyfikacji. Ustawienia powinny być zastosowane na obiektach sieci w mniej niż minutę (jeżeli są one online). Jeżeli obiekty sieciowe nie są online, ustawienia nie będą stosowane tak długo jak nie pojawią się online.
- Polityka ma zastosowanie tylko do zainstalowanych modułów ochrony. Należy pamiętać, że tylko ochrona antymalware jest dostępna dla systemów operacyjnych serwera.
- Nie możesz edytować polityk stworzonych przez innych użytkowników (chyba że właściciel polityki dopuszcza to w ustawieniach polityki), ale nie możesz zmienić ich przypisując obiektom docelowym innej polityki.

6.1. Zarządzanie politykami

Możesz przeglądać i zarządzać politykami na stronie **Polityki**

Polityka	Nazwa polityki	Utworzono przez	Zmodyfikowany	Cele	Zastosowane/ Oczekujące	Firma
<input type="checkbox"/>	Polityka domyślna	admin@comp.com		0	1/ 1	

Strona Polityki

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

- Nazwa polityki.
- Użytkownik, który stworzył politykę.
- Data i czas ostatniej modyfikacji polityki.
- Liczba obiektów do których została wysłana polityka. Naciśnij liczbę celi jakie chcesz wyświetlić w zasobach sieciowych.
- Liczba celi dla których polityka została zastosowana / jest w toku. Naciśnij liczbę celi jakie chcesz wyświetlić w zasobach sieciowych.

Możesz [sortować](#) dostępne polityki i [wyszukać](#) niektórych polityk używając dostępnych kryteriów.

6.1.1. Tworzenie polityk

Możesz utworzyć polityki na dwa sposoby: dodaj nową politykę lub powiel (sklonuj) istniejącą politykę.

Aby utworzyć nową politykę:

1. Przejdź do strony **Polityki**.
2. Wybierz metodę tworzenia polityki:
 - **Dodaj nową politykę.**
 - Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Ta Komenda tworzy nową politykę używając domyślnego szablonu polityki.

- **Sklonuj istniejącą politykę.**
 - a. Zaznacz pole wyboru polityki jaką chcesz powielić.
 - b. Kliknij przycisk **Klonuj** po prawej stronie tabeli.
- 3. Konfiguruj ustawienia polityki. Aby uzyskać szczegółowe informacje, odwołaj się do „[Polityki Komputera](#)” (p. 74).
- 4. Naciśnij **Zapisz** aby utworzyć politykę i powrócić do listy polityk.

6.1.2. Zmiany ustawień polityk.

Ustawienia polityki mogą zostać wstępnie skonfigurowane podczas tworzenia polityki. Później, możesz je zmienić, w zależności od potrzeb, kiedy tylko chcesz.



Notatka

Domyślnie, tylko użytkownik, który stworzył politykę może ją modyfikować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

Aby zmienić ustawienia istniejącej polityki:

1. Przejdź do strony **Polityki**.
2. Znajdź politykę poszukiwaną politykę na liście i naciśnij jej nazwę by edytować.
3. Skonfiguruj ustawienia polityki według uznania. Aby uzyskać szczegółowe informacje, odwołaj się do „[Polityki Komputera](#)” (p. 74).
4. Kliknij **Zapisz**.

Polityki są wysyłane do docelowych obiektów sieci zaraz po zmianie polityki przypisanej lub później modyfikując ustawienia polityki. Ustawienia powinny być zastosowane na obiektach sieci w mniej niż minutę (jeżeli są one online). Jeżeli obiekty sieciowe nie są online, ustawienia nie będą stosowane tak długo jak nie pojawią się online.

6.1.3. Zmianie nazw polityk

Polityki powinny mieć sugestywne nazwy tak by administratorzy mogli szybko je zidentyfikować.

Aby zmienić nazwę polityki:

1. Przejdź do strony **Polityki**.
2. Naciśnij nazwę polityki. To otworzy stronę polityki.
3. Podaj nową nazwę dla polityki.
4. Kliknij **Zapisz**.

**Notatka**

Nazwa polityki jest unikalna. musisz podać inną nazwę dla każdej nowej polityki.

6.1.4. Usuwanie polityki

Jeżeli dłużej nie potrzebujesz polityki, usuń ją. Kiedy polityka zostanie usunięta, obiekty sieci, do których się ją stosuje zostaną przypisane do polityki grupy dominującej. Jeśli żadna inna polityka nie jest stosowana, ostatecznie będzie egzekwowana polityka domyślna.

**Notatka**

Domyślnie, tylko użytkownik, który stworzył politykę może ją skasować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

Aby usunąć politykę:

1. Przejdź do strony **Polityki**.
2. Zaznacz odpowiednie pole.
3. Kliknij przycisk **Usuń** po prawej stronie tabeli. Czynności należy potwierdzić, klikając **Tak**.

6.1.5. Przypisywanie Polityk do obiektów sieci

Jak zdefiniowałeś niezbędne polityki w sekcji **Polityki**, możesz przypisać je do obiektów sieci w sekcji **Sieć**.

Wszystkie obiekty sieciowe są początkowo przypisane do domyślnej polityki.

**Notatka**

Możesz przypisać tylko polityki które stworzyłeś. Aby przypisać politykę stworzona przez innego użytkownika, możesz ją najpierw sklonować na stronie **Polityki**.

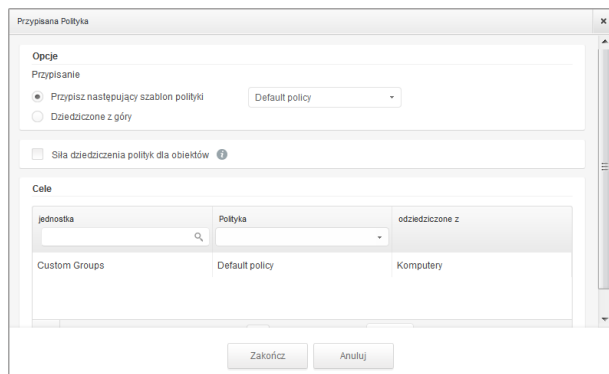
Aby przypisać politykę:

1. Przejdź do strony **Sieć**.
2. Zaznacz pole żądanego obiektu sieciowego. Możesz wybrać jeden z kilku obiektów tylko tego samego poziomu.
3. Kliknij przycisk **Przypisz Polityki** po prawej stronie tabeli.

**Notatka**

Możesz również nacisnąć prawym klawiszem mysz na grupę w drzewie sieci i wybrać **Przypisz politykę** z menu podręcznego.

Wyświetlono okno **Przypisania polityki**:



Ustawienia Przypisania Polityki

4. Skonfiguruj przypisanie ustawień polityki dla wybranych obiektów:

- Zobacz przypisanie obecnej polityki dla wybranych obiektów w tabeli poniżej sekcji **Cele**.
- **Przypisz następujący szablon polityki.** wybierz tę opcje aby przypisać obiekty docelowe z jedną polityką z wyświetlonego menu po prawej stronie. Tylko polityki stworzone z twojego konta będą dostępne w menu.
- **Dziedziczone z góry.** Wybierz opcje **Dziedziczenie z góry** aby przypisać wybrane obiekty sieciowe z grupy macierzystej polityki.
- **Siła dziedziczenia polityk dla obiektów.** Domyślnie, każdy obiekt sieciowy dziedziczy polityką grupy macierzystej. Jeżeli zmieniasz grupę polityki, będzie miało to wpływ na wszystkie dzieci tej grupy, z wyjątków członków grupy ze specjalnie przypisaną inną polityką.

Wybierz opcje **Dziedziczenie polityki przez obiekty** aby zastosować wybraną politykę dla grupy, w tym grup podrzędnych przypisanych do innej polityki. W tym przypadku, tabela poniżej wyświetla wybrane grupy podzędne, które nie dziedziczą polityki grupy.

5. Naciśnij **Zakończ** aby zapisać i potwierdzić zmiany.

Polityki są wysyłane do docelowych obiektów sieci zaraz po zmianie polityki przypisanej lub później modyfikując ustawienia polityki. Ustawienia powinny być zastosowane na obiektach sieci w mniej niż minutę (jeżeli są one online). Jeżeli obiekty sieciowe nie są online, ustawienia będą zastosowane jak tylko pojawią się online.

Aby sprawdzić czy polityka została poprawnie przypisana, przejdź do strony **Sieć** i naciśnij nazwę obiektu jaki cię interesuje w wyświetlonym oknie **Szczegóły**. Sprawdź sekcję **Polityka** aby zobaczyć stan obecnej polityki. Jeżeli w oczekiwaniu na stan, polityka nie została zastosowana do obiektu docelowego.

6.2. Polityki Komputera

Ustawienia polityki mogą zostać wstępnie skonfigurowane podczas tworzenia polityki. Później, możesz je zmienić, w zależności od potrzeb, kiedy tylko chcesz.

Aby skonfigurować ustawienia polityki:

1. Przejdź do strony **Polityki**.
 2. Naciśnij nazwę polityki. To otworzy stronę ustawień polityki.
 3. Skonfiguruj ustawienia polityki według uznania. Ustawienia pogrupowano w następujące kategorie:
 - [Ogólne](#)
 - [Antimalware](#)
 - [Zapora sieciowa](#)
 - [Kontrola zawartości](#)
- Możesz wybrać kategorie ustawień używając menu po lewej stronie.
4. Naciśnij **Zapisz** aby zapisać zmiany i zastosować je na komputerach docelowych. Aby opuścić stronę polityki bez zapisywania zmian, naciśnij **Anuluj**.



Notatka

Aby nauczyć się jak działają polityki, odwołaj się do „[Zarządzanie politykami](#)” (p. 70).

6.2.1. Ogólne

Ustawienia ogólne pomogą Ci zarządzać wyświetlaniem opcji interfejsu użytkownika, opcji komunikacji, preferencjami aktualizacji, ochroną hasłem i innymi ustawieniami Endpoint Security.

Ustawienia są zorganizowane w poniższych sekcjach:

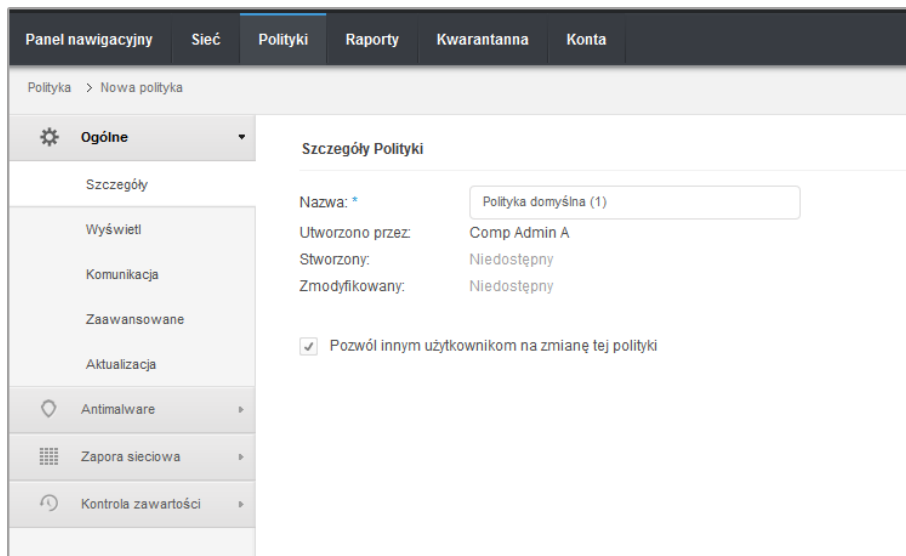
- [Szczegóły](#)
- [Wyświetl](#)
- [Komunikacja](#)
- [Zaawansowane](#)
- [Aktualizacja](#)

Szczegóły

Strona Szczegółów wyświetla ogólne szczegóły polityki:

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

- Data i czas ostatniej modyfikacji polityki



The screenshot shows the 'Polityki' (Policies) section in the Bitdefender Small Office Security interface. The navigation bar includes 'Panel nawigacyjny', 'Sieć', 'Polityki', 'Raporty', 'Kwarantanna', and 'Konta'. The breadcrumb trail is 'Polityka > Nowa polityka'. The left sidebar has a 'Szczegóły' (Details) section with options: 'Wyświetl' (View), 'Komunikacja' (Communication), 'Zaawansowane' (Advanced), 'Aktualizacja' (Update), 'Antimalware', 'Zapora sieciowa' (Firewall), and 'Kontrola zawartości' (Content Control). The main area is titled 'Szczegóły Polityki' (Policy Details) and contains the following information:

Nazwa: *	Polityka domyślna (1)
Utworzono przez:	Comp Admin A
Stworzony:	Niedostępny
Zmodyfikowany:	Niedostępny

Pozwól innym użytkownikom na zmianę tej polityki

Polityki Komputera

Możesz zmienić nazwę polityki poprzez dodanie nowej nazwy w polu **Zapisz**. Polityki powinny mieć sugestywne nazwy tak by administratorzy mogli szybko je zidentyfikować.



Notatka

Domyślnie, tylko użytkownik, który stworzył politykę może ją modyfikować. Aby zmienić właściciela polityki musisz sprawdzić opcje **Zezwalaj innym użytkownikom na zmianę polityki** ze strony polityki **Szczegóły**.

Wyświetl

W tej sekcji można skonfigurować opcje wyświetlania interfejsu użytkownika.

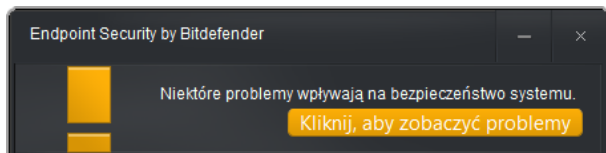
Polityki komputera - Wyświetl ustawienia

- **Włącz Tryb Cichy.** Użyj pola wyboru aby włączyć lub wyłączyć Tryb Cichy. Tryb Cichy jest zaprojektowany by pomóc Ci łatwo wyłączyć interakcje z użytkownikiem w Endpoint Security. Przelączając w tryb Cichy, poniższe zmiany zostaną wprowadzone do konfiguracji polityki:
 - Opcje **Wyświetl ikonę w obszarze powiadomień**, **Wyświetlaj powiadomienia pop-up** i **Wyświetlaj alerty pop-up** będą wyłączone w tej sekcji.
 - Jeżeli **poziom ochrony zapory sieciowej** jest ustawiony na **Zestaw reguł i zapytaj** lub **Zestaw reguł, znanych plików i zapytaj** można zmienić na **Zestaw reguł, znanych plików i zezwól**. W przeciwnym razie, ustawienia poziomu bezpieczeństwa nie zmienią się.
- **Pokaż ikonę w obszarze powiadomień.** Wybierz tę opcje aby wyświetlić ikonę Bitdefender **B** w obszarze powiadomień (znanym również jako zasobnik systemu) Ikona informuje użytkowników o ich statusie ochrony przez zmianę wyglądu i wyświetlenie odpowiedniego powiadomienia pop-up. Dodatkowo, użytkownicy mogą nacisnąć prawy klawisz myszy żeby szybko otworzyć główne okno Endpoint Security lub okno **O produkcie**. Otwieranie okna **O produkcie** automatycznie rozpoczyna aktualizację na żądanie.
- **Wyświetl powiadomienia pop-up.** Wybierz tę opcję aby informować użytkowników o ważnych zdarzeniach dotyczących bezpieczeństwa, takich jak wykrycie malware i podjęte działanie, poprzez małe powiadomienia pop-up. Powiadomienia pop-up znikną automatycznie po kilku minutach bez reakcji użytkownika.

- **Wyświetl powiadomienia pop-ups.** Inne dla powiadomień pop-up, alert pop-up powiadamia użytkowników o działaniu. Jeżeli wybierzesz aby nie wyświetlać alertów pop-up, Endpoint Security automatycznie wykona zalecane działanie. Alerty pop-up są generowane w poniższych sytuacjach:
 - Jeżeli zapora sieciowa jest ustawiana aby prosić użytkownika o podjęcie działania kiedy nieznanne aplikacje żądają dostępu do sieci lub internetu.
 - Jeżeli Aktywna Kontrola wirusów / System Wykrycia Intruzów jest są włączone, gdy zostaną wykryte potencjalnie niebezpieczne aplikacje.
 - Jeżeli skanowanie urządzenia jest włączone, gdy zewnętrzne urządzenie magazynujące jest połączone z komputerem. Możesz skonfigurować te ustawienia w sekcji **Antymalware > Na żądanie**
- **Alarmy statusu.** Użytkownicy określają, kiedy ich punkt końcowy ma skonfigurować problemy bezpieczeństwa lub inne ryzyko bezpieczeństwa, bazujące na statusie alertów. Na przykład, użytkownicy mogą zobaczyć jeżeli jest problem powiązany z ich ochroną antymalware, takie jak: moduł skanowania na żądanie jest wyłączony lub jest zaległe pełne skanowanie systemu.

Użytkownicy są informowani o ich statusie ochrony w dwa sposoby:

- Obszar powiadomień w głównym oknie, który wyświetla odpowiedni komunikat o stanie i zmienia kolor w zależności od nasilenia problemów bezpieczeństwa. Użytkownicy mają możliwość zobaczyć szczegóły problemów, przez kliknięcie dostępnego przycisku.



Obszar Powiadomień Endpoint Security



- Ikona Bitdefender **B** w zasobniku systemowym, która zmienia wygląd podczas wykrycia problemu.

Endpoint Security używa poniższego schematu kolorów w obszarze powiadomień:

- Zielone: Żadne problemy nie zostały wykryte.
- Pomarańczowy: Punkt końcowy nie ma krytycznych problemów wpływających na bezpieczeństwo. Użytkownicy nie muszą przerywać swojej pracy aby rozwiązać problemy.
- Czerwony: Punkt końcowy ma krytyczne problemy, które wymagają natychmiastowego działania.

aby skonfigurować status alertów, wybierz poziom powiadomień, który najbardziej ci pasuje (**Włącz wszystkie, Niestandardowy, Wyłącz wszystkie**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

Jeżeli chcesz dostosować powiadomienia:

1. Wybierz poziom **Niestandardowy**.
2. Nacisnij odnośnik **Ustawienia** aby otworzyć okno konfiguracyjne.
3. Wybierz aspekt ochrony, który chcesz by był monitorowany. Opcje są opisane tutaj:
 - **Ogólne**. stan alertu jest generowany podczas ponownego uruchamiania systemu, jest wymagany podczas lub po konserwacji produktu. Możesz wybrać aby wyświetlać alerty jako ostrzeżenia lub krytyczne problemy.
 - **Antimalware**. Alerty są generowane w poniższych sytuacjach:
 - Skanowanie na żądanie jest dostępne ale wiele lokalizacji plików jest pomijana.
 - Określona liczba dni, która minęła od ostatniego pełnego skanowania systemu wykonanego na maszynie.Możesz wybrać jak wyświetlać alerty i zdefiniować liczbę dni od ostatniego pełnego skanowania.
 - **Zapora sieciowa**. Alarm ten jest generowany, gdy Moduł Firewall jest wyłączony.
 - **Kontrola zawartości**. Alarm ten jest generowany, gdy Moduł Kontrola Treści jest wyłączony.
 - **Aktualizacja**. Alarm jest generowany, kiedy system wymaga ponownego uruchomienie aby zakończyć operacje aktualizacji. Możesz wybrać aby wyświetlić alert jako ostrzeżenie o krytycznych problemach.
- **Informacje o Pomocy Technicznej**. Możesz dostosować pomoc techniczną i dostępne informacje kontaktowe w Endpoint Security wpisując je w odpowiednie pola. Użytkownicy mają dostęp do tych informacji z okna Endpoint Security naciskając ikonę  w prawym dolnym rogu (lub naciskając prawym klawiszem myszy ikonę Bitdefender  w zasobniku systemowym i wybierając **O Programie**).

Komunikacja

Gdy wielu Endpoint Security Relay jest dostępnych w docelowych sieciach, możesz przypisać wybrane komputery z jednym albo kilkoma Endpoint Security Relay przez politykę.

Aby przypisać Endpoint Security Relay dla docelowych komputerów:

1. W tabeli **Przypisanie Komunikacji Punktu końcowego** naciśnij pole **Nazwa**. Wyświetlenie listy Endpoint Security Relay wykrytej w twojej sieci.
2. Wybierz jednostkę.

Polityki Komputera - Ustawienia Komunikacji

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

dodano Endpoint Security Relay do listy. Wszystkie komputery docelowe będą komunikować się z Control Center tylko przez określonego Endpoint Security Relay.

4. Zrób te same kroki, aby dodać kilka Endpoint Security Relay, jeżeli jest to możliwe.

5. Możesz skonfigurować Endpoint Security Relay priorytet używając strzałek góra i dół dostępnych po prawej stronie każdego wpisu. Komunikacja z docelowymi komputerami będzie przeprowadzona przez jednostkę na górze listy. Gdy nie można skomunikować się z tym wpisem, następnym zostanie wzięty do konta.

6. Aby usunąć wpis z listy, naciśnij przycisk **- Usuń** po prawej stronie tabeli.

Zaawansowane

W tej sekcji możesz skonfigurować ogólne ustawienia i hasło do odinstalowania.

Polityki Komputera - Ustawienia zaawansowane

- **Usuń zdarzenia starsze niż (dni).** Endpoint Security zapisuje wszelkie zdarzenia dotyczące jego aktywności na komputerze (włącznie z aktywnością komputera monitorowaną przez Kontrolę Zawartości) w szczegółowym dzienniku. Domyślnie, zdarzenia są usuwane z dziennika po 30 dniach. Jeżeli chcesz zmienić przedział, wybierz inne opcje z menu.
- **Złóż raport o awariach do Bitdefender.** Wybierz tę opcję żeby raporty zostały wysłane do Laboratorium Bitdefender w celu analizy awarii Endpoint Security. Raporty pomogą naszym inżynierom znaleźć co jest powodem problemu i zapobiec jego wystąpieniu następnym razem. Żadne prywatne informacje nie zostaną wysłane.
- **Konfiguracja hasła.** Aby uniemożliwić użytkownikom z prawami administracyjnymi odinstalowanie ochrony, należy ustawić hasło.

Hasło dezinstalacji może zostać skonfigurowana przed instalacją, dostosowując pakiet instalacyjny. Jeżeli to zrobisz, wybierz **Zatrzymaj obecne ustawienia** aby zachować obecne hasło.

Aby ustawić hasło, albo zmienić obecne hasło, wybierz **Włącz hasło** i podaj wybrane hasło. Aby usunąć ochronę hasłem, wybierz **Wyłącz hasło**.

Aktualizacja

W tej sekcji możesz skonfigurować Endpoint Security i ustawienia aktualizacji bazy wirusów. Aktualizacje są bardzo ważne ponieważ umożliwiają zwalczanie najnowszych zagrożeń.

Polityki komputera - Opcje Aktualizacji

- **Aktualizacja Produktu.** Endpoint Security automatycznie sprawdza co godzinę czy są aktualizacje, następnie je pobiera i instaluje (domyślne ustawienie). Automatyczne aktualizacje są wykonywane w tle.

- **Powtarzalność.** Aby zmienić częstotliwość automatycznej aktualizacji, wybierz inną opcję z menu i skonfiguruj ją według własnych potrzeb w kolejnych polach.
- **Przełóż ponowne uruchomienie.** Niektóre aktualizacje wymagają restartu systemu aby mogły zostać zainstalowane i działać poprawnie. Wybierając tę opcję, program będzie działał ze starszymi plikami, dopóki komputer nie zostanie uruchomiony ponownie, nie informując o tym użytkownika. W przeciwnym przypadku, powiadomienie w interfejsie użytkownika poprosi użytkownika o ponowne uruchomienie systemu, gdy aktualizacja będzie tego wymagać
- Jeżeli zdecydujesz się uruchomić ponownie później, możesz ustawić dogodny czas, w którym komputer automatycznie uruchomi się ponownie, jeżeli nadal będzie potrzebował. Może to być bardzo przydatne dla serwerów. Wybierz **Jeżeli potrzeba, uruchom ponownie po instalacji aktualizacji** i określ, kiedy jest to wygodne aby ponownie uruchomić komputer (codziennie lub co tydzień w określonym dniu, o określonej porze dnia).
- **Aktualizacja Sygnatur.** Endpoint Security automatycznie sprawdza co godzinę czy ma aktualną bazę wirusów (domyślne ustawienie). Automatyczne aktualizacje są wykonywane w tle. Aby zmienić częstotliwość automatycznej aktualizacji, wybierz inną opcję z menu i skonfiguruj ją według własnych potrzeb w kolejnych polach.
- **Ustawienia Proxy.** Wybierz tę opcję jeżeli komputer łączy się z Internetem (lub z lokalnym serwerem aktualizacji) przez serwer proxy. Są trzy sposoby na zmianę ustawień proxy:
 - **Zaimportuj ustawienia proxy z domyślnej przeglądarki.** Endpoint Security może zaimportować ustawienia proxy z większości popularnych przeglądarek, m.in. z najnowszych wersji przeglądarek Internet Explorer, Mozilla Firefox oraz Opera.
 - **Automatyczne wykrywanie sieci proxy.** Endpoint Security wykorzystuje protokół Web Proxy Auto-Discovery (WPAD) dołączony do systemu Windows, aby automatycznie pobrać ustawienia serwera proxy z pliku Proxy Auto-Configuration (PAC) opublikowanego w sieci lokalnej. Jeśli żaden plik PAC nie jest dostępny, aktualizacja nie powiedzie się.
 - **Użyj własnych ustawień proxy.** Jeżeli znasz ustawienia proxy, wybierz tę opcję i określ je:
 - **Serwer** – wpisz IP serwera proxy.
 - **Port** – wpisz port używany do łączenia z serwerem proxy.
 - **Nazwa użytkownika** - wpisz nazwę użytkownika rozpoznawanego przez proxy.
 - **Hasło proxy** - wpisz poprawne hasło dla wcześniej podanego użytkownika.

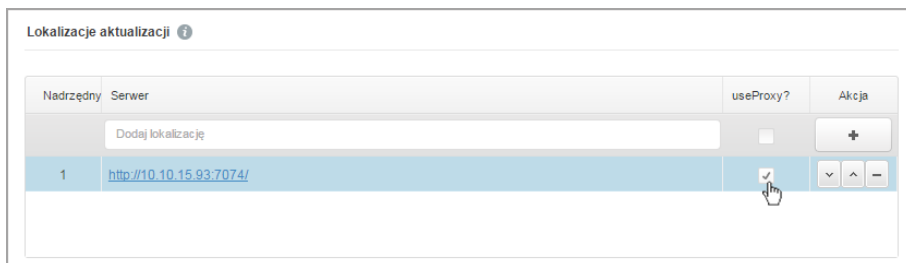


Notatka

Zmiana opcji konfiguracyjnych proxy nadpisze istniejące ustawienia proxy w Endpoint Security.

Dodatkowo, musisz wybrać **Użyj Proxy** zaznacz pole odpowiadające lokacji aktualizacji gdzie ustawienia są zastosowane (Internet lub lokalny adres serwera aktualizacji).

- **Lokalizacje aktualizacji.** Aby uniknąć przeciążenia ruchu w sieci zewnętrznej Endpoint Security jest skonfigurowany aby aktualizować się z <http://upgrade.bitdefender.com>. Możesz również dodać inne lokalne serwery aktualizacji do listy i skonfigurować ich priorytet używając przycisków góra i dół, które wyświetlą się po nakierowaniu myszką. Jeśli pierwszy serwer aktualizacji jest niedostępny, następny zostanie sprawdzony i tak dalej.



Polityki komputera - Lokalizacja Aktualizacji

Aby ustawić adres lokalnych aktualizacji:

1. Podaj adres lokalnego serwera aktualizacji w polu **Dodaj lokalizację**. Użyj jednej z tych składni:
 - aktualizacja_serwer_ip:port
 - aktualizacja_serwer_nazwa:port
 Domyślny port 7074.
2. Jeżeli klient komputerów łączy się do lokalnego serwera aktualizacji przez serwer proxy, wybierz **Użyj Proxy**.
3. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli.
4. Użyj strzałek ▲ Góra / ▼ Dół w kolumnie **Działanie** aby ustawić adres lokalnej aktualizacji jako pierwszy na liście. Nakieruj kursor myszy nad odpowiedni wiersz aby strzałki stały się widoczne.

Aby usunąć lokalizację z listy, przesunij kursor nad nią, a następnie kliknij odpowiedni przycisk **- Usuń**. Można usunąć domyślną lokalizację, jednak nie jest to zalecane.

6.2.2. Antimalware

Moduł antymalware chroni system przed wszelkimi rodzajami złośliwego oprogramowania (wirusami, trojanami, oprogramowaniem typu spyware/adware, rootkitami i nie tylko). Ochrona jest podzielona na dwie kategorie:

- Skanowanie dostępowe: - nie dopuszcza, aby nowe szkodliwe oprogramowanie dostało się do systemu.

- Skanowanie na żądanie - funkcja ta służy do wykrywania i usuwania złośliwego oprogramowania zainstalowanego w systemie.

W przypadku wykrycia wirusa lub innego złośliwego oprogramowania, Endpoint Security dokona automatycznej próby usunięcia kodu złośliwego oprogramowania z zainfekowanego pliku i odtworzenia oryginalnego pliku. Ta operacja określana jest mianem dezynfekcji. Plików, których nie można zdezynfekować, są poddawane kwarantannie, aby izolować infekcję. Kiedy wirus znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być uruchomiony lub otwierany.

Zaawansowani użytkownicy mogą skonfigurować wyjątki, aby pominąć określone pliki lub typy plików podczas skanowania.

Ustawienia są zorganizowane w poniższych sekcjach:

- [Dostępowe](#)
- [Na żądanie](#)
- [Wyjątki](#)
- [Kwarantanna](#)

Dostępowe

W tej sekcji możesz skonfigurować ochronę dla dwóch elementów ochrony antymalware w czasie rzeczywistym.

Ogólne >

Antimalware >

Dostępowe

Na żądanie

Wyjątki

Kwarantanna

Zapora sieciowa >

Kontrola zawartości >

Skanowanie dostępne Ustawienia

- Agresywny Normalny - Standardowa ochrona, niskie wykorzystanie zasobów

- Normalny Opcja ta ma na celu zapewnienie optymalnej równowagi między bezpieczeństwem a wydajnością.

- Tolerancyjny - Chroni przeciw każdemu typem malware przez skanowanie:

- Użytkownika - Wszystkich dostępnych plików z dysków lokalnych i aplikacji z dysków sieciowych (z wyjątkiem archiwów i plików prawie zerowym ryzykiem)

Aktywna Kontrola Wirusów

Domyślne działanie na zainfekowanych aplikacjach: Wylecz

- Agresywny Normalny - Zalecany w większości systemów

- Normalny Ta opcja ustawia wykrywanie wirusów przez Bitdefender na poziom średni. Mogą pojawić się fałszywe powiadomienia (czyste aplikacje mogą zostać uznane za szkodliwe).

- Tolerancyjny

Polityki Komputera - Ustawienia Na żądanie

- [Skanowanie dostępne](#)
- [Aktywna Kontrola Wirusów](#)

Ustawienia skanowania dostępowego

Skanowanie na żądanie zapobiega przed dostaniem się nowego malware do systemu przez skanowanie lokalne i plików sieciowych podczas dostępu do nich (otwieranie, przenoszenie, kopiowanie, uruchamianie), sektory rozruchu i potencjalnie niechciane aplikacje (PUA).

Aby skonfigurować skanowanie zależne od dostępu:

1. Użyj pola wyboru, żeby włączyć lub wyłączyć skanowanie zależne od dostępu. Jeżeli wyłączysz skanowanie zależne od dostępu, komputery będą podatne na złośliwe oprogramowanie.
2. Dla szybkiej konfiguracji, wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.
3. Możesz skonfigurować szczegóły ustawień skanowania poprzez **niestandardowy** poziom ochrony i naciśnięcie odnośnika **Ustawienia**. Pojawiające się okno **Ustawianie Skanowanie na żądanie** zawiera kilka opcji zorganizowanych w dwóch kartach **Ogólne** i **Zaawansowane**. Opcje są opisane poniżej od pierwszej do ostatniej zakładki:

- **Skanuj pliki lokalne.** Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Preferencje skanowania mogą zostać skonfigurowane osobno dla plików lokalnych (przechowywanych na lokalnym komputerze) lub plików sieciowych (przechowywanych w zasobach sieciowych). Jeżeli ochrona antymalware jest zainstalowana na wszystkich komputerach w sieci, możesz wyłączyć skanowanie plików sieciowych aby dopuścić dostęp do szybszej sieci.

Możesz ustawić Endpoint Security aby skanował wszystkie pliki do których ma dostęp (niezależnie od rozszerzenia pliku), tylko pliki aplikacji lub określone rozszerzenia plików, które uważasz, że mogą być niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich użytych plików, natomiast lepszą wydajność zapewnia skanowanie tylko aplikacji.



Notatka

Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „[Lista Typów Plików Aplikacji](#)” (p. 149).

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

Dla lepszej wydajności systemu, możesz również wykluczyć duże pliki ze skanowania. Zaznacz pole wyboru **Maksymalny rozmiar (MB)** i określ limit wielkości plików, które będą skanowane. Używaj tej opcji mądrze, ponieważ złośliwe oprogramowanie może mieć wpływ na większe pliki.

- **Archiwa** Wybierz **Skanuj wewnątrz archiwów** jeśli chcesz umożliwić dostęp na żądanie do plików archiwalnych. Skanowanie wewnątrz archiwów to powolny i zasobożerny proces, który z tego powodu nie jest zalecany dla użycia w ochronie w czasie rzeczywistym. Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony na żądanie.

Jeżeli zdecydowałeś aby używać tej opcji, możesz skonfigurować poniższe opcje optymalizacji:

- **Maksymalny rozmiar archiwum (MB)** . Możesz ustawić maksymalną akceptowalną wielkość archiwum do skanowania zależnego od dostępu. Zaznacz odpowiadające pole wyboru i wpisz maksymalny rozmiar archiwum (w MB).
- **Maksymalna głębokość archiwum (poziomy)**. Zaznacz odpowiednie pole i wybierz maksymalną głębokość archiwum z menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.
- **Inne**. Zaznacz odpowiednie pola, aby włączyć żądane opcje skanowania.
 - **Skanowanie sektorów startowych**. Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu bootowania. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
 - **Skanuj tylko nowe i zmienione pliki**. Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
 - **Skanuj w poszukiwaniu keyloggerów**. Keyloggery zapisują to, co wpiszesz na klawiaturze i wysyłają raporty przez internet do hakera. Haker może poznać ważne informacje z ukradzionych danych, takie jak numer i hasło do konta bankowego i użyć ich na własną korzyść.
 - **Skanuj w poszukiwaniu niepożądanych aplikacji (PUA)**. Potencjalnie nie chciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-supported). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.
- **Skanowanie**: W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:

- **Domyślne działanie dla zainfekowanych plików.** Pliki, w których wykryto infekcję, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania Bitdefender. Endpoint Security można normalnie usunąć kod malware z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

W przypadku wykrycia zainfekowanego pliku Endpoint Security podejmie automatyczną próbę jego dezynfekcji. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.



WAŻNE

W przypadku określonych typów złośliwego oprogramowania dezynfekcja jest niemożliwa, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Domyślne działanie dla podejrzanych plików.** Pliki są wykrywane jako podejrzane przez analizę heurystyczną. Ponieważ B-HAVE to technologia oparta na analizie heurystycznej, Endpoint Security nie może być pewny, że plik jest rzeczywiście zainfekowany przez szkodliwe oprogramowanie. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

Jeżeli podejrzany plik zostanie wykryty, użytkownicy dostaną odmowę dostępu do pliku, żeby zapobiec potencjalnej infekcji.

Choć nie jest to polecane, możesz zmienić domyślne działania. Możesz zdefiniować dwie akcje dla każdego typu pliku. Dostępne są następujące działania:

Blokuj dostęp

Odmowa dostępu do wykrytych plików.

Wylecz

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

Usuń

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

Przenieś do kwarantanny

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

Ustawienia Aktywnej Kontroli Wirusów

Aktywna Kontrola Wirusów Bitdefender to innowacyjna, proaktywna technologia detekcji, która do wykrywania w czasie rzeczywistym nowych, potencjalnych zagrożeń korzysta z zaawansowanych metod heurystycznych.

Moduł Aktywnej Kontroli Wirusów nieustannie monitoruje aplikacje działające na komputerze w poszukiwaniu aktywności charakterystycznej dla złośliwego oprogramowania. Każde z tych działań jest oceniane, a dla każdego procesu obliczana jest ocena ogólna. Gdy wynik ogólny dla danego procesu osiąga podany próg, proces ten zostaje uznany za szkodliwy. Aktywna Kontrola Wirusów automatycznie spróbuje wyleczyć wykryty plik. Jeśli rutynowe leczenie się nie powiedzie, Aktywna kontrola Wirusów usunie plik.



Notatka

Przed zastosowaniem działań dezynfekcji, kopia pliku jest wysyłana do kwarantanny, dzięki czemu masz możliwość przywrócenia jej później, w przypadku błędnego zaklasyfikowania. To działanie można skonfigurować używając opcji **Kopiuj pliki kwarantanny przed zastosowaniem działań dezynfekcji** dostępna jest w zakładce **Kwarantanna** ustawień polityki. Ta opcja jest włączona domyślnie w szablonie polityki.



Notatka

Aby uzyskać więcej informacji, odwiedź naszą witrynę internetową i zapoznaj się z [opracowaniem na temat Aktywnej kontroli wirusowej](#).

Konfigurowanie Aktywnej Kontroli Wirusowej:

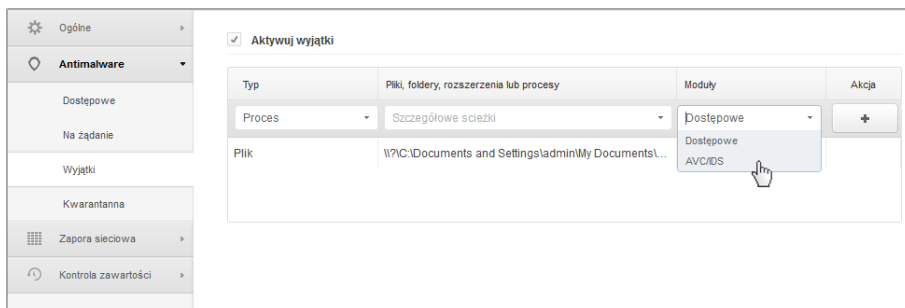
1. Użyj pola wyboru aby włączyć lub wyłączyć Aktywną Kontrolę Wirusów. Jeżeli wyłączysz Aktywną Kontrolę Wirusów, komputery będą podatne na nieznanne złośliwe oprogramowanie.
2. Aktywna Kontrola wirusów domyślnie będzie próbowała wyleczyć zainfekowane aplikacje. Aby ustawić inne domyślne działanie, użyj dostępnego menu.
3. Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.



Notatka

Jeśli podniesiesz poziomy ochrony, Aktywna Kontrola Wirusów będzie wymagać mniejszej liczby oznak złośliwego zachowania, by zgłosić dany proces. To sprawi, że raportowana będzie większa liczba aplikacji, a jednocześnie wzrośnie prawdopodobieństwo wystąpienia fałszywych alarmów (nieszkodliwych aplikacji rozpoznanych jako złośliwe).

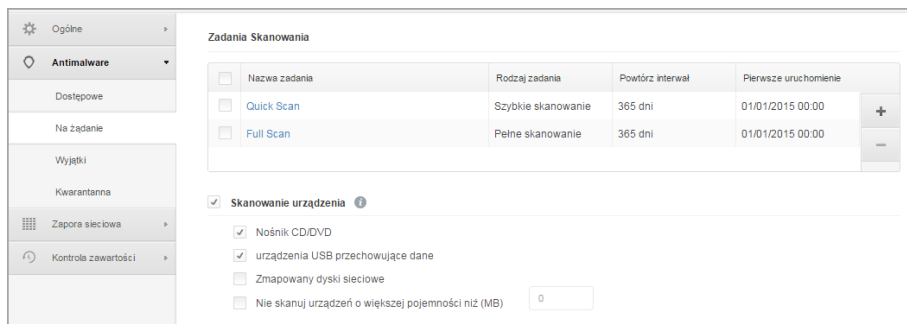
4. Możesz stworzyć reguły wyjątków dla powszechnie znanych aplikacji w celu uniknięcia fałszywych alarmów (niepoprawne wykrycie legalnych aplikacji). Przejdź do zakładki [Wyjątki](#) i skonfiguruj **reguły wyjątków procesów AVC/IDS** dla zaufanych aplikacji.



Polityka komputera - wyjątki procesów AVC/IDS

Na żądanie

W tej sekcji możesz skonfigurować zadania skanowanie antymalware, które będą uruchamiana się regularnie na docelowych komputerach, według ustalonego harmonogramu.



Polityki Komputera - Zadania skanowania na żądanie

Proces skanowania odbywa się w tle. Użytkownik jest informowany o procesie skanowania za pośrednictwem ikony znajdującej się w zasobniku procesowym.

Choć nie jest obowiązkowe, zaleca się zaplanować kompleksowe skanowanie systemu aby uruchamiano się co tydzień na wszystkich komputerach. Regularne skanowanie komputerów jest pro aktywnym zabezpieczeniem, które może pomóc wykrywać i blokować złośliwe oprogramowanie, które może uchronić się przed ochroną w czasie rzeczywistym.

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

Zarządzanie Zadaniem skanowania

Tabela Zadań skanowania informuje o istniejących zadaniach skanowania, dostarcza ważnych informacji na temat każdego z nich:

- Nazwa i rodzaj zadania.
- Harmonogram bazujący na zadaniach, które działają regularnie (rekurencyjnie).
- Czas kiedy zadanie zostanie po raz pierwszy uruchomione.

Są dwa domyślne zadania skanowania systemu, które możesz skonfigurować aby uruchomić, jeżeli potrzebujesz:

- **Szybkie skanowanie** Do wykrywania w systemie złośliwego oprogramowania Szybkie Skanowanie wykorzystuje skanowanie w chmurze. Wykonanie Szybkiego Skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.
- **Pełne Skanowanie** sprawdza cały komputer w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu, takiego jak wirusy, oprogramowanie typu spyware/adware, rootkity i inne.

Opcje skanowania domyślnych zadań skanowania są wstępnie skonfigurowane i nie można ich zmienić.

Oprócz domyślnych zadań skanowania (których nie możesz usunąć ani zduplikować) możesz utworzyć tak wiele niestandardowych zadań skanowania ile chcesz. Zadanie niestandardowe skanowanie dopuszcza wybranie konkretnej lokacji, które mają zostać przeskanowane i skonfigurować opcje skanowania.

aby utworzyć i skonfigurować nowe niestandardowe zadanie skanowania, naciśnij przycisk **+ Dodaj** po prawej stronie tabeli. Aby zmienić ustawienia istniejących zadań skanowania, naciśnij nazwę tego zadania. Zobacz poniższy temat aby dowiedzieć się jak skonfigurować zadanie.

Aby usunąć zadanie z listy, wybierz zadanie i naciśnij przycisk **- Usuń** po prawej stronie tabeli.

Konfiguracja Zadania Skanowania

Ustawienia zadania skanowania można organizować w trzech zakładkach:

- **Ogólne:** ustaw nazwę zadania i harmonogram realizacji.
- **Opcje:** wybierz profil skanowania dla szybkiej konfiguracji ustawień skanowania i zdefiniuj ustawienia skanowania dla niestandardowego skanowania.
- **Cel** wybierz pliki i foldery do skanowania.

Opcje są opisane poniżej od pierwszej do ostatniej zakładki:

Polityki Komputera - Skonfiguruj Ogólne Ustawienia zadanie skanowania na żądanie

- **Szczegóły.** Wybierz sugestywną nazwę dla zadania, aby w łatwy sposób móc zidentyfikować co zawiera. Kiedy wybierasz nazwę, weź pod uwagę cel zadania skanowania i ewentualne ustawienia skanowania.
- **Harmonogram.** Użyj opcji planowania aby skonfigurować harmonogram skanowania. Możesz ustawić skanowanie aby uruchamiano się co kilka godzin, dni lub tygodni, rozpoczynając się określonego dnia o ustalonej porze.

Proszę wziąć pod uwagę, że komputery muszą być włączone, w trakcie wykonywaniu zaplanowanych zadań. Zaplanowane skanowanie nie zostanie uruchomione jeżeli komputer jest wyłączony, za hibernowany, uśpiony lub żaden użytkownik nie jest zalogowany. W takich sytuacjach, skanowanie zostanie odłożone do następnego razu.

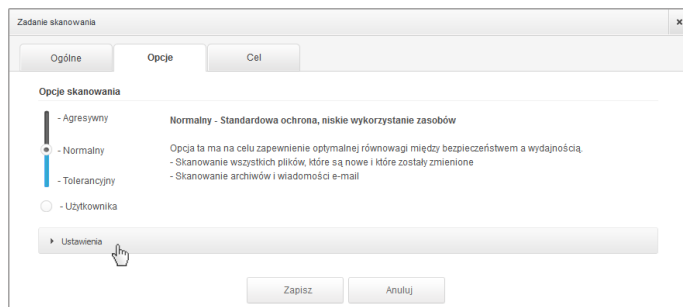


Notatka

Zaplanowane skanowanie uruchomi się na docelowych punktach końcowych według czasu lokalnego. Na przykład, jeżeli zaplanowane skanowanie jest ustawione o 18:00 i punkt końcowy posiada inną strefę czasową niż Control Center, skanowanie odbędzie się o 18:00 według czasu punktu końcowego.

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

Bazując na wybranym profilu, opcje skanowania w sekcji **Ustawienia** zostaną automatycznie skonfigurowane. Jednak, jeżeli chcesz, możesz skonfigurować je szczegółowo. Aby to zrobić, zaznacz pole wyboru **Niestandardowe** i przejdź do sekcji **ustawienia**.



Zadanie skanowania komputerów

- **Typy plików.** Użyj tych opcji aby określić rodzaj plików jakie chcesz skanować. Możesz ustawić Endpoint Security aby skanował pliki (niezależnie od rozszerzenia pliku), tylko pliki aplikacji lub określone rozszerzenia plików, które uważasz, że mogą być niebezpieczne. Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.



Notatka

Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików. Aby uzyskać więcej informacji, odwołaj się do „[Lista Typów Plików Aplikacji](#)” (p. 149).

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

- **Archiwa.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym. Zaleca się użycie tej opcji, w celu wykrycia i usunięcia wszelkich potencjalnych zagrożeń, nawet jeśli nie jest to zagrożenie bezpośrednie.



Notatka

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

- **Skanowanie wewnątrz archiwów.** Wybierz tę opcję tylko jeżeli chcesz sprawdzać pliki archiwów w poszukiwaniu malware. Jeżeli zdecydowałeś aby używać tej opcji, możesz skonfigurować poniższe opcje optymalizacji:
 - **Ogranicz rozmiar archiwum do (MB).** Możesz ustawić maksymalną akceptowalną wielkość archiwum do skanowania. Zaznacz odpowiadające pole wyboru i wpisz maksymalny rozmiar archiwum (w MB).

- **Maksymalna głębokość archiwum (poziomy).** Zaznacz odpowiednie pole i wybierz maksymalną głębokość archiwum z menu. Aby uzyskać najlepszą wydajność należy wybrać najniższą wartość, dla maksymalnej ochrony należy wybrać najwyższą wartość.
- **Skanowanie archiwum e-mail.** Zaznacz tę opcję jeżeli chcesz włączyć skanowanie plików wiadomości e-mail i bazy e-mail, włączając formaty takie jak .eml, .msg, .pst, .dbx, .mbx, .tbb i inne.



Notatka

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

- **Inne.** Zaznacz odpowiednie pola, aby włączyć żądane opcje skanowania.
 - **Skanowanie sektorów startowych.** Aby skanować boot sektor systemu. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu bootowania. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
 - **Skanowanie rejestru.** Włącz tę opcję, aby skanować klucze rejestru. Rejestr Windows jest bazą danych przechowującą ustawienia konfiguracji i opcje dla komponentów systemu operacyjnego Windows oraz dla zainstalowanych aplikacji.
 - **Skanowanie w poszukiwaniu rootkitów.** Zaznacz tę opcję, aby skanować w poszukiwaniu [rootkitów](#) ukrytych obiektów, które korzystają z tego rodzaju oprogramowania.
 - **Skanuj w poszukiwaniu keyloggerów.** Zaznacz opcje skanowania dla oprogramowania [keylogger](#).
 - **Skanowanie pamięci.** Wybierz tę opcję, aby przeskanować programy działające w pamięci systemu.
 - **Skanowanie ciasteczek.** Wybierz tę opcję, aby przeskanować ciasteczka zapisane w przeglądarce.
 - **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
 - **Skanuj w poszukiwaniu niepożądanych aplikacji (PUA).** Potencjalnie niechciana aplikacja (PUA) to program którego możesz nie chcieć na swoim komputerze, czasami jest dostarczany z darmowym oprogramowaniem. Takie programy mogą być instalowane bez zgody użytkownika (zwane również adware) lub zostaną załączone domyślnie podczas ekspresowej instalacji (ad-supported). Możliwe działanie takich programów to wyświetlanie pop-upów, instalowanie niechcianych toolbarów w domyślnej przeglądarce lub działanie kilku procesów w tle spowalniających działanie komputera.

- **Działania.** W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:

- **Domyślne działanie dla zainfekowanych plików.** Pliki, w których wykryto infekcję, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania Bitdefender. Endpoint Security można normalnie usunąć kod malware z zainfekowanego pliku i zrekonstruować oryginalny plik. Ta operacja określana jest mianem dezynfekcji.

W przypadku wykrycia zainfekowanego pliku Endpoint Security podejmie automatyczną próbę jego dezynfekcji. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.



WAŻNE

W przypadku określonych typów złośliwego oprogramowania dezynfekcja jest niemożliwa, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Domyślne działanie dla podejrzanych plików.** Pliki są wykrywane jako podejrzane przez analizę heurystyczną. Ponieważ B-HAVE to technologia oparta na analizie heurystycznej, Endpoint Security nie może być pewny, że plik jest rzeczywiście zainfekowany przez szkodliwe oprogramowanie. Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

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

- **Domyślne działanie dla rootkitów.** Rootkity stanowią specjalistyczne oprogramowanie wykorzystywane do ukrywania plików systemowych. Rootkity choć są nieszkodliwe, często są używane do ukrywania złośliwego oprogramowania lub intruza w systemie.

Wykrywanie rootkitów i ukrywanie plików jest domyślnie ignorowane.

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

Nie podejmuj żadnych działań

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

Wylecz

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

Usuń

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

Przenieś do kwarantanny

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

- **Cel Skanowania.** Dodaj listę wszystkich lokacji które chciałbyś przeskanować na docelowych komputerach.

Aby dodać nowy plik lub folder do skanowania:

1. Wybierz wcześniej zdefiniowaną lokalizację z rozwijanego menu lub wprowadź **Określoną ścieżkę**, którą chciałbyś przeskanować.
2. W polu edycji określ ścieżkę do obiektów, które mają zostać przeskanowane.

- Jeżeli wybrałeś wcześniej zdefiniowaną lokalizację, wypełnij ścieżkę jeśli potrzebujesz. Na przykład, aby przeskanować folder `Program Files` wystarczy wybrać odpowiednią ścieżkę z rozwijanego menu. Aby przeskanować konkretny folder z `Program Files`, musisz uzupełnić ścieżkę dodając backslash (\) i nazwę folderu.
- Jeżeli wybrałeś **Określona ścieżka**, podaj pełną ścieżkę do obiektu, który chcesz przeskanować. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.

3. Naciśnij przycisk **+ Dodaj**.

Aby edytować istniejącą lokalizację, kliknij ją. Aby usunąć lokalizację z listy, przesuń kursor nad nią, a następnie kliknij odpowiedni przycisk **- Usuń**.

- **Wyjątki.** Możesz korzystać z wyjątków z sekcji **Antymalware > Wyjątki** obecnej polityki, lub zdefiniować niestandardowe wyjątki dla bieżącego zadania skanowania. Aby uzyskać więcej informacji dotyczących wykluczeń, odwołaj się do „Wyjątki” (p. 96).

Skanowanie urządzenia

Możesz skonfigurować Endpoint Security aby automatycznie wykrywał i skanował zewnętrzne urządzenia pamięci masowej, kiedy są przyłączone do komputera. Wykryte urządzenia są przyporządkowywane do jednej z tych kategorii:

- CD/DVD

- Urządzenia pamięci masowej USB, takie jak flash i zewnętrzne dyski twarde.
- Zmapowany dyski sieciowe
- Urządzenia z większą ilością przechowywanych danych niż określona.

Skanowanie urządzenie automatycznie podejmując próbę wyleczenia plików wykrytych jako zainfekowane lub przenosi je do kwarantanny jeżeli wyleczenie nie jest możliwe. Weź pod uwagę, że żadne działania nie mogą być podejmowane na zainfekowanych plikach wykrytych na płytach CD / DVD lub na zmapowanych dyskach sieciowych, które umożliwiają dostęp tylko do odczytu.



Notatka

Podczas skanowania urządzenia, użytkownik może mieć dostęp do danych z urządzenia.

Jeżeli powiadomienia pop-up są włączone w sekcji **Ogólne > Wyświetl** użytkownik jest monitowany o rozpoczęcie skanowania, gdy zostanie wykryte urządzenie, zamiast automatycznego rozpoczęcia skanowania.

Gdy rozpocznie się skanowanie urządzenia:

- Powiadomienia pop-up informują użytkownika o skanowaniu urządzenia, pod warunkiem, że powiadomienia pop-ups są włączone w sekcji **Ogólne > Wyświetlanie**.
- Ikona skanowania pojawia się w [zasobniku systemu](#). Użytkownik może podwójnie nacisnąć tę ikonę aby otworzyć okno skanowania i sprawdzić jego postęp.

Po zakończeniu skanowania, użytkownik powinien sprawdzić wykryte zagrożenia, jeżeli zostaną znalezione.

Aby włączyć automatyczne wykrywanie i skanowanie urządzeń, zaznacz **Skanowanie Urządzenia**. Aby skonfigurować skanowanie urządzenia indywidualnie dla każdego rodzaju urządzenia, można użyć następujących opcji:

- **Nośnik CD/DVD**
- **urządzenia USB przechowujące dane**
- **Zmapowany dyski sieciowe**
- **Nie skanuj urządzeń o większej pojemności niż (MB)**. Użyj tej opcji aby automatycznie pominąć skanowanie wykrytych urządzeń, jeżeli ilość przechowywanych danych przekroczy określoną wielkość. W odpowiednim polu podaj limit (w megabajtach). Zero oznacza brak limitu.



Notatka

Opcja ta dotyczy tylko CD/DVD i urządzeń magazynujących USB.

Wyjątki

W tej sekcji można skonfigurować reguły wyjątków skanowania. Wyjątki mogą być stosowane podczas skanowania na żądanie, podczas dostępu lub obu. Opierając się na wykluczonych obiektach, mamy cztery typy wykluczeń:

Polityki Komputera - Wyjątki Antymalware

- **Wykluczone pliki:** określa pliki, które są wykluczone ze skanowania.
- **Folder wykluczeń:** wszystkie pliki wewnątrz określonego folderu i wszystkich podfolderach są wykluczone ze skanowania.
- **Wykluczone Rozszerzenia:** wszystkie pliki posiadające podane rozszerzenie są wykluczone ze skanowania.
- **Wykluczone procesy:** każdy obiekt dostępny przez wykluczony proces jest również wykluczony ze skanowania. Możesz również skonfigurować wyjątki dla [Aktywnej Kontroli Wirusów](#) i technologii [System wykrywania intruzów](#).



WAŻNE

Wyjątki skanowania są stosowane w szczególnych okolicznościach lub razem z Microsoft lub jako zalecenie Bitdefender. Aktualna lista wyjątków, zalecana przez Microsoft, znajduje się w tym [artykule](#). Jeżeli na komputerze znajduje się plik testowy EICAR służący do okresowego sprawdzania ochrony antymalware, należy pominąć go podczas skanowania na żądanie.

Użyj pola wyboru **Wyjątek aktywacji** aby włączyć lub wyłączyć wyjątki.

Aby skonfigurować zasady wyjątków:

1. Wybierz rodzaje wyjątków z menu.
2. Zależnie od rodzaju wyjątku, określ obiekt jaki ma być wykluczony według poniższych zaleceń:
 - **wyjątki rozszerzeń.** Określ jedno lub więcej rozszerzeń plików, które mają zostać pominięte przy skanowaniu, oddzielając ich nazwy za pomocą średnika ";". Możesz

wprowadzić rozszerzenia poprzedzając je kropką, ale nie musisz. Na przykład, wpisz `txt` aby wykluczyć pliki tekstowe.



Notatka

Zanim wykluczysz rozszerzenie, udokumentuj swoje działanie aby zobaczyć, który rozszerzenia są najczęstszym celem dla malware, a które nie.

- **Pliki, foldery i procesy wyjątków.** Musisz określić ścieżkę do wykluczonych obiektów na docelowych komputerów.
 - a. Wybierz z menu wstępnie zdefiniowaną lokalizację lub opcje **Określ Ścieżkę**.
 - b. Jeżeli wybrałeś wcześniej zdefiniowaną lokalizację, wypełnij ścieżkę jeśli potrzebujesz. Na przykład, aby wykluczyć folder `Program Files` wystarczy wybrać odpowiednią ścieżkę z menu. Aby wykluczyć konkretny folder z `Program Files`, musisz uzupełnić ścieżkę dodając backslash (\) i nazwę folderu. Aby wykluczyć proces, musisz również dodać nazwę pliku wykonywalnego aplikacji.
 - c. Jeżeli wybrałeś **Określona ścieżka**, podaj pełną ścieżkę do obiektu, który chcesz wykluczyć. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.
- 3. Wybierz rodzaje skanowania dla których będą zastosowane dla reguły. Niektóre wyjątki mogą mieć znaczenie tylko dla skanowania dostępowego, niektóre tylko dla skanowania na żądanie, a niektóre mogą być zalecane dla obu. Wyjątki procesów można skonfigurować dla skanowania na żądanie i dla [Aktywnej Kontroli Wirusów](#) i technologii [System wykrywania intruzów](#).



Notatka

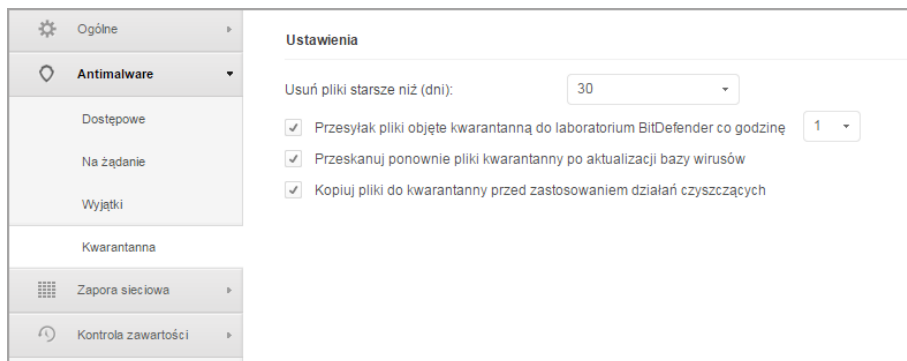
Należy pamiętać, że wyjątki skanowania na żądania nie zostaną zastosowane w skanowaniu kontekstowym. Skanowanie kontekstowe uruchamia się poprzez kliknięcie pliku lub folderu prawym przyciskiem myszy i wybranie **Skanuj z Endpoint Security przez Bitdefender**.

4. Kliknij przycisk **+ Dodaj**. Do listy zostanie dodana nowa reguła.

Aby usunąć zasadę z listy, kliknij odpowiadający jej przycisk **- Usuń**.

Kwarantanna

W tej sekcji można skonfigurować ustawienia kwarantanny.



Polityki Komputera - Kwarantanna

Istnieje możliwość, aby program Endpoint Security automatycznie wykonywał poniższe akcje:

- **Usuń pliki starsze niż (dni).** Domyślnie wszystkie pliki objęte kwarantanną dłużej niż 30 dni są automatycznie usuwane. Jeżeli chcesz zmienić przedział, wybierz inne opcje z menu.
- **Przesyłaj pliki kwarantanny do Laboratorium Bitdefender co godzinę.** Zostaw tę opcję wybraną aby automatycznie wysyłać pliki kwarantanny do Laboratorium Bitdefender. Możesz edytować przedziały czasu pomiędzy plikami kwarantanny, które zostały wysłane (domyślnie, co godzinę). Przykładowe pliki będą przeanalizowane przez badaczy szkodliwego oprogramowania firmy Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.
domyślnie, pliki kwarantanny są automatycznie wysyłane do laboratorium Bitdefender co godzinę. Jeżeli chcesz zmienić przedział, wybierz inne opcje z menu.
- **Ponowne skanowanie kwarantanny po aktualizacji sygnatur malware.** Zostaw tą opcję wybraną aby automatycznie skanować pliki kwarantanny po każdej aktualizacji sygnatur malware. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.
- **Kopiuj pliki do kwarantanny przed zastosowaniem działań dezynfekcji.** Wybierz tę opcję aby zapobiec utracie danych w przypadku fałszywych alarmów i skopiować wszystkie zainfekowane pliki do kwarantanny przed zastosowaniem działań dezynfekcji. Można potem przywrócić legalne pliki ze strony **Kwarantanna**.

6.2.3. Zapora sieciowa

Zapora sieciowa chroni twój komputer przed niechcianymi połączeniami z zewnątrz i od środka.

Funkcjonalność zapory opiera się na profilach sieciowych. Profile bazują na zaufanych poziomach, które są zdefiniowane dla każdej sieci.

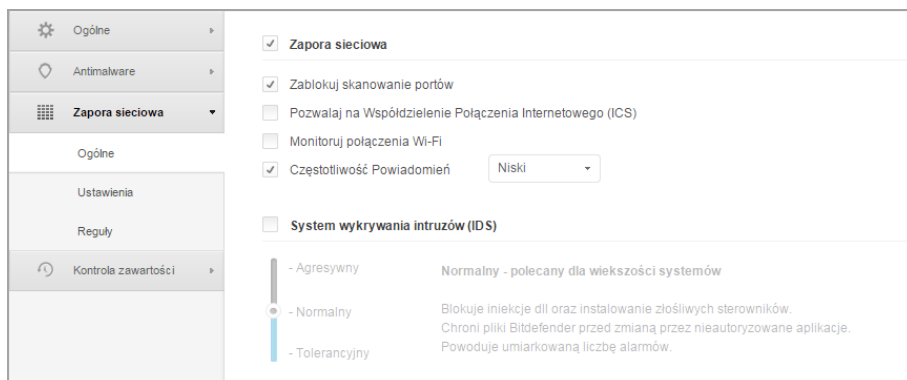
Każdego razu jak połączenie jest tworzone, Zapora sieciowa wykrywa je i porównuje z informacjami adaptera połączenia z informacjami z istniejących profili, stosując poprawny profil. W celu uzyskania szczegółowych informacji jak stosować profile, zobacz [ustawienia sieciowe](#).

Ustawienia są zorganizowane w poniższych sekcjach:

- [Ogólne](#)
- [Ustawienia](#)
- [Reguły](#)

Ogólne

W tej sekcji możesz włączyć lub wyłączyć zaporę sieciową programu Bitdefender, a także skonfigurować ustawienia ogólne.



Polityki Komputera - Ogólne ustawienia zapory sieciowej

- **Zapora sieciowa.** Użyj pola wyboru aby włączyć lub wyłączyć Zaporę Sieciową. Jeżeli wyłączysz zaporę sieciową, komputery będą podatne na ataki sieciowe i Internetowe.
- **Zablokuj skanowanie portów.** Operacja skanowania portów jest często wykorzystywana przez hakerów w celu znalezienia otwartych portów na komputerze. Napastnicy mogą włamać się do komputera, jeśli znajdują słabo zabezpieczony lub podatny port.
- **Pozwalaj na Współdzielenie Połączenia Internetowego (ICS).** Wybierz tę opcję aby ustawić zaporę sieciową tak aby dopuszczała udostępnianie połączenia internetowego.



Notatka

Ta opcja nie włącza automatycznie ICS w systemie użytkownika.

- **Monitoruj połączenia Wi-Fi.** Program Endpoint Security może informować użytkowników podłączonych do sieci Wi-Fi o podłączeniu do sieci nowego komputera. Aby wyświetlić informacje na ekranie użytkownika, wybierz tę opcję.
- **Częstotliwość Powiadomień.** Endpoint Security zapisuje zdarzenia dotyczące użycia Zapory sieciowej do dziennika (włączanie / wyłączenie modułu, blokowanie ruchu sieciowego, modyfikacja ustawień) oraz zdarzenia aktywności wykrytej przez ten moduł (skanowanie portów, blokowanie prób połączenia i ruchu sieciowego zgodnie z regułami). Wybierz opcje z **Częstotliwość Powiadomień** aby określić jak wiele informacji powinien zawierać dziennik.
- **System wykrywania włamań.** Wykrywanie/Zapobieganie włamań sprawdza system pod kątem podejrzanych działań (na przykład: nieautoryzowany dostęp do plików programu Bitdefender, wstrzykiwanie bibliotek DLL, próby logowania naciskanych klawiszy itp.).

Konfigurowanie Systemu Wykrywania Włamań:

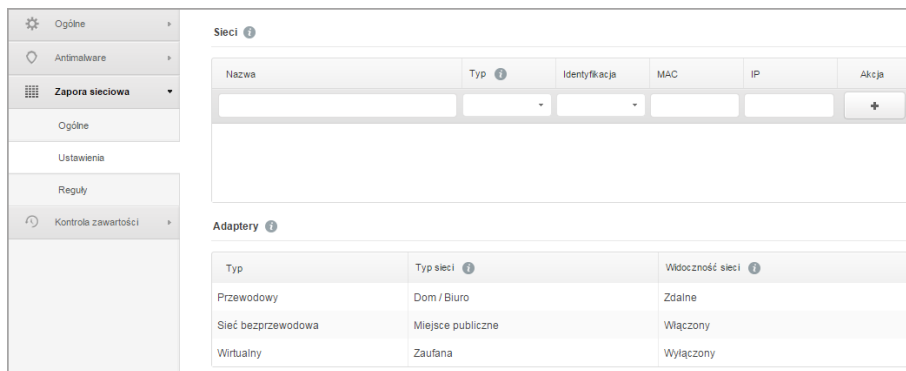
1. Użyj pola wyboru aby włączyć lub wyłączyć system wykrywania włamań.
2. Wybierz poziom bezpieczeństwa, który najbardziej Ci odpowiada (Agresywny, Normalny lub Tolerancyjny). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór.

Aby zapobiec wykryciu legalnych aplikacji przez System wykryć włamań, dodaj **regułę wyjątku procesu AVC/IDS** dla aplikacji w sekcji **Antymalware > Wyjątki**.

Ustawienia

Zapora automatycznie stosuje profil na podstawie rodzaju sieci. Możesz określić profile, które zostaną zastosowane zależnie od rodzaju adaptera i dodatkowo określając profile indywidualne dla sieci twojej firmy. Ustawienia są zorganizowane w poniższych tabelach:

- [Sieci](#)
- [Adaptery](#)



Nazwa	Typ	Identyfikacja	MAC	IP	Akcja
					+

Typ	Typ sieci	Wdrożenie sieci
Przewodowy	Dom / Biuro	Zdalne
Sieć bezprzewodowa	Miejsce publiczne	Włączony
Wirtualny	Zaufana	Wyłączony

Polityki Komputera - Ustawienia Zapory Sieciowej

Ustawienia Sieci

Aby zapora sieciowa działała prawidłowo, administrator musi zdefiniować sieci, którymi będzie zarządzał w tabeli **Sieci**. Pola w tabeli **Sieci** są opisane w poniższy sposób:

- **Nazwa.** Nazwa po której administrator może rozpoznać sieć na liście.
- **Typ.** Wybierz z menu rodzaj profilu przypisanego do sieci.
Endpoint Security automatycznie zatwierdza jedno z czterech profili zapory sieciowej dla każdego wykrytego połączenia sieciowego aby zdefiniować podstawowe opcje filtrowania. Profile zapory sieciowej:
 - **Zaufana** sieć. Wyłącza zapórę sieciową dla odpowiedniego urzędu.
 - Sieć **domowa/biurowa**. Zezwól na cały ruch z komputerów w sieci lokalnej.
 - Sieć **publiczna**. Cały ruch jest filtrowany.
 - **Nie Zaufana** sieć. Kompletnie blokuje ruch sieciowy i internetowy poprzez odpowiednie urządzenie.
- **Identyfikacja.** wybierz z menu metodę w jaki sposób sieć będzie identyfikować Endpoint Security. Sieci mogą być zidentyfikowane przez trzy metody: **DNS**, **Brama Sieciowa** i **Sieć**.
- **MAC.** Użyj tego pola żeby określić adres MAC konkretnego serwera DNS.



Notatka

To pole jest obowiązkowe jeżeli została wybrana metoda identyfikacji DNS.

- **IP.** Użyj tego pola żeby zdefiniować konkretny adres IP w sieci. Możesz również użyć maski do zdefiniowania całej podsięci.

Jak zdefiniujesz sieć, naciśnij przycisk **Dodaj** po prawej stronie tabeli aby dodać ją do listy.

Ustawienia Adapterów

Jeżeli sieć, która nie została zdefiniowana w tabeli **Sieci** została wykryta, Endpoint Security wykryje rodzaj adaptera sieciowego i zastosuje odpowiedni profil połączenia. Pola w tabeli **Adaptory** są opisane w poniższy sposób:

- **Typ.** Wyświetl rodzaje adapterów sieciowych. Endpoint Security może wykryć trzy wstępnie zdefiniowane rodzaje adapterów: **Przewodowy**, **Bezprzewodowy** i **Wirtualny** (Prywatna Wirtualna Sieć).
- **Typ sieci.** Opis profil sieci przypisany do konkretnych rodzajów adapterów. Rodzaje sieci są opisane w [sekcji ustawień sieci](#). Naciskając na pole rodzaju sieci możesz zmienić ustawienia. Jeżeli wybrałeś **Pozwól decydować Windows**, dla każdego połączenia sieciowego wykrytego po zastosowaniu polityki, Endpoint Security zastosuje profil zapory sieciowej bazujący na klasyfikacji sieci w Windows, ignorując ustawienia z tabeli **Adaptory**.
Jeśli wykrywanie oparte na Menadżerze Sieci Windows nie powiedzie się, zostanie podjęta próba wykrywania podstawowego. Generyczny profil jest używany gdy rodzaj sieci jest **Publiczny** i ustawienia ukrywania są **Włączone**. Jeżeli adres IP domeny komputera został znaleziony w jednej z sieci przypisanych do adaptera, wtedy poziom zaufania sieci zostanie określony jako **Dom/Praca** i i ukryte ustawienia zostaną **Zdalnie włączone**. Jeżeli komputer nie jest w domenie, warunek ten nie ma zastosowania.
- **Tryb Ukryty.** Ukrywanie komputera przed złośliwym oprogramowaniem i hakerami w sieci lokalnej lub Internecie. Skonfiguruj tryb Ukryty jeżeli potrzebujesz dla każdego rodzaju adaptera przez wybranie jednej z poniższych opcji:
 - **Włączony.** Komputer jest niewidoczny zarówno dla sieci lokalnej, jak i internetu.
 - **Wyłączony.** Każdy w sieci lokalnej i internecie może pingować i wykryć komputer.
 - **Zdalne.** Komputer nie może być wykryty z internetu. Każdy w sieci lokalnej może pingować i wykryć komputer.

Reguły

W tej sekcji możesz skonfigurować dostęp do sieci aplikacji i reguły ruchu danych egzekwowane przez zaporę. Należy pamiętać, że dostępne ustawienia mają zastosowanie tylko do **Dom/Praca** i **Publiczne Profile zapory**.

Ustawienia

Poziomy ochrony: Zestaw reguł, znane pliki i pozwolenia

Tworzenie agresywnych reguł
 Utwórz zasady dla aplikacji zablokowanych przez IDS
 Monitoruj procesy zmian
 Ignoruj podpisane procesy

Reguły

<input type="checkbox"/>	Nadrzędny	Nazwa	Typ reguły	Sieć	Protokół	Zezwolenie	
<input type="checkbox"/>	1	Przychodzący ICMP	Aplikacja	Dom / Biuro, ...	ICMP	Zezwól	+
<input type="checkbox"/>	2	Przychodzący ICMPv6	Aplikacja	Dom / Biuro, ...	IPv6-ICMP	Zezwól	-
<input type="checkbox"/>	3	Przychodzące połączenia zdalnego pulpitu	Połączenia	Dom / Biuro, ...	TCP	Zezwól	▲
<input type="checkbox"/>	4	Wysyłanie wiadomości e-mail	Połączenia	Dom / Biuro, ...	TCP	Zezwól	▼
<input type="checkbox"/>	5	Przeglądanie internetu HTTP	Aplikacja	Dom / Biuro, ...	TCP	Zezwól	
<input type="checkbox"/>	6	Drukowanie w innej sieci	Aplikacja	Dom / Biuro, ...	Dowolny	Zabroń	
<input type="checkbox"/>	7	Ruch związany z Windows Explorer przez FTP	Aplikacja	Dom / Biuro, ...	TCP	Zabroń	
<input type="checkbox"/>	8	Ruch związany z Windows Explorer przez H...	Aplikacja	Dom / Biuro, ...	TCP	Zabroń	

Polityki Komputerów - Ustawienia Zasad Zapory Sieciowej

Ustawienia

Możesz skonfigurować następujące ustawienia:

- **Poziomy ochrony.** Wybrany poziom ochrony określa logikę procesów decyzyjnych zapory sieciowej podczas żądania dostępu aplikacji do usług sieciowych i internetowych. Dostępne są następujące opcje:

Zestaw reguł i pozwoleń

Zastosuj istniejące reguły zapory sieciowej i automatycznie zezwól na wszystkie inne próby połączeń. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

Zestaw reguł i pytań

Zastosuj istniejące reguły zapory sieciowej i powiadom użytkownika o działaniu dla wszystkich innych prób połączeń. Zostanie wyświetlone okno alertu na ekranie użytkownika ze szczegółowymi informacjami o próbie nieznanego połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

Zestaw reguł i odmów

Zastosuj istniejące reguły zapory sieciowej i automatycznie zabroń wszystkich innych prób połączeń. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

Zestaw reguł, znane pliki i pozwolenia

Zastosuj istniejące reguły zapory sieciowej, automatycznie dopuść próby połączeń, stworzone przez znane aplikacje i automatycznie dopuść wszystkie inne nieznanne

próby połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

Zestaw reguł, znane pliki i zapytania

Zastosuj istniejące reguły zapory sieciowej, automatycznie dopuść próby połączeń, stworzone przez znane aplikacje i powiadom użytkownika o działaniu dla wszystkich innych prób połączenia. Zostanie wyświetlone okno alertu na ekranie użytkownika ze szczegółowymi informacjami o próbie nieznanego połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.

Zestaw reguł, znane pliki i odmowy

Zastosuj istniejące reguły zapory sieciowej, automatycznie dopuść próby połączeń, stworzone przez znane aplikacje i automatycznie odmów dostępu wszystkim innym nieznanym próbom połączenia. Dla każdej nowej próby połączenia, zostanie stworzona reguła i dodana do zestawu reguł.



Notatka

Znane pliki należą do dużej kolekcji bezpiecznych, zaufanych aplikacji, które są opracowane i utrzymywane w sposób ciągły przez Bitdefender.

- **Tworzenie agresywnych reguł.** Przy tej opcji zaznaczonej, zapora sieciowa stworzy reguły dla każdego procesu otwierającego aplikacje wymagającą dostępu do sieci lub Internetu.
- **Utwórz zasady dla aplikacji zablokowanych przez IDS.** Wybierając tę opcję, zapora sieciowa automatycznie utworzy zasadę **Odmowa** za każdym razem jak System wykrycia włamań blokuje aplikacje.
- **Monitoruj procesy zmian.** Wybierz tę opcję, jeśli chcesz, aby program sprawdzał, czy od czasu dodania reguły kontrolującej dostęp do Internetu żadna aplikacja łącząca się z Internetem nie została zmieniona. Jeżeli aplikacja zostanie zmieniona nowa reguła zostanie stworzona zgodnie z istniejącym poziomem ochrony.



Notatka

Zazwyczaj zmiany w aplikacjach powstają na skutek aktualizacji. Istnieje jednak możliwość, że zmiany zostaną dokonane przez aplikacje będące oprogramowaniem złośliwym, w celu zainfekowania komputera lokalnego i innych komputerów pracujących w sieci.

Podpisane aplikacje powinny być zaufane i mieć wyższy poziom zabezpieczeń. Możesz wybrać **Ignoruj podpisane procesy** aby automatycznie zezwalać na łączenie się z Internetem zmienionych podpisanych aplikacji.

Reguły

Tabela reguł zawiera reguły istniejącej zapory sieciowej, dostarczając ważnych informacji na temat każdej z nich:

- Odnosi się do nazwy reguły lub aplikacji.
- Protokół, którego dotyczy dana reguła.
- Działanie reguły (dopuszczanie lub blokowanie pakietów).
- Działania jakie możesz podjąć na regule.
- Priorytet reguły.



Notatka

Takie są reguły zapory wyraźnie wymuszone przez politykę. Dodatkowe przepisy mogą być skonfigurowane na komputerach w wyniku stosowania ustawień zapory.

Liczba domyślnych reguł zapory sieciowej pomaga łatwo zezwolić lub zabronić dostępu dla popularnych rodzajów ruchu. Wybierz wymaganą opcję z menu **Pozwolenie**.

Przychodzący ICMP / ICMPv6

Zezwól lub odmów ICMP/ ICMPv6 wiadomości. Wiadomości ICMP są często używane przez hakerów do ataków na sieci komputerowe. Domyślnie ten typ ruchu będzie zabroniony.

Przychodzące połączenia zdalnego pulpitu

Zezwól lub zabroń innym komputerom łączyć się z pulpitem zdalnym. Domyślnie ten typ ruchu będzie dozwolony.

Wysyłanie wiadomości e-mail

Zezwól na lub zablokuj wysyłanie wiadomości e-mail przez SMTP. Domyślnie ten typ ruchu będzie dozwolony.

Przeglądanie internetu HTTP

Zezwól na przeglądanie lub zabroń przeglądania stron przez HTTP. Domyślnie ten typ ruchu będzie dozwolony.

Drukowanie w innej sieci

Zezwól lub zabroń dostępy do drukarek w innym lokalnym obszarze sieci. Domyślnie ten typ ruchu będzie zabroniony.

Ruch HTTP / FTP związany z Eksploratorem Windows

Zezwól lub zablokuj ruch HTTP i FTP związany z Eksploratorem Windows. Domyślnie ten typ ruchu będzie zabroniony.

Oprócz domyślnych reguł, można utworzyć dodatkowe reguły zapory dla innych aplikacji zainstalowanych na komputerach. Ta konfiguracja jest zarezerwowana dla administratorów z dużą wiedzą na temat sieci.

aby utworzyć i skonfigurować nową regułę skanowania, naciśnij przycisk **+** **Dodaj** po prawej stronie tabeli. Zobacz następujący temat aby uzyskać więcej informacji.

Aby usunąć regułę z listy, naciśnij przycisk **-** **Usuń** po prawej stronie tabeli.



Notatka

Nie można ani usunąć, ani zmodyfikować domyślnej reguły zapory.

Konfigurowanie niestandardowych reguł

Możesz skonfigurować dwa rodzaje reguł zapory sieciowej:

- **Aplikacja bazuje na regułach.** Takie zasady stosują się do konkretnego oprogramowania znalezione na komputerach klienckich.
- **Połączenie bazuje na regułach.** Takie zasady stosują się do dowolnej aplikacji lub usługi przy użyciu określonego połączenia.

Aby stworzyć i skonfigurować nową regułę, naciśnij przycisk **+** **Dodaj** po prawej stronie tabeli i wybierz odpowiedni rodzaj reguły z menu. Aby edytować istniejącą regułę, naciśnij nazwę reguły.

Można skonfigurować następujące ustawienia:

- **Nazwa reguły.** Podaj nazwę dla reguły, która będzie na liście reguł w tabeli (na przykład, nazwa aplikacji, której dotyczy reguła).
- **Ścieżka aplikacji** (tylko dla aplikacji bazujących na regułach). Musisz określić ścieżkę do wykluczonych plików aplikacji na docelowych komputerach.
 - Wybierz z menu wcześniej zdefiniowaną lokalizację i uzupełnij potrzebną ścieżkę. Na przykład, dla aplikacji zainstalowanych w folderze `Program Files`, wybierz `%ProgramFiles%` i uzupełnij ścieżkę dodając backslashes (\) i nazwę foldera aplikacji.
 - Podaj pełną ścieżkę w polu edycji. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.
- **Linia komend** (tylko dla aplikacji bazujących dla reguły). Jeśli chcesz zastosować regułę tylko kiedy określona aplikacja jest uruchomiona przez komendę z interfejsu linii komend Windows, wpisz komendę w polu edycji. W przeciwnym razie pozostaw to pole puste.
- **Aplikacja MD5** (tylko dla aplikacji bazujących na regułach). Jeżeli chcesz regułę do sprawdzenia integracji danych pliku aplikacji bazującej na hash kodzie MD5, podaj go w polu edycji. W innym wypadku pole należy pozostawić puste.
- **Adres lokalny.** Określ lokalny adres IP oraz port, do którego odnosi się dana reguła. Jeśli masz więcej niż jeden adapter sieciowy, możesz odznaczyć pole wyboru „**Dowolny**” i podać konkretny adres IP. Podobnie, aby filtrować połączenia na określonym porcie lub zakresie portów, wyczyść pole wyboru **Dowolny** i wprowadź żądany port lub zakres portów w odpowiednim polu.
- **Adres zdalny.** Określ zdalny adres IP oraz port, do którego odnosi się dana reguła. Aby filtrować ruch w określonym komputerze, odznacz pole **Dowolne** i wpisz jego adres IP.

- **Zastosuj regułę tylko do bezpośrednio podłączonych komputerów.** Możesz filtrować dostęp do adresu Mac.
- **Protokół.** Wybierz protokół IP do którego stosowana jest reguła.
 - Jeśli chcesz aby reguła była stosowana dla wszystkich protokołów, zaznacz **Dowolne**.
 - Jeśli chcesz zastosować tą regułę do protokołu TCP, wybierz **TCP**.
 - Jeśli chcesz zastosować tą regułę do protokołu UDP, wybierz **UDP**.
 - Jeżeli chcesz regułę do zastosowania określonego protokołu, wybierz protokół z menu **Inne**.



Notatka

Numery protokołów IP są przypisane przez Internet Assigned Numbers Authority (IANA). Kompletną listę protokołów IP możesz znaleźć tutaj: <http://www.iana.org/assignments/protocol-numbers>.

- **Kierunek.** Wybierz kierunek ruchu do którego stosowana jest reguła.

Kierunek	Opis
Wysyłane	Reguła będzie dotyczyła tylko ruchu wychodzącego.
Odbierane	Reguła będzie dotyczyła tylko ruchu przychodzącego.
Oba	Reguła będzie dotyczyła obu kierunków.

- **Wersja IP.** Wybierz wersje IP (IPv4, IPv6 lub dowolną) dla którego ma być stosowana reguła.
- **Sieć.** Wybierz typ sieci, do której stosuje się ta reguła.
- **Zezwolenie.** Wybierz jedno z dostępnych uprawnień:

Zezwolenie	Opis
Zezwól	Podana aplikacja dostanie zezwolenie na dostęp do sieci / internetu pod pewnymi warunkami.
Zabroń	Podana aplikacja nie dostanie dostępu do sieci / internetu pod pewnymi warunkami.

Aby dodać regułę, kliknij **Zapisz**.

Dla reguł, które stworzyłeś, użyj strzałek po prawej stronie tabeli aby ustawić priorytet reguł. Reguła z wysokim priorytetem jest bliżej szczytu listy.

6.2.4. Kontrola zawartości

Używając modułu Kontroli Zawartości aby skonfigurować preferencje dotyczące filtrowania treści i ochrony danych dotyczących aktywności użytkowników, takich jakich przeglądanie sieci, e-mail i aplikacje. Możesz zastrzec lub zezwolić na dostęp do sieci aplikacji, skonfigurować skanowanie ruchu, antyphishing i reguły ochrony danych. Zwróć uwagę, że po skonfigurowaniu ustawień kontroli Treści, pokaże się wszystkim użytkownikom dziennik na docelowych komputerach.

Ustawienia są zorganizowane w poniższych sekcjach:

- [Ruch sieciowy](#)
- [Sieć WWW](#)
- [Ochrona danych](#)
- [Aplikacje](#)

Ruch sieciowy

Skonfiguruj preferencje bezpieczeństwa ruchu używając ustawień w poniższej sekcji:


- [Opcje](#)
- [Skanowanie ruchu](#)
- [wyjątki w skanowaniu ruchu](#)

Typ	Wykluczone wpisy	Akcja
	jednostka	+

Polityki komputera - Kontrola Treści - Ruch

Opcje


- **Skanuj SSL.** Wybierz tę opcję jeżeli chcesz aby ruch sieciowy Secure Sockets Layer (SSL) był kontrolowany przez moduł ochrony Endpoint Security.
- **Pokaż pasek narzędzi przeglądarki.** Toolbar Bitdefender informuje użytkowników o ocenie stron internetowych, które są przeglądane. Pasek narzędzi produktu Bitdefender

nie jest Twoim typowym paskiem narzędzi przeglądarki. Jedynym elementem dodanym do przeglądarki jest mały element przeciągający  na górze każdej wyświetlanej strony. Naciskając dragger otwiera się toolabar.

W zależności od tego, jak Bitdefender zaklasyfikuje stronę, jedna z wymienionych ocen pojawi się po lewej stronie paska narzędzi:

- Wiadomość "Ta strona nie jest bezpieczna" pojawia się na czerwonym tle.
 - Wiadomość "Należy zachować ostrożność" pojawia się na pomarańczowym tle.
 - Wiadomość "Strona jest bezpieczna" pojawia się na zielonym tle.
- **Doradca wyszukiwania.** Doradca wyszukiwania, ocenia rezultaty wyszukiwania w Google, Bing i Yahoo!, a także linki z serwisów Facebook i Twitter poprzez umieszczenie ikony przy każdym rezultacie wyszukiwania: Używane ikony i ich znaczenie:

 Nie powinieneś wchodzić na tę stronę.

 Ta strona może zawierać niebezpieczną treść. Należy zachować ostrożność, jeśli zdecydujesz się ją odwiedzić.

 Ta strona jest bezpieczna.

Skanowanie ruchu

Przychodzące maile i ruch sieciowy są skanowane w czasie rzeczywistym aby powstrzymać złośliwe oprogramowanie przez zainstalowaniem na komputerze. Wychodzące wiadomości e-mail są skanowane aby powstrzymać złośliwe oprogramowanie przez zainfekowaniem innych komputerów. Skanowanie ruchu sieciowego może nieco spowolnić przeglądanie sieci, ale będzie blokować złośliwe oprogramowanie pochodzące z internetu, w tym także przypadkowe pobieranie plików.

Gdy zostanie znaleziona zainfekowana wiadomość e-mail, jest automatycznie zamieniana z standardową wiadomością e-mail informującą, że oryginalna wiadomość jest zainfekowana. Jeżeli strona internetowa zawiera lub rozprowadza złośliwe oprogramowanie, zostaje automatycznie zablokowana. Specjalna strona z ostrzeżeniem pojawia się aby poinformować użytkownika, że wybrana strona jest niebezpieczna.

Choć nie jest to zalecane, możesz wyłączyć skanowanie antywirusowe poczty lub ruchu sieciowego, aby zwiększyć wydajność systemu. To nie jest poważne zagrożenie, o ile dostęp na żądanie do plików lokalnych, pozostaje włączony.

wyjątki w skanowaniu ruchu

Możesz wybrać, żeby ominąć ruch związany ze skanowaniem w poszukiwaniu złośliwego oprogramowania podczas gdy opcje skanowania ruchu są włączone.

Aby zdefiniować wyjątek:

1. Wybierz rodzaje wyjątków z menu.

2. Zależnie od rodzaju wyjątku zdefiniuj ruch jednostek wykluczonych ze skanowania według poniższych:

- **IP.** Wpisz adres IP, dla którego nie chcesz skanować ruchu przychodzącego i wychodzącego.
- **URL.** Wyklucz ze skanowania określone adresy sieciowe. Aby zdefiniować wyjątki URL skanowania:
 - Podaj adres URL, taki jak `www.example.com/example.html`
 - Użyj znaków do określenia wzorów adresów:
 - Gwiazdka (*) zastępuje zero lub więcej znaków.
 - Znak zapytania zastępuje dokładnie jeden znak. Możesz użyć kilku znaków zapytania aby zdefiniować każdą kombinację określonej liczby znaków. Na przykład, ??? zastępuje każdą kombinację dokładnie 3 znaków.

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

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

- **aplikacja.** Wyklucz ze skanowania określony proces lub aplikację. Aby zdefiniować wyjątki aplikacji skanowania:
 - Wprowadź pełną ścieżkę aplikacji. Na przykład, `C:\Program Files\Internet Explorer\iexplore.exe`
 - Użyj zmiennych środowiskowych do określenia ścieżki aplikacji. Na przykład: `%programfiles%\Internet Explorer\iexplore.exe`

- Użyj symboli wieloznacznych, aby określić pewien wzorec nazw pasujący do aplikacji. Na przykład:
 - `c*.exe` pasuje do wszystkich aplikacji zaczynających się na "c" (chrome.exe).
 - `?????.exe` pasuje do wszystkich aplikacji, których nazwa zawiera część znaków (chrome.exe, safari.exe, etc.).
 - `[^c]*.exe` pasuje do wszystkich aplikacji, pomijając te rozpoczynające się na "c".
 - `[^ci]*.exe` pasuje do wszystkich aplikacji, pomijając te rozpoczynające się na "c" lub "i".

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

Aby usunąć spis z listy, kliknij odpowiadający mu przycisk **- Usuń**.

Sieć WWW

W tej sekcji można skonfigurować ustawienia zabezpieczeń w przeglądarce internetowej.

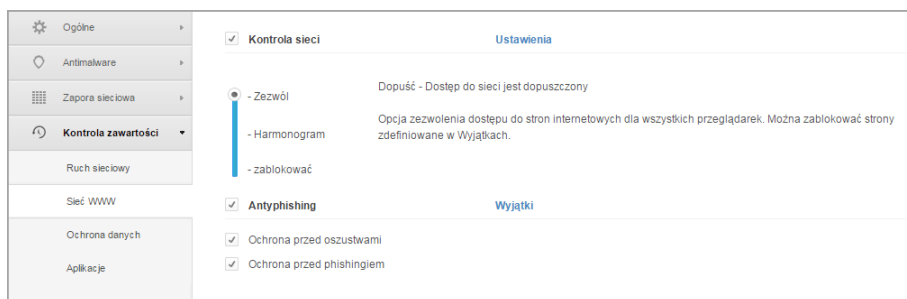
Ustawienia są zorganizowane w poniższych sekcjach:

- [Kontrola sieci](#)
- [Antyphishing](#)

Kontrola sieci

Funkcja kontroli stron internetowych służy do zezwalania użytkownikom i aplikacjom na dostęp do sieci lub blokowanie go w określonych przedziałach czasowych.

Strony www blokowane przez kontrolę stron www nie wyświetlają się w przeglądarce. Zamiast tego wyświetlana jest domyślna strona www informująca użytkownika, że dana strona została zablokowana przez kontrolę stron www.



Polityki Komputera - Kontrola Zawartości - Sieci

Użyj przełącznika, aby włączyć lub wyłączyć **Kontrolę stron WWW**.

Masz trzy opcje konfiguracyjne:

- Wybierz **Pozwól** aby zawsze udzielić dostępu do sieci.
- Wybierz **blokuj** aby nigdy nie udzielać dostępu do sieci.
- Wybierz **Harmonogram** aby umożliwić ograniczenia czasowe w dostępie do stron internetowych w szczegółowym harmonogramie.

Jeżeli wybierasz żeby dopuścić lub zablokować dostęp do strony internetowej, możesz zdefiniować wyjątki do tych działań dla całych kategorii internetowych lub tylko dla określonych adresów internetowych. Naciśnij **Ustawienia** aby skonfigurować twój harmonogram dostępu do sieci i wyjątki według poniższych zaleceń:

Harmonogram

Aby ograniczyć dostęp do internetu o określonych porach dnia, cotygodniowo:

1. Wybierz z siatki przedziały czasowe, w których chcesz aby dostęp do internetu był zablokowany.

Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu. Naciśnij ponownie na komórkę, aby odwrócić zaznaczenie.

Aby rozpocząć nowe zaznaczenie, naciśnij **Zezwól wszystkie** lub **Zablokuj wszystkie**, w zależności od rodzaju ograniczenia, które chcesz wprowadzić.

2. Kliknij **Zapisz**.



Notatka

Endpoint Security będzie dokonywał aktualizacji bez względu na to, czy dostęp do internetu jest zablokowany, czy nie.

Kategorie

Filtr kategorii sieciowych dynamicznie filtruje dostęp do stron internetowych w oparciu o ich zawartość. Możesz użyć Filtru Kategorii internetowych aby zdefiniować wyjątki dla wybranych działań Kontroli Sieci (Zezwalaj lub Blokuj) dla całych kategorii stron internetowych (takich jak gry, treści dla dorosłych lub sieci on-line).

Aby skonfigurować filtr kategorii sieciowych:

1. Wybierz **Filtr kategorii sieci web**.
2. W celu szybkiej kontynuacji, naciśnij jeden ze zdefiniowanych profili (**Agresywny**, **Normalny** lub **Tolerancyjny**). Użyj opisu po prawej stronie skali aby potwierdzić swój wybór. Możesz zobaczyć zdefiniowane wcześniej działania dostępne dla kategorii internetowych przez naciśnięcie przycisku **Kategorie** dostępnego poniżej.
3. Jeśli nie jesteś zadowolony z ustawień domyślnych, możesz zdefiniować niestandardowe filtry.
 - a. Zaznacz **Własny**.
 - b. Naciśnij przycisk **Kategorie** aby rozwinąć odpowiednią sekcję.
 - c. Znajdź kategorię, którą chcesz w na liście i wybierz pożądane działanie z menu.

- Możesz również wybrać **Traktuj kategorie internetowe jak wyjątki dostępu do sieci** jeżeli chcesz zignorować istniejące ustawienia dostępu do sieci i zatwierdzić tylko filtr kategorii sieciowych.
- Kliknij **Zapisz**.



Notatka

- Zezwól** pozwolenie na określenie kategorii sieciowej jest również stosowane do konta w przedziałach czasu w których dostęp do sieci jest zablokowany przez kontrolę sieci.
- Zezwól** pozwala na pracę tylko kiedy dostęp do sieci jest zablokowany przez Kontrolę sieci, kiedy **Blokuj** pozwala na pracę tylko kiedy dostęp do sieci jest dopuszczony przez kontrolę sieci.
- Możesz zastąpić uprawnienia kategorii dla indywidualnych adresów sieciowych przez dodawanie ich z przeciwnymi zezwoleniami w **Kontrola Sieci > Ustawienia > Wyjątki**. Na przykład, jeżeli adres sieciowy jest zablokowany przez Filtr Kategorii Sieciowych, dodaj regułę sieci dla adresów z zezwoleniami ustawionymi na **Zezwól**.

Wyjątki

Możesz również zdefiniować reguły sieci aby jawnie blokować lub zezwalać określone adresy sieciowe, zastępując istniejące ustawienia kontroli Sieci. Użytkownicy będą w stanie, na przykład, uzyskać dostęp do odpowiedniej strony również podczas przeglądanie stron internetowych są zablokowane przez kontrolę internetowej.

Aby stworzyć regułę sieci:

- Wybierz **Użyj wyjątków** aby włączyć wyjątki sieci.
- Podaj adresy jakie chcesz dopuścić albo zablokować w polu **Adresy Sieciowe**.
- Wybierz **Zezwól** lub **Zablokuj** z menu **Pozwolenia**.
- Naciśnij przycisk **+ Dodaj** po prawej stronie tabeli aby dodać adres do listy wyjątków.
- Kliknij **Zapisz**.

Aby edytować regułę sieci:

- Naciśnij na adres internetowy jaki chcesz edytować.
- Zmień istniejący URL.
- Kliknij **Zapisz**.

Usuń regułę sieci:

- Przesuń kursor nad adres sieciowy, który chcesz usunąć.
- Kliknij przycisk **- Usuń**.
- Kliknij **Zapisz**.

Antyphishing

Ochrona Antyphishing automatycznie blokuje znane strony phishingowe aby ustrzec użytkownika przed przypadkowym ujawnieniem prywatnych lub poufnych informacji oszustom internetowym. Zamiast strony phishingu, w przeglądarce zostanie wyświetlona specjalna strona z ostrzeżeniem informująca użytkownika, że wybrana strona jest niebezpieczna.

Zaznacz **Antyphishing** aby aktywować ochronę przed phishingiem. Możliwe jest dalsze dostosowanie Antyphishing przez skonfigurowanie następujących ustawień:

- **Ochrona przed oszustwem.** Wybierz tę opcję jeżeli chcesz rozszerzyć ochronę na inne rodzaje oszustw poza phishingiem. Na przykład, strony internetowe reprezentujące fałszywe firmy, które nie proszą bezpośrednio o informacje prywatne, zamiast tego próbują udawać legalne przedsiębiorstwa i zbierać profity dzięki oszukiwaniu ludzi i przekonywaniu ich do prowadzenia działalności gospodarczej z nimi.
- **Ochrona przed phishingiem.** Zachowaj tę opcję wybraną aby ochronić użytkowników przed próbami phishingu.

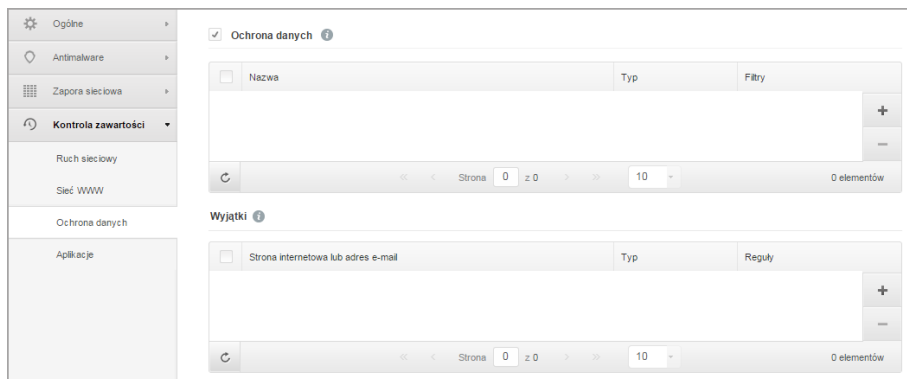
Jeżeli legalna strona internetowa jest niepoprawnie wykryta jako phishing i zablokowana, możesz dodać ją do białej listy aby zezwolić użytkownikom na dostęp. Na tej liście powinny znajdować się tylko w pełni zaufane strony.

Zarządzaj wyjątkami antyphishing:

1. Naciśnij **Wyjątki**.
2. Podaj adres sieciowy i naciśnij przycisk **+** **Dodaj**.
Aby usunąć wyjątek z listy, przesunij kursor nad nią, a następnie kliknij przycisk **-** **Usuń**.
3. Kliknij **Zapisz**.

Ochrona danych

Ochrona danych przed nieautoryzowanym ujawnieniem danych wrażliwych na podstawie reguł określonych przez administratora.



Polityki komputera - Kontrola Zawartości - Ochrona Danych

Możesz utworzyć reguły aby chronić dowolne osobiste lub poufne informacje, takie jak:

- Osobiste informacje klienta
- Szczegóły nazwy i klucza dla wdrożonych produktów i technologii.
- Dane kontaktowe kierownictwa firmy

Chronione informacje mogą zawierać nazwy, numery telefonów, kart kredytowych i kont bankowych itd.

opierając się na regułach ochrony danych stwórz skanowanie Endpoint Security ruchu sieciowego i e-mail opuszczających komputer, zawierających określony ciąg znaków (np. numer karty kredytowej). Jeżeli znajdzie dopasowanie, strona www lub wiadomość e-mail zostaną zablokowane, aby zapobiec wysłaniu chronionych danych. Użytkownik jest natychmiast informowany o podjętym działaniu przez Endpoint Security przez powiadomienie na stronie lub e-mail.

Aby skonfigurować ochronę danych:

1. Użyj pola wyboru, żeby zaznaczyć Ochronę Danych.
2. Utwórz reguły ochrony danych dla wszystkich wrażliwych danych jakie chcesz ochronić. Aby stworzyć regułę:
 - a. Kliknij przycisk *** Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
 - b. Podaj nazwę pod którą reguła będzie przypisana w tabeli reguł. Wybierz sugestywną nazwę, po której administratorzy będą mogli w łatwy sposób zidentyfikować do czego odnosi się ta reguła.
 - c. Podaj dane jakie chcesz ochronić (na przykład, numer telefonu firmy wykonawczej lub wewnętrzną nazwę nowego produktu nad którym pracuje firma). Każda kombinacja słów, liter lub ciągów znaków składających się ze znaków alfanumerycznych i znaków specjalnych (takie jak @, # lub \$) jest dopuszczalna.

Upewnij się, że wprowadziłeś przynajmniej trzy znaki, aby zapobiec omyłkowemu blokowaniu wiadomości i stron internetowych.



WAŻNE

Pod warunkiem, że dane są przechowywane w postaci zaszyfrowanej na zabezpieczonych komputerach, ale są one widoczne w koncie Control Center. Dla dodatkowego bezpieczeństwa, nie należy wprowadzać wszystkich danych, które chcesz chronić. W tym przypadku, musisz wyczyścić opcję **Dopasuj całe słowa**.

d. Skonfiguruj opcje skanowania ruchu według uznania:

- **Skanuj ruch internetowy (HTTP)** - skanuje ruch HTTP (strony WWW) i blokuje wysyłane dane, które pasują do tych zapisanych w regule.
- **Skanuj ruch e-mail (SMTP)** - skanuje ruch SMTP (wiadomości) i blokuje wszystkie wychodzące wiadomości e-mail, które zawierają podane w regule ciągi znaków.

Możesz wybrać zastosowanie reguły tylko jeśli zawartość reguły zgadza się z całym słowami lub jeśli zawartość reguły i jakiegokolwiek wykryty ciąg znaków są identyczne.

e. Kliknij **Zapisz**. Do listy zostanie dodana nowa reguła.

3. Skonfiguruj wyjątki do zasad ochrony danych, dzięki którym użytkownicy będą mogli wysłać chronione dane do autoryzowanych stron i odbiorców. Wyjątki mogą być stosowane globalnie (dla wszystkich reguł) lub tylko dla określonych reguł. Aby dodać wyjątek:

- a. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
- b. Podaj adres sieci lub e-mail na którym użytkownicy są upoważnieni do ujawniania chronionych danych.
- c. Wybierz rodzaj wyjątków (strony internetowe lub adres e-mail).
- d. Z tabeli **Reguły** wybierz reguły ochrony danych w których zostaną zastosowane wyjątki.
- e. Kliknij **Zapisz**. Do listy zostanie dodana nowy nowy wyjątek.



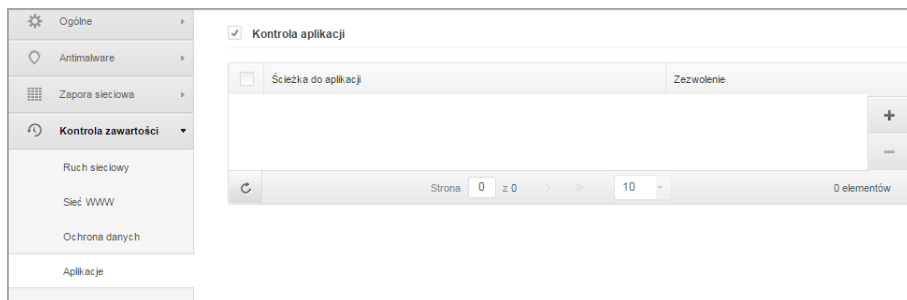
Notatka

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

Aby usunąć regułę lub wyjątek z listy, naciśnij przycisk **- Usuń** po prawej stronie tabeli.

Aplikacje

W tej sekcji można skonfigurować kontrolę aplikacji. Kontrola Aplikacji pomaga w pełni zablokować lub ograniczyć dostęp użytkowników do aplikacji na ich komputerach. W ten sposób można blokować gry, nośniki oraz komunikatory, a także inne rodzaje oprogramowania zwykłego oraz złośliwego.



Polityki Komputera - Kontrola Zawartości - Aplikacje

Aby skonfigurować Kontrole Aplikacji:

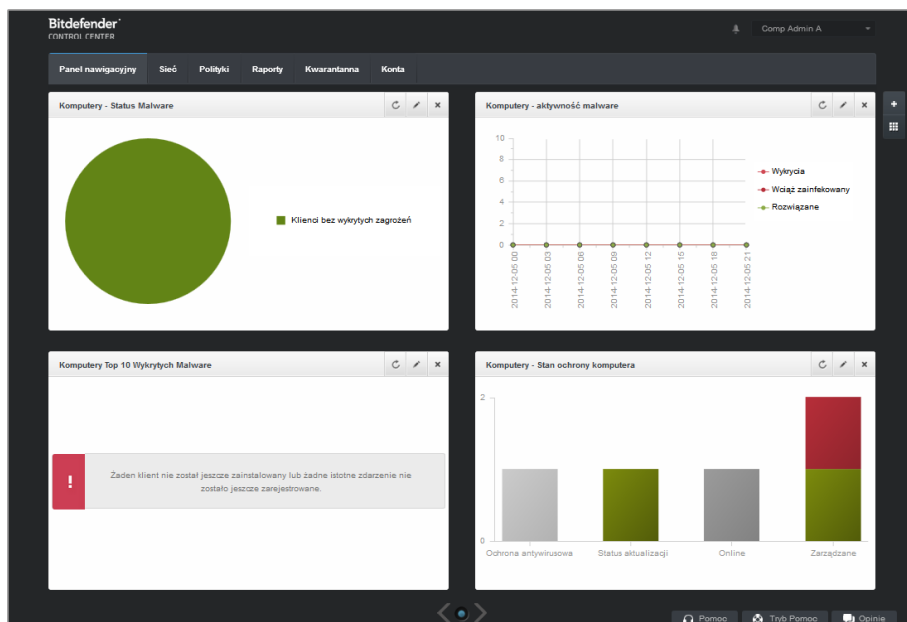
1. Użyj przełącznika, aby włączyć Kontrolę Aplikacji.
2. Określ aplikacje do których chcesz ograniczyć dostęp. Aby ograniczyć dostęp do aplikacji:
 - a. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
 - b. Musisz określić ścieżkę do wykluczonych plików aplikacji na docelowych komputerach. Są na to dwa sposoby:
 - Wybierz z menu wcześniej zdefiniowaną lokalizację i uzupełnij potrzebną ścieżkę w polu edycji. Na przykład, dla aplikacji zainstalowanych w folderze Program Files, wybierz %ProgramFiles% i uzupełnij ścieżkę dodając backslshs (\) i nazwę foldera aplikacji.
 - Podaj pełną ścieżkę w polu edycji. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.
 - c. **dostęp do harmonogramu**. Harmonogram dostępu do aplikacji podczas określonego czasu w trakcie dnia co tydzień.
 - Wybierz z siatki przedziały czasowe, w których chcesz aby dostęp do aplikacji był zablokowany. Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu. Naciśnij ponownie na komórkę, aby odwrócić zaznaczenie.
 - Aby rozpocząć nowe zaznaczenie, naciśnij **Zezwól wszystkie** lub **Zablokuj wszystkie**, w zależności od rodzaju ograniczenia, które chcesz wprowadzić.
 - Kliknij **Zapisz**. Do listy zostanie dodana nowa reguła.

Aby usunąć regułę z listy, naciśnij przycisk **- Usuń** po prawej stronie tabeli. Aby edytować istniejącą regułę, naciśnij nazwę aplikacji.

7. Monitorowanie Panelu

Panel Control Center jest wizualnie dostosowywany poprzez szybki przegląd bezpieczeństwa dla wszystkich chronionych obiektów sieciowych.

Portlety panelu wyświetlają różne informacje bezpieczeństwa w czasie rzeczywistym, używając łatwych do przeczytania wykresów, pozwalając w ten sposób szybko zidentyfikować wszystkie problemy, które mogą wymagać uwagi.



Panel


To jest to co potrzebujesz, żeby wiedzieć o portletach w Panelu:

- Control Center ma kilka wstępnie zdefiniowanych portletów w panelu.
- Każdy portlet w panelu zawiera szczegółowy raport w tle, dostępny za pomocą jednego kliknięcia na wykresie.
- Jest kilka rodzajów portletów zawierających różne informacje o ochronie twoich obiektów sieciowych, takich jak aktualizacje stanu, stan malware, aktywność zapory sieciowej, itp. Aby uzyskać więcej informacji o rodzajach portletów w panelu, odwołaj się do „Dostępne rodzaje raportów” (p. 121)


- Informacje wyświetlone przez portlety zależą tylko od obiektów sieci w twoim koncie. Możesz dostosować cel każdego portletu używając komendy **Edytuj Portlet**.
- Kliknij pozycje legendy wykresu, gdy jest dostępna, aby ukryć lub wyświetlić odpowiednią zmienną na wykresie.
- Portlety są wyświetlane w czterech grupach. Użyj suwaka na dole strony aby przemieszczać się pomiędzy grupami portletów.

Panel łatwo konfigurować, bazuje on na indywidualnych preferencjach. Możesz **Edytować** ustawienia portletu, **dodaj** dodatkowe portlety, **usuń** lub **zmień pozycję** istniejących portletów.

7.1. Odświeżanie Danych Portletów

Aby upewnić się, że portlety wyświetlają ostatnie informacje, naciśnij ikonę  **Odśwież** na pasku tytułowym.


7.2. Edytowanie ustawień portletów

Niektóre portlety oferują informacje o stanie, podczas innego raportu w wydarzeniach bezpieczeństwa w ostatnim czasie. Możesz sprawdzić i skonfigurować okres raportowania dla portletów naciskając ikonę  **Edytuj Portlet** na pasku tytułu.

7.3. Dodawanie nowego portletu

Możesz dodać dodatkowe portlety aby uzyskać informacje, które potrzebuje.

Aby dodać nowe portlety:

1. Przejdź do strony **Panel**.
2. Naciśnij przycisk  **Dodaj Portlet** po prawej stronie panelu. Wyświetlono okno konfiguracji.
3. W zakładce **Szczegóły**, skonfiguruj szczegóły portletu:
 - Rodzaje raportów w tle
 - Sugestywna nazwa portletu
 - Okres aktualizacji

Aby uzyskać więcej informacji o dostępnych rodzajach raportów, odwołaj się do „**Dostępne rodzaje raportów**” (p. 121)

4. W zakładce **Celem** wybierz obiekty sieciowe i grupy zawierające.
5. Kliknij **Zapisz**.

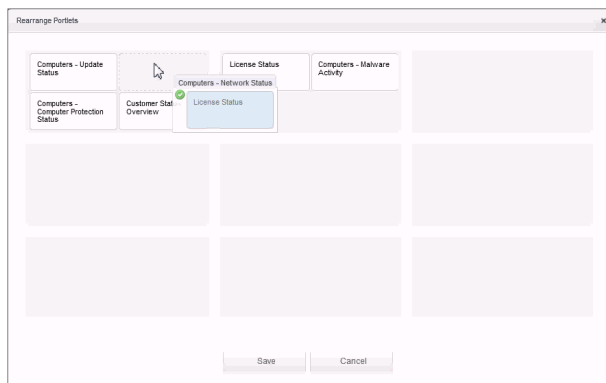
7.4. usuwanie Portletu

Możesz w łatwy sposób usunąć każdy portlet naciskając ikonę **Usuń** na pasku tytułu. Jeżeli usuniesz portlet, nie będziesz mógł go już więcej odzyskać. Jednak, możesz utworzyć inny portlet z takimi samymi ustawieniami.

7.5. Zmiana Układu Portletów

Możesz ułożyć portlety w panelu aby lepiej dostosować go do swoich potrzeb. Aby zmienić układ portletów:

1. Przejdź do strony **Panel**.
2. Naciśnij przycisk **Zmiana układu portletów** po prawej stronie panelu. Okno mapy portletów jest widoczne.
3. Przeciągnij i upuść portlet do żądanej pozycji.
4. Kliknij **Zapisz**.



Zmiana układu portletów w panelu

8. Używanie raportów

Control Center dopuszcza utworzenie i zobaczenie scentralizowanych raportów w statusie bezpieczeństwa zarządzanych obiektów sieciowych. Raporty można używać do różnych celów, m.in.:

- do monitorowania i zapewnienia zgodności z polityką bezpieczeństwa danej organizacji.
- do kontrolowania i oceny stanu zabezpieczeń sieci.
- do identyfikowania problemów z bezpieczeństwem sieci, zagrożeń i luk.
- do monitorowania zdarzeń związanych z bezpieczeństwem oraz aktywności złośliwego oprogramowania.
- zapewniając kierownictwu wyższego szczebla łatwe do zinterpretowania dane na temat bezpieczeństwa sieciowego.

Kilka różnych rodzajów raportów są dostępne więc możesz łatwo dostać informacje, które potrzebujesz. Informacje są przedstawione w formie interaktywnych wykresów i tabel, co pozwala na szybkie sprawdzenie statusu bezpieczeństwa sieci i zidentyfikowanie problemów.

Raporty mogą obejmować dane z całej sieci zarządzanych obiektów sieciowych lub jedynie z określonych grup. W ten sposób z jednego raportu możesz uzyskać:

- Dane statystyczne dotyczące wszystkich lub wybranych grup zarządzanych obiektów sieciowych.
- Szczegółowe informacje dla każdego zarządzanego obiektu sieciowego.
- Lista komputerów z określonymi kryteriami (np. z wyłączoną ochroną antymalware).

Wszystkie raporty są dostępne w Control Center ale możesz zapisać je na swój komputer lub wysłać na e-mail.

Dostępne formaty zawierające Przenośny format dokumentu (PDF) i wartości oddzielone przecinkami (CSV).

8.1. Dostępne rodzaje raportów

To jest lista dostępnych rodzajów raportów dla komputerów:

Status aktualizacji

Pokaż status aktualizacji dla ochrony Endpoint Security zainstalowanej na wybranych komputerach. Status aktualizacji odnosi się do wersji produktu i silników (podpisanych) wersji.

Używając dostępnych filtrów, możesz łatwo znaleźć którzy klienci dokonali aktualizacji lub nie w ciągu ostatnich 24 godzin.

Aktywność malware

Zapewnia informacje na temat wykrytego złośliwego oprogramowania w określonym czasie, na wybranych komputerach. Widać:

- Liczba wykryć (pliki, które zostały znalezione są zainfekowane przez malware)
- Liczba usuniętych infekcji (pliki, które zostały wyleczone lub przesunięte do [kwarantanny](#))
- Liczba infekcji z którymi sobie nie poradzono (pliki, które da się wyleczyć, ale nie można uzyskać dostępu; np. zainfekowany plik przechowywany w niektórych formatach archiwum).

Dla każdego wykrytego zagrożenia, naciśnij na dostępny odnośnik w kolumnach szczegółów dezynfekcji, możesz zobaczyć listę zarażonych komputerów i ścieżek plików. Na przykład, jeśli klikniesz liczbę z kolumny **Rozwiązane** możesz przeglądać pliki i komputery, z których zagrożenie zostało usunięte.

Status szkodliwego oprogramowania

Pomoże Ci znaleźć ile z wybranych komputerów zostało zarażonych malware w określonym przedziale czasowym i jak poradzono sobie z zagrożeniami.

Komputery są pogrupowane w oparciu o te kryteria:

- Komputery bez wykrycia (nie ma zagrożenia malware został wykryty przez określony okres czasu)
- Komputery wyleczone z malware (wszystkie wykryte pliki zostały pomyślnie wyleczone lub przeniesiony do [kwarantanny](#))
- komputery nadal są zainfekowane malware (niektóre z wykrytych plików, odmawiają dostępu)

Dla każdego komputera, naciśnij na dostępny odnośnik w kolumnach szczegółów dezynfekcji, możesz zobaczyć listę zarażeń i ścieżek do zarażonych plików.

Status sieci

Zapewnia dodatkowe informacje o stanie bezpieczeństwa wybranych komputerów. Komputery są pogrupowane w oparciu o te kryteria:

- Stan problemów
- Stan zarządzania
- Stan Infekcji
- Stan ochrony antymalware
- Status aktualizacji produktu
- Status Licencji
- Stan aktywacji sieci dla każdego komputera (online/offline). Jeżeli komputer jest offline, gdy raport jest generowany, musisz zobaczyć datę i czas kiedy był ostatnio widoczny online przez Control Center.

Top 10 zainfekowanych komputerów

Pokazuje Ci top 10 najbardziej zainfekowanych komputerów według ilości wykrytych infekcji w określonym czasie bez wybranych komputerach.



Notatka

Szczegółowa tabela wyświetla wszystkie wykryte malware w top 10 zainfekowanych komputerów.

Top 10 wykrytych malware

Pokazuje top 10 wykrytych malware w określonym czasie na wybranych komputerach.



Notatka

Szczegółowa tabela wyświetla wszystkie komputery, które są zainfekowane przez wykryte malware należące do top 10.

Aktywność Zapory Sieciowej

Informuje Cię o aktywności modułu Firewall Endpoint Security. Możesz zobaczyć liczbę zablokowanych prób ruchu i zablokowanych skanowań portów na wybranych komputerach

Zablokowane strony

Informuje Cię o aktywności modułu kontroli Sieci Endpoint Security. Możesz zobaczyć liczbę zablokowanych stron na wybranych komputerach.

Zablokowane aplikacje

Informuje Cię o aktywności modułu Kontrola Aplikacji Endpoint Security. Możesz zobaczyć liczbę zablokowanych aplikacji na wybranych komputerach.

Aktywność Antyphishingowa

Informuje Cię o aktywności modułu Antyphishing Endpoint Security. Możesz zobaczyć liczbę zablokowanych stron na wybranych komputerach.

Stan ochrony komputera

Zapewnia różne informacje o stanie dotyczącym wybranych komputerów w sieci.

- Stan ochrony antymalware
- Endpoint Security aktualizacja statusu
- Status aktywności sieci (online/offline)
- Stan zarządzania

Możesz zastosować filtry w aspekcie bezpieczeństwa i stanu, aby znaleźć informacje, których szukasz.

Ochrona danych

Informuje Cię o aktywności modułu Ochrony Danych Endpoint Security. Możesz zobaczyć liczbę zablokowanych wiadomości e-mail i stron internetowych na wybranych komputerach.

Zablokowane aplikacje przez skanowanie behawioralne

Informuje o aplikacjach zablokowanych przez AVC (Aktywna Kontrola Wirusów) / IDS (System Wykrycia Intruzów) Możesz zobaczyć liczbę aplikacji zablokowanych przez AV / IDS dla wybranego komputera. Naciśnij liczbę zablokowanych aplikacji dla komputera, który Cię interesuje aby zobaczyć listę zablokowanych aplikacji z połączonymi informacjami (nazwa aplikacji, powód dla którego została zablokowana, liczna zablokowanych prób z data i czasem ostatniego blokowania).

Status Modułu Punktu Końcowego

Zapewnia przegląd stanu modułów ochrony Endpoint Security dla wybranych komputerów. Możesz zobaczyć, które moduły są aktywne, a które są wyłączone lub nie są zainstalowane.

8.2. Tworzenie raportów

Możesz utworzyć dwie kategorie raportów:

- **Raporty natychmiastowe.** Natychmiastowe raporty są automatycznie wyświetlane po wygenerowaniu.
- **Zaplanowane raporty.** Zaplanowane raporty mogą zostać skonfigurowane aby uruchomić się określonego dnia o danej godzinie. Lista wszystkich zaplanowanych raportów wyświetla się na stronie **Raporty**.



WAŻNE

Raporty natychmiastowe są automatycznie usuwane kiedy zamykasz stronę raportów. raporty zaplanowane są zapisane i wyświetlone na stronie **Raporty**.

aby stworzyć raport:

1. Przejdź do strony **Raporty**.
2. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.

Edytuj raport

Szczegóły

Typ: Aktywność malware

Nazwa: * Aktywność malware

Ustawienia

Teraz

Zaplanowane

Występowanie: cogodzinny

Co (godziny): 1

Odstępy między raportami: Dziś

Pokaż:

Wszystkie malware

Tylko nierozwiązane malware

Dostawa:

Wyślij e-mailem

Wybierz Cel

Zapisz Anuluj

Opcje raportów komputera

- Wybierz interesujący cię rodzaj raportu z menu. Aby uzyskać więcej informacji, odwołaj się do „[Dostępne rodzaje raportów](#)” (p. 121).
- Podaj sugestywną nazwę dla raportu. Kiedy wybierasz nazwę, weź pod uwagę rodzaj raportu, cel i ewentualne opcje raportu.
- Skonfiguruj powtórzenia raportu:
 - wybierz **Teraz** aby stworzyć natychmiastowy raport.
 - Wybierz **Planowane** aby skonfigurować raport, który zostanie automatycznie wygenerowany w określonym czasie:
 - Po godzinach, w określonym przedziale pomiędzy godzinami.
 - Codziennie. W tym przypadku, można także ustawić czas rozpoczęcia (godzinę i minuty).
 - Raz w tygodniu, w określonych dniach tygodnia i o określonym czasie rozpoczęcia (godzinę i minuty).

- Raz w miesiącu, w określonych dniach miesiąca i o określonym czasie rozpoczęcia (godzinę i minuty).
6. dla większości rodzajów musisz określić przedział czasu, których zawarte dane się odnoszą. Raport wyświetli tylko dane z wybranego przedziału czasu.
 7. Kilka rodzajów raportów zapewniają opcje filtrowania, aby pomóc Ci łatwo znaleźć informacje, które Cię interesują. Użyj opcji filtrowania opcji w sekcji **Pokaż** w celu uzyskania jedynie potrzebnych informacji.
Na przykład dla raportu **Status Aktualizacji** możesz wybrać aby wyświetlić tylko listę komputerów, które zostały zaktualizowane w określonych przedziałach czasu, lub te które potrzebują zostać ponownie uruchomione aby ukończyć aktualizacje.
 8. **Dostawa.** Aby otrzymać zaplanowane raport e-mail, wybierz odpowiednią opcję. Podaj adres e-mail, który chcesz w polu poniżej.
 9. **Wybierz cel.** Przewiń w dół, aby skonfigurować cel raportu. Wybierz grupę dla jakiej chcesz uruchomić raporty.
 10. Naciśnij **Generuj** aby utworzyć natychmiastowy raport lub **Zapisz** aby zaplanować raport.
 - Jeżeli chcesz utworzyć natychmiastowy raport, zostanie wyświetlony zaraz po naciśnięciu **Generuj**. Czas wymagany do utworzenia raportów uzależniony jest od liczby zarządzanych komputerów. Zaczekaj na stworzenie raportu.
 - Jeżeli wybrałeś stworzenie zaplanowanego raportu, wyświetli się on na liście na stronie **Raporty**. Gdy raport został stworzony możesz zobaczyć go naciskając na odpowiedni link w kolumnie **Zobacz raport** na stronie **Raport**

8.3. Przeglądania i zarządzanie zaplanowanych raportów

Aby zobaczyć i zarządzać zaplanowanymi raportami przejdź do strony **Raporty**.

Nazwa raportu	Typ	Powtarzalność	Pokaż raport
Rap1	Status Modułu Punktu ...	codziennie	09 Gru 2014 - 08:49
Rap2	Status aktualizacji	Codziennie	09 Gru 2014 - 00:00
Rap3	Zablokowane aplikacje	Tygodniowo	09 Gru 2014 - 00:00

Strona Raportów

Wszystkie zaplanowane raporty wyświetlono w tabeli. Możesz zobaczyć wygenerowane raporty zaplanowane i użyć informacji o nich:

- Nazwa i rodzaj raportu.
- Kiedy raport zostanie wygenerowany.



Notatka

Zaplanowane raporty są dostępne tylko dla użytkownika, który je stworzył.

Aby posortować raporty według określonej kolumny, naciśnij na nagłówek kolumny. Kliknij nagłówek ponownie, aby zmienić kolejność porządkowania.

Szczegółowe dane raportu wyświetlone są w tabeli, która składa się z kilkunastu kolumn, zawierających różne informacje. Tabela może rozciągać się na kilka stron (domyślnie, na stronie mieści się tylko 10 wpisów). Do przeglądania kolejnych stron raportu służą przyciski znajdujące się na dole tabeli.

Aby łatwo znaleźć to, czego szukasz, skorzystaj z pola wyszukiwania lub poniżej opcje filtrowania w nagłówkach kolumn.

Aby uporządkować szczegóły raportu według określonej kolumny, kliknij jej nagłówek. Kliknij nagłówek ponownie, aby zmienić kolejność porządkowania.

Aby wyczyścić pole wyszukiwania, umieść nad nim kursor i kliknij w ikonę ✕ **Usuń**.

aby upewnić się, że ostatnie informacje się wyświetlają naciśnij ikonę ↻ **Odśwież** w lewym dolnym rogu tabeli.

8.3.1. Przeglądanie raportów

Aby zobaczyć raport:

1. Przejdź do strony **Raporty**.
2. Sortowanie raportów po nazwie, rodzaju lub powtarzalność, aby łatwo znaleźć raport, którego szukasz.
3. Naciśnij odpowiedni link w kolumnie **Zobacz raport** aby wyświetlić raport.

Wszystkie raporty składają się z sekcji podsumowania (górną część raportu) i sekcji szczegółów (dolną część raportu).

- Sekcja Podsumowanie zapewnia dane statystyczne (wykresy kołowe i grafiki) dla wszystkich obiektów sieciowych lub grup docelowych, a także ogólne informacje na temat raportu, takie jak okres sprawozdawczy (jeśli dotyczy), cel raportu itp.
- Sekcja Szczegóły dostarcza szczegółowych informacji dla każdego zarządzanego obiektu sieci.



Notatka

- Aby skonfigurować informacje wyświetlone na wykresie, naciśnij legendę wpisów, aby pokazać lub ukryć wybrane dane.
- Naciśnij graficzny obszar, który cie interesuje, żeby zobaczyć szczegóły w tabeli umieszczonej poniżej wykresu.

8.3.2. Edytowanie zaplanowanego raportu.



Notatka

kiedy edytujesz zaplanowany raport, aktualizacja zostanie zastosowana od następnego uruchomienia raportu. Wcześniej generowane raporty nie zostaną zmienione przez edycję.

Aby zmienić ustawienia zaplanowanego raportu:

1. Przejdź do strony **Raporty**.
2. Naciśnij nazwę raportu.
3. Zmień ustawienia raportu jeżeli potrzebujesz. Możesz zmienić jedną z następujących:
 - **Nazwa raportu.** Wybierz sugestywną nazwę dla raportu, aby w łatwy sposób móc zidentyfikować co zawiera. Kiedy wybierasz nazwę, weź pod uwagę rodzaj raportu, cel i ewentualne opcje raportu. Raporty wygenerowane przez zaplanowany raport jest nazwany po nim.
 - **Wznowienie raportu (harmonogram).** Możesz zaplanować automatyczne generowanie raportu godzinne(w odstępie godzinowym), dzienne (w odstępie dziennym), tygodniowe (w konkretnym dniu tygodnia o danej godzinie) lub miesięcznie (konkretnego dnia miesiąca o danej godzinie). W zależności od wybranego planu, raport będzie zawierał tylko dane z ostatniego dnia, tygodnia lub miesiąca, odpowiednio.
 - **Ustawienia.**
 - Możesz zaplanować automatyczne generowanie raportu godzinne(w odstępie godzinowym), dzienne (w odstępie dziennym), tygodniowe (w konkretnym dniu tygodnia o danej godzinie) lub miesięcznie (konkretnego dnia miesiąca o danej godzinie). W zależności od wybranego planu, raport będzie zawierał tylko dane z ostatniego dnia, tygodnia lub miesiąca, odpowiednio.
 - Raport będzie zawierał dane z wybranego przedziału czasu. Możesz zmienić przedział czasu przy następnym uruchomieniu.
 - Większość raportów zapewnia opcje filtrowania, które pomogą ci łatwo znaleźć informacje które Cie interesują. Kiedy przeglądasz raport na konsoli, wszystkie informacje będą dostępne, niezależnie od wybranych opcji. Jeżeli pobierasz lub wysyłasz raport e-mailem, tylko podsumowanie raportu i wybrane informacje

zostaną załączone do pliku PDF. Szczegóły raportu będą dostępne tylko w formacie CSV.


- Możesz wybrać aby dostać raport mailem.
- **Wybierz cel.** Wybrana opcja wskazuje rodzaj aktualnego raportu docelowego (zarówno grupy jak i indywidualne obiekty sieciowe). Naciśnij odpowiadający link aby wyświetlić aktualny raport docelowy. aby zmienić, wybierz grupy i obiekty sieciowe, które mają być zawarte w raporcie.

4. Naciśnij **Zapisz** aby zastosować zmiany.

8.3.3. Usuwanie zaplanowanych raportów

Kiedy zaplanowany raport nie jest dłużej potrzebny, najlepiej go usunąć. Usuwając zaplanowany raport, zostaną usunięte wszystkie raporty, które zostały wygenerowane automatycznie do tego czasu.

Aby usunąć zaplanowany raport:

1. Przejdź do strony **Raporty**.
2. Wybierz raport, który chcesz usunąć.
3. Kliknij przycisk  **Usuń** po prawej stronie tabeli.

8.4. Zapisywanie raportów

Domyślnie, zaplanowane raporty są automatycznie zapisywane w Control Center.

Jeżeli potrzebujesz żeby raporty były dostępne przez dłuższy okres czasu, możesz zapisać je na komputerze. Podsumowanie raportu będzie dostępne w formacie PDF, gdzie szczegóły raportu będą dostępne tylko w formacie CSV.

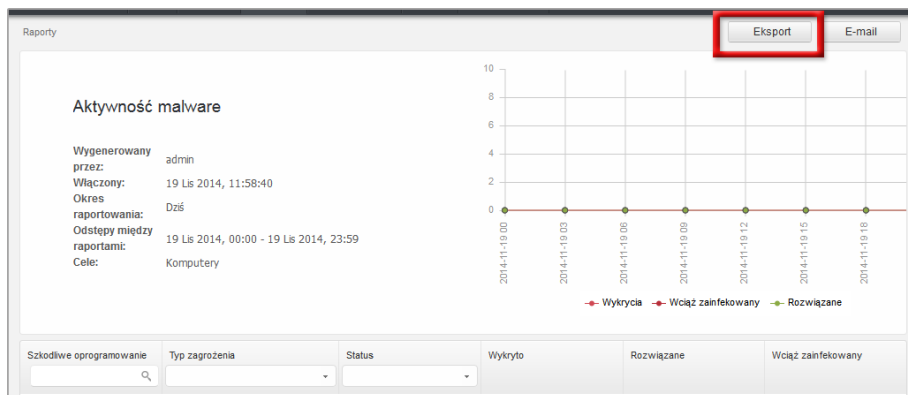
Masz dwie możliwości zapisywania raportów:

- [Eksport](#)
- [Pobierz](#)

8.4.1. Eksportowanie raportów

Aby wyeksportować raport do twojego komputera:

1. Kliknij na przycisk **Eksport** w górnym prawym rogu strony raportu.



Raporty - Opcje eksportu

- Wybierz odpowiedni format raportu:
 - Przeñośny Format Dokumentu (PDF) lub
 - Wartości oddzielone przecinkami (CSV)
- W zależności od ustawień przeglądarki, plik można pobrać automatycznie do domyślnej lokalizacji pobierania, lub określić folder docelowy w oknie pobierania, które się pojawi.

8.4.2. Raporty pobierania

Archiwum Raport zawiera zarówno podsumowanie raportów i szczegółowych raportów.

Aby pobrać archiwum raportu:

- Przejdź do strony **Raporty**.
- wybierz raport jaki chcesz zapisać.
- Naciśnij przycisk **Pobierz** i wybierz **Ostatnia Instancja**, aby pobrać ostatni wygenerowany raport lub **Pełne Archiwum** aby pobrać archiwum zawierające wszystkie instancje.

W zależności od ustawień przeglądarki, plik można pobrać automatycznie do domyślnej lokalizacji pobierania, lub określić folder docelowy w oknie pobierania, które się pojawi.

8.5. Raporty E-mailów

Możesz wysłać raporty na e-mail używając poniższych opcji:

- Aby wysłać raport, który oglądasz e-mailem, naciśnij przycisk **E-mail** w prawym górnym rogu strony raportów. Raport zostanie wysłany na adres E-mail połączony z Twoim kontem.

2. Aby skonfigurować zaplanowane raporty dostawy e-mail:
 - a. Przejdź do strony **Raporty**.
 - b. Naciśnij wybraną nazwę raportu.
 - c. W **Opcje > dostawa**, wybierz **Wyślij przez e-mail na**.
 - d. Podaj odpowiedni adres e-mail w polu poniżej. Możesz dodać dowolną liczbę adresów poczty elektronicznej.
 - e. Kliknij **Zapisz**.



Notatka

Tylko podsumowanie raportu i wykres zostaną uwzględnione w pliku PDF wysłanym przez e-mail. Szczegóły raportu będą dostępne w pliku CSV.

8.6. Drukowanie raportów

Control Center nie obsługuje obecnie funkcji przycisku drukowania. aby wydrukować raport, musisz najpierw zapisać go na swoim komputerze.

9. Kwarantanna

Domyślnie, Endpoint Security izoluje podejrzane pliki i pliki zainfekowane złośliwym oprogramowaniem, których nie można wyleczyć w bezpiecznym obszarze zwanym kwarantanna. Kiedy wirus znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być uruchomiony lub otwierany.

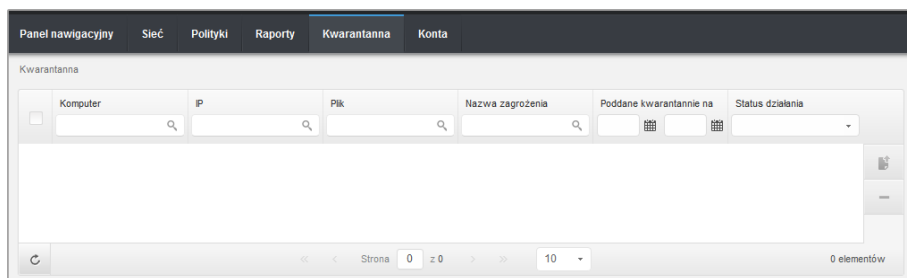
Security for Endpoints przechowuje pliki kwarantanny na każdym zarządzanym komputerze. Używając Control Center masz opcje do usunięcia lub przywrócenia konkretnych plików kwarantanny.

Pliki poddane kwarantannie są domyślnie wysyłane do laboratoriów firmy Bitdefender w celu analizy szkodliwego oprogramowania dokonywanej przez badaczy Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

Ponadto pliki poddane kwarantannie są skanowane po każdej aktualizacji sygnatur wirusów. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.

Control Center zawiera szczegółowe informacje na temat wszystkich plików przeniesiony do kwarantanny na obiektach sieciowych zarządzanych z twojego konta.

Aby sprawdzić i zarządzać plikami w kwarantannie, przejdź do strony **Kwarantanna**.




Strona Kwarantanny

Informacje o plikach kwarantanny są wyświetlane w tabeli. Możesz korzystać z następujących informacji:

- Nazwa obiektów sieciowych, na których zostało wykryte zagrożenie.
- Adres IP obiektów sieciowych na których zostało wykryte zagrożenie.
- Ścieżka do zainfekowanego lub podejrzanego pliku na obiekcie sieci na którym został wykryty.

- Nazwa nadana dla zagrożenia malware przez testerów bezpieczeństwa Bitdefender.
- Czas w jakim plik był w kwarantannie.
- Zawieszenie działań w oczekiwaniu na wniosek administratora, które należy podjąć na pliku poddanym kwarantannie.

aby upewnić się, że ostatnie informacje się wyświetlają naciśnij przycisk  **Odśwież** w lewym dolnym rogu tabeli. Może być potrzebne abyś spędził więcej czasu na tej stronie.

9.1. Nawigacja i Wyszukanie

W zależności od liczby zarządzanych obiektów sieciowych i charakteru infekcji, liczba plików kwarantanny może być czasami większa. Tabela może rozciągać się na kilka stron (domyślnie, na stronie mieści się tylko 10 wpisów).


Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

Jeżeli wyświetla się za dużo wpisów, możesz użyć pola wyszukiwania pod nagłówkiem kolumny aby filtrować wyświetlone daty. Na przykład, możesz wyszukać określonego zagrożenia wykrytego w sieci dla określonego obiektu sieciowego. Możesz również nacisnąć nagłówki kolumny aby posortować dane według określonej kolumny.

9.2. Przywracanie plików kwarantanny

W konkretnych przypadkach może być konieczne, aby przywrócić pliki kwarantanny do ich oryginalnej lokalizacji lub do lokalizacji alternatywnej. Jedną sytuacją jest wtedy gdy chcesz odzyskać ważne pliki przechowywane w zainfekowanym archiwum, które jest w kwarantannie.

Aby przywrócić jeden lub więcej plików kwarantanny:

1. Przejdź do strony **Kwarantanna**.
2. Zaznacz pola odpowiadające plikom kwarantanny które chcesz odzyskać.
3. Naciśnij przycisk  **Przywróć** po prawej stronie tabeli.
4. wybierz lokalizację gdzie chcesz przywrócić pliki (oryginalna lub niestandardowa lokalizacja na docelowym komputerze).

Jeżeli wybierzesz, żeby przywrócić do niestandardowej lokalizacji, musiszz najpierw podać ścieżkę w odpowiednim polu. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych. Aby uzyskać więcej informacji, odwołaj się do „[Używa zmiennych systemowych](#)” (p. 149).

- Wybierz **Automatyczne dodawanie wyjątków w polityce** aby wykluczyć pliki, które mają być przywrócone w następujących skanowaniach. Wyjątki mają zastosowanie do wszystkich polityk mających wpływ na wybrane pliki, z wyjątkiem polityki domyślnej, która nie może być modyfikowana.
- Naciśnij **Zapisz** aby żądać przywrócenia pliku. Możesz zobaczyć oczekujące działania w kolumnie **Działanie**.
- Żądane działanie jest przekazywane do komputerów docelowych bezpośrednio lub jak tylko pojawią się online. Gdy plik zostanie przywrócony, to odpowiedni wpis zniknie z tabeli kwarantanny.

9.3. Automatyczne usunięcie plików kwarantanny

Domyślnie wszystkie pliki objęte kwarantanną dłużej niż 30 dni są automatycznie usuwane. To ustawienie może zostać zmienione edytując przypisane polityki do zarządzanych obiektów sieciowych.

Aby zmienić przedział automatycznego usuwania plików poddanych kwarantannie:

- Przejdź do strony **Polityki**.
- Znajdź politykę przypisaną do obiektów sieciowych dla których chcesz zmienić ustawienia i naciśnij jego nazwę.
- Przejdź do sekcji **Antymalware > Kwarantanna**.
- Wybierz żądany czas automatycznego usuwania z menu.
- Naciśnij **Zapisz** aby zastosować zmiany.

9.4. Usuwanie plików kwarantanny

Jeżeli chcesz usunąć pliki kwarantanny ręcznie, musisz najpierw być pewien, że pliki, które wybrałeś nie są potrzebne. Użyj tych porad jeżeli chcesz usunąć pliki kwarantanny:

- Plik faktycznie może być złośliwym oprogramowaniem. Jeśli prowadzisz badania, mogą doprowadzić cię do takiej sytuacji, możesz szukać w kwarantannie określonego zagrożenia i usunąć je z kwarantanny.
- Możesz bezpiecznie usunąć:
 - Nieważne pliki archiwum.
 - Zainfekowane pliki instalacyjne

Aby usunąć jeden lub więcej plików kwarantanny:

- Przejdź do strony **Kwarantanna**.
- Sprawdź listę plików kwarantanny i wybierz pole odpowiadające plikowi, który chcesz usunąć.

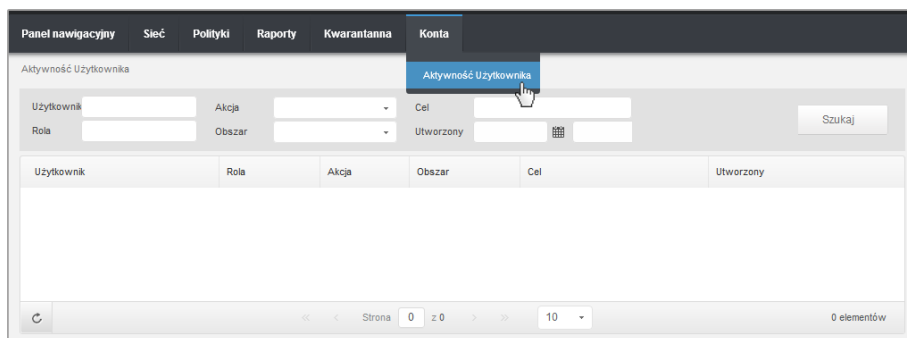
3. Kliknij przycisk **Usuń** po prawej stronie tabeli. Możesz zobaczyć oczekujący status w kolumnie **Działanie**.
4. Żądane działanie jest przekazywane do docelowych obiektów sieciowych bezpośrednio lub jak tylko pojawią się online. Gdy plik zostanie usunięty, w odpowiedni wpis zniknie z tabeli kwarantanny.

10. Dziennik Aktywności Użytkownika

Control Center rejestruje wszystkie operacje i akcje wykonane przez użytkowników. Lista aktywności użytkownika zawiera poniższe wydarzenia, zależne od twojego poziomu dostępu administracyjnego:

- Logowanie i wylogowywanie
- Tworzenie, edytowanie, zmiana nazwy i usuwanie raportów
- Dodawanie i usuwanie portletów z panelu
- Tworzenie, edytowanie i usuwanie poświadczeń
- Tworzenie, modyfikowanie, pobieranie i usuwanie pakietów internetowych
- Tworzenie zadań sieciowych
- Tworzenie, edytowanie, zmiana nazwy i usuwanie kont użytkowników
- Usuwanie i przesuwanie komputerów pomiędzy grupami
- Tworzenie, przesuwanie, zmiana nazwy i usuwanie grup
- Usuwanie i przywracanie plików kwarantanny
- Tworzenie, edytowanie i usuwanie kont użytkowników
- Tworzenie, edytowanie, zmienianie nazwy, przypisywanie i usuwanie polityk

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



Strona aktywności użytkownika

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


Kolumny tabeli dostarczają przydatnych informacji na temat wymienionych wydarzeń:

- Nazwa użytkownika, który wykonał akcję.

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

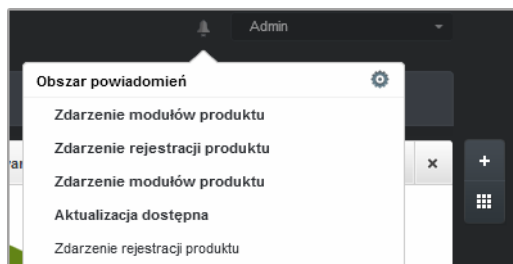
Aby posortować wydarzenia według określonej kolumny, naciśnij na nagłówek kolumny. Naciśnij nagłówek kolumny ponownie aby odwrócić kolejność sortowania.

Aby zobaczyć szczegółowe informacje o wydarzeniu, wybierz je i sprawdź sekcje pod tabelą.


aby upewnić się, że ostatnie informacje się wyświetlają naciśnij przycisk  **Odśwież** w lewym dolnym rogu tabeli.

11. Powiadomienia

W zależności od zdarzeń mogących wpłynąć na twoją sieć, Control Center wyświetli różne powiadomienia, informując o stanie bezpieczeństwa twojego środowiska. Powiadomienia zostaną wyświetlone w **Obszarze Powiadomień**, znajdującym się u góry interfejsu Control Center.



Obszar powiadomień

Gdy nowe zdarzenie zostanie wykryte w sieci, obszar powiadomień wyświetli czerwoną ikonę  wskazującą liczbę nowo wykrytych zdarzeń. Naciskając ikonę wyświetlasz listę wykrytych zdarzeń.

11.1. Rodzaje powiadomień

To jest lista aktywnych rodzajów powiadomień:

Epidemia Malware

To powiadomienie jest wysłane do użytkowników, którzy mają przynajmniej 5% z wszystkich zarządzanych obiektów sieciowych zainfekowanych przez to samo malware.

Możesz skonfigurować próg epidemii malware w oknie **Ustawienia Powiadomień**. Aby uzyskać więcej informacji, odwołaj się do „[Konfiguracja ustawień powiadomień](#)” (p. 141).

Licencja wygasła

Powiadomienia są wysyłane 30, siedem dni i zawsze jeden dzień przed wygaśnięciem licencji.

Limit wykorzystania licencji został osiągnięty

To powiadomienie jest wysyłane jeżeli wszystkie z aktywnych licencji zostały użyte.

Limit wykorzystania licencji został prawie osiągnięty

To powiadomienie jest wysyłane jeżeli 90% z aktywnych licencji zostało użytych.

Aktualizacja dostępna

To powiadomienie poinformuje Cię o nowej aktualizacji Small Office Security.

Zdarzenie Antyphishing

To powiadomienie informuje cię za każdym razem jak agent punktu końcowego blokuje znana stronę phishing przed próbą dostępu. To powiadomienie również podaje szczegóły o próbach dostępu przez punkty końcowe do niezauważanych stron (nazwa i IP), zainstalowanym agencie i blokowanych URL.

Zdarzenie Firewall

Z tym powiadomieniem jesteś informowany za każdym razem gdy moduł zapory sieciowej zainstalowanego agenta blokuje port skanowania lub aplikacje przed dostępem do internetu w zależności od zastosowanej polityki.

Zdarzenie AVC/IDS

To powiadomienie jest wysyłane za każdym razem jak potencjalnie niebezpieczna aplikacja jest wykryta i zablokowana na punkcie końcowym w twojej sieci. Możesz również znaleźć szczegóły dotyczące niebezpiecznego rodzaju aplikacji, nazwy i ścieżki.

Zdarzenie Kontroli Użytkownika

To powiadomienie jest uruchamiane za każdym razem gdy aktywność użytkownika taka jak przeglądanie stron internetowych lub aplikacje są zablokowane przez klienta punktu końcowego poprzez zastosowanie polityki.

Zdarzenie Ochrony Danych

To powiadomienie jest wysyłane za każdym razem gdy ruch danych jest zablokowany w punkcie końcowym poprzez reguły ochrony danych.


Zdarzenie modułów produktu

To powiadomienie jest wysyłane za każdym razem jak moduł bezpieczeństwa na zainstalowanym agencie zostanie zablokowany.

Zdarzenie rejestracji produktu

To powiadomienie informuje cię o zmianach stanu rejestracji zainstalowanych agentów w twojej sieci.

11.2. Zobacz powiadomienia

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

Powiadomienia	
Typ	Utworzony
<input type="checkbox"/> Zdarzenie modułów produktu	14 Lis 2014, 16:41:45
<input type="checkbox"/> Zdarzenie rejestracji produktu	14 Lis 2014, 16:40:39
<input type="checkbox"/> Zdarzenie modułów produktu	14 Lis 2014, 16:40:39
<input type="checkbox"/> Aktualizacja dostępna	13 Lis 2014, 11:00:35
<input type="checkbox"/> Zdarzenie rejestracji produktu	12 Lis 2014, 10:19:12
<input type="checkbox"/> Zdarzenie modułów produktu	12 Lis 2014, 10:19:12

Strona powiadomień

W zależności od liczby powiadomień, tabela może obejmować kilka stron (domyślnie tylko 10 wpisów jest wyświetlanych na jednej stronie).

Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli.



Aby zmienić liczbę wpisów wyświetlanych na stronie, wybierz inną opcję z menu obok przycisków nawigacyjnych.

Jeżeli jest za mało wpisów, możesz użyć pola wyszukiwania pod nagłówkiem kolumny w menu filtry na górze tabeli, aby odfiltrować wyniki według daty.

- Aby odfiltrować powiadomienia, wybierz rodzaj powiadomień jaki chcesz zobaczyć z menu **Rodzaj**. Jeżeli wiele powiadomień zostało wygenerowanych, możesz wybrać przedziały czasu podczas których powiadomienia zostały wygenerowane, aby zredukować ilość wpisów w tabeli.
- Aby zobaczyć szczegóły powiadomień, naciśnij nazwę powiadomienia w tabeli. Sekcja **Szczegóły** gdzie możesz zobaczyć wydarzenia, które generują powiadomienia, wyświetla się pod tabelą.

11.3. Usuwanie powiadomień

Aby usunąć powiadomienia:



1. Naciśnij przycisk  **Obszar Powiadomień** po prawej stronie menu i naciśnij **Zobacz wszystkie powiadomienia**. Wyświetlana jest tabela zawierająca wszystkie powiadomienia.
2. Wybierz powiadomienia, które chcesz usunąć.
3. Kliknij przycisk  **Usuń** po prawej stronie tabeli.

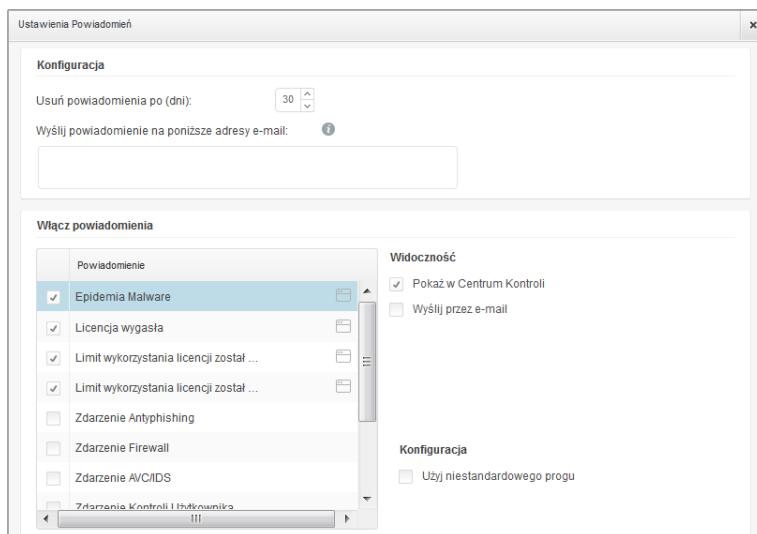
Możesz dodatkowo skonfigurować powiadomienia, które zostaną automatycznie usunięte po określonej ilości dni. Aby uzyskać więcej informacji, odwołaj się do „[Konfiguracja ustawień powiadomień](#)” (p. 141).

11.4. Konfiguracja ustawień powiadomień

Rodzaj powiadomień jaki ma być wysłany na adres e-mail, może być konfigurowany dla każdego użytkownika.

Aby skonfigurować ustawienia powiadomień:

1. Naciśnij przycisk  **Obszar Powiadomień** po prawej stronie menu i naciśnij **Zobacz wszystkie powiadomienia**. Wyświetlana jest tabela zawierająca wszystkie powiadomienia.
2. Kliknij przycisk  **konfiguruj** po prawej stronie tabeli. Okno **ustawienia Powiadomień** jest widoczne.



Ustawienia Powiadomień




Notatka

Masz dodatkowo dostęp do okna **Ustawienia Powiadomień** używając ikony  **konfiguracja** z górnego prawego rogu okna **Obszar Powiadomień**.

3. W sekcji **Konfiguracja** możesz zdefiniować poniższe ustawienia:
 - Możesz skonfigurować powiadomienia, które zostaną automatycznie usunięte po pewnej ilości dni. Podaj ilość dni jaka chcesz, w polu **Usunąć Powiadomienia po (dni)**
 - Opcjonalnie, możesz wybrać żeby wysłać powiadomienia na określony adres e-mail. Podaj adresy e-mail w odpowiednim polu, naciskając **Enter** po każdym adresie.

4. W sekcji **Włącz Powiadomienia** możesz wybrać rodzaj powiadomień jakie chcesz otrzymywać od Small Office Security. Możesz również skonfigurować widoczność i opcje wysyłania indywidualne dla każdego rodzaju powiadomień.

Wybierz jakie chcesz powiadomienia z listy. Aby uzyskać więcej informacji, odwołaj się do „Rodzaje powiadomień” (p. 138). Podczas wyboru rodzaju powiadomień, możesz skonfigurować specyficzne opcje po prawej stronie:

- **Pokaż w konsoli** określa rodzaje zdarzeń wyświetlanych w Control Center, z pomocą ikon  **Obszaru Powiadomień**.
- **Wyślij przez e-mail** określa rodzaje zdarzeń jakie są wysyłane na określone adresy e-mail. W tym przypadku, wymaga podania adresu e-mail w odpowiednim polu, naciśnij **Enter** po każdym adresie.



Notatka

Domyślnie, powiadomienie o epidemii Malware jest wysyłane do użytkowników, którzy mają przynajmniej 5% z wszystkich zarządzanych obiektów sieciowych zainfekowanych przez to samo malware. Aby zmienić wartość dla progu epidemii, wybierz opcję **Użyj niestandardowego progu**, następnie podaj wartość jaką chcesz w polu **Próg Epidemii Malware**.

5. Kliknij **Zapisz**.

12. 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.

12.1. Bitdefender Wsparcie Techniczne

Bitdefender Centrum pomocy dostępne pod adresem <http://www.bitdefender.com/support/business.html>, to miejsce gdzie uzyskasz wszelką pomoc dla twoich produktów Bitdefender.

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

- Znana baza artykułów
- Bitdefender forum pomocy
- Dokumentacja produktu

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

Znana baza artykułów

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

Baza wiedzy Bitdefender jest publiczna i bezpłatna. Informacje, które zawiera, stanowią kolejny sposób na dostarczenie klientom Bitdefender, potrzebnej wiedzy technicznej i wsparcia. Prawidłowe żądania informacji lub raportów o błędach, pochodzące od klientów Bitdefender, w końcu znajdują drogę do Bazy Wiedzy Bitdefender. jako raporty informujące o poprawkach, sposoby ominięcia problemów czy pliki pomocy produktu i teksty informacyjne.

Baza Wiedzy Bitdefender dla produktów biznesowych jest dostępna w każdej chwili na <http://www.bitdefender.com/support/business.html>.

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 znalezienie 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.

Możesz sprawdzić i pobrać najnowszą wersję dokumentacji dla produktów firmy Bitdefender na [Centrum pomocy](#) > Dokumentacja.

12.2. Prośba o pomoc

Prosimy o kontakt w celu uzyskania pomocy za pośrednictwem naszego Centrum pomocy online:

1. Odwiedź <http://www.bitdefender.com/support/contact-us.html>.
2. Skorzystaj z formularza kontaktowego, aby otworzyć pomoc e-mail lub uzyskać dostęp do innych dostępnych opcji kontaktu.

12.3. Używanie Narzędzi Pomocy

Narzędzie wsparcia Small Office Security jest stworzone żeby pomagać użytkownikom i łatwo uzyskać potrzebne informacje ze wsparcia technicznego. Uruchoom Narzędzie Wsparcia na zagrożonych komputerach i wyślij otrzymane archiwum z informacjami o problemach do wsparcia przedstawiciela Bitdefender.

Aby użyć Narzędzi wsparcia:

1. pobierz Narzędzie wsparcia i prześlij je do zagrożonych komputerów. Aby pobrać narzędzie wsparcia:
 - a. Połącz się z Control Center używając twojego konta.

- b. Naciśnij link **Pomoc i Wsparcie** w prawym dolnym rogu konsoli.
 - c. Linki do pobrania są dostępne w sekcji **Wsparcie**. Dwie wersje są dostępne: jedna dla systemu 32-bit i druga dla systemu 64-bit. Upewnij się, że używasz odpowiedniej wersji gdy uruchamiasz Narzędzie wsparcia na komputerze.
2. Uruchom Narzędzie wsparcia lokalnie na każdym zarażonym komputerze.
- a. Zaznacz pole wyboru oznaczające zgodę, a następnie kliknij „**Dalej**”.
 - b. Wypełnij pola formularza niezbędnymi danymi:
 - i. Wpisz swój adres e-mail.
 - ii. Podaj swoje imię.
 - iii. Z odpowiedniego menu wybierz swój kraj.
 - iv. Opisz problem, który napotkałeś.
 - v. opcjonalnie, możesz spróbować odtworzyć problem przed rozpoczęciem zbierania danych. W tym przypadku, należy postępować w następujący sposób:
 - A. Włącz opcje **Spróbuj odtworzyć problem przed wysłaniem**.
 - B. Kliknij **Dalej**.
 - C. Wybierz rodzaj napotkanego problemu.
 - D. Kliknij **Dalej**.
 - E. Odtwórz problem na swoim komputerze. Kiedy zrobione, wróć do Narzędzi wsparcia i wybierz opcje **Powielanie problemu**.
 - c. Kliknij **Dalej**. Narzędzie pomocy zbiera informacje o produkcie, innych zainstalowanych aplikacjach oraz o konfiguracji systemu (sprzętowej i programowej).
 - d. Poczekaj na zakończenie działania.
 - e. Aby zamknąć to okno, kliknij **Zakończ**. Archiwum plików zostało utworzone na twoim pulpicie.

Wyślij archiwum zip razem z twoją prośbą do wsparcia przedstawiciela Bitdefender używając formularza pomocy technicznej dostępnego na stronie **Pomoc i Wsparcie** w konsoli.

12.4. Informacje o produkcie

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 10 lat Bitdefender uzyskał niekwestionowaną reputację dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiegokolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

12.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com

Centrum pomocy: <http://www.bitdefender.com/support/business.html>

Dokumentacja: documentation@bitdefender.com

Lokalni Dystrybutorzy: <http://www.bitdefender.com/partners>

Program partnerski: partners@bitdefender.com

Rzecznik prasowy: pr@bitdefender.com

Wysyłanie Próbek Wirusów: virus_submission@bitdefender.com

Wysyłanie Próbek Spam: spam_submission@bitdefender.com

Raportowanie Abuse: abuse@bitdefender.com

Strona internetowa: <http://www.fmantivirus.com>

12.4.2. 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

PROFIL TECHNOLOGY

49, Rue de la Vanne

92120 Montrouge

Fax: +33 (0)1 47 35 07 09

Telefon: +33 (0)1 47 35 72 73

Adres e-mail: supportpro@profiltechnology.com

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

Centrum pomocy: <http://www.bitdefender.fr/support/professionnel.html>

Hiszpania

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+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: <http://www.bitdefender.es>
Centrum pomocy: <http://www.bitdefender.es/support/business.html>

Niemcy

Bitdefender GmbH

Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Telefon (biuro i sprzedaż): +49 (0)2301 91 84 222
Telefon (pomoc techniczna): +49 (0)2301 91 84 444
Sprzedaż: vertrieb@bitdefender.de
Strona: <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 (0) 8451-305096
Adres e-mail: info@bitdefender.co.uk
Sprzedaż: sales@bitdefender.co.uk
Strona: <http://www.bitdefender.co.uk>
Centrum pomocy: <http://www.bitdefender.co.uk/support/business.html>

Rumunia

BITDEFENDER SRL

DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax: +40 21 2641799
Telefon (sprzedaż&pomoc techniczna): +40 21 2063470
Sprzedaż: sales@bitdefender.ro

Strona: <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

Fax: 00971-4-44565047

Sprzedaż: sales@bitdefender.com

Internet: <http://www.bitdefender.com/world>

Centrum pomocy: <http://www.bitdefender.com/support/business.html>

A. Aneksy

A.1. Lista Typów Plików Aplikacji

Silnik zwalczający złośliwe oprogramowanie dołączony do programu Bitdefender można skonfigurować tak, aby skanował jedynie pliki aplikacji (lub programów). Pliki aplikacji są bardziej podatne na ataki złośliwego oprogramowania niż inne rodzaje plików.

Ta kategoria zawiera pliki o następujących rozszerzeniach:

386; a6p; ac; accda; accddb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mp; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xls; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.2. Używa zmiennych systemowych

Niektóre z ustawień dostępnych w konsoli wymagają podania ścieżki na komputerach docelowych. Wskazane jest aby używać zmiennych systemowych (w odpowiednich przypadkach), aby upewnić się, że ścieżka jest poprawna dla wszystkich komputerów docelowych.

Oto lista predefiniowanych zmiennych systemowych:

`%ALLUSERSPROFILE%`

Folder profil wszystkich użytkowników. Typowa ścieżka:

`C:\Documents and Settings\All Users`

`%APPDATA%`

folder danych aplikacji zalogowanego użytkownika. Typowa ścieżka:

- **Windows XP:**
C:\Documents and Settings\{username}\Application Data
- **Windows Vista/7:**
C:\Users\{username}\AppData\Roaming

%HOMEPATH%

Foldery użytkownika. Typowa ścieżka:

- **Windows XP:**
\Documents and Settings\{username}
- **Windows Vista/7:**
\Users\{username}

%LOCALAPPDATA%

Tymczasowe pliki Aplikacji. Typowa ścieżka:

C:\Users\{username}\AppData\Local

%PROGRAMFILES%

Folder Program Files. Typowa ścieżka to C:\Program Files.

%PROGRAMFILES(X86)%

Folder Program Files dla 32-bitowej aplikacji (w 64-bitowym systemie). Typowa ścieżka:

C:\Program Files (x86)

%COMMONPROGRAMFILES%

Folder Common Files. Typowa ścieżka:

C:\Program Files\Common Files

%COMMONPROGRAMFILES(X86)%

Folder Common Files dla 32-bitowej aplikacji (w 64-bitowym systemie). Typowa ścieżka:

C:\Program Files (x86)\Common Files

%WINDIR%

Katalog Windows lub SYSROOT. Standardowa ścieżka to C:\Windows.

Słownik

Adware

Adware jest często łączony z aplikacją, która może być używana bezpłatnie tak długo, jak użytkownik zgadza się na adware. Ponieważ aplikacje typu adware są zazwyczaj instalowane po zaakceptowaniu przez użytkownika warunków umowy licencyjnej określającej cele aplikacji, zadanie ochrony przed takim adware nie jest wykonywane.

Jednak reklamy typu pop-up mogą być irytujące, a w niektórych wypadkach mogą obniżyć wydajność systemu. Ponadto informacje zbierane przez niektóre aplikacje tego typu mogą rodzić obawę naruszenia prywatności użytkowników, którzy nie byli w pełni świadomi warunków umowy licencyjnej.

Aktualizacja

Nowa wersja oprogramowania lub sprzętu przeznaczona do zastąpienia starszej wersji tego samego produktu. Dodatkowo standardowe procedury instalacyjne dla aktualizacji często sprawdzają, czy na komputerze zainstalowana jest starsza wersja produktu; jeśli nie, nie możesz zainstalować aktualizacji.

Bitdefender posiada własny moduł uaktualnienia, który pozwala tobie manualnie wprowadzać uaktualnienia lub przeprowadzać to automatycznie.

Archiwum

Dysk, taśma, lub katalog, który zawiera pliki kopii zapasowej.

Plik, który zawiera jeden lub więcej plików w skompresowanym formacie.

Backdoor

Luka w obszarze bezpieczeństwa systemu celowo pozostawiona przez projektantów lub opiekunów systemu. Luki nie zawsze są pozostawione w złej wierze. Niektóre systemy operacyjne są dostarczane z kontami uprzywilejowanymi przeznaczonymi do użytku przez serwis techniczny lub opiekunów ds. programowania po stronie sprzedawcy.

Ciasteczka

W przemyśle internetowym cookie są określane jako małe pliki zawierające informacje o poszczególnych komputerach, które mogą być analizowane i wykorzystywane przez reklamodawców, aby śledzić online Twoje zainteresowania i gusta. W tej dziedzinie technologia związana z plikami cookie nadal się rozwija, a celem tego jest profilowanie reklam tak, by były bezpośrednio związane z Twoimi zainteresowaniami. Z jednej strony dla wielu ludzi stanowi to obosieczny miecz: jest efektywne i trwałe, gdyż wyświetlane są tylko reklamy na interesujący Cię temat. Z drugiej strony śledzi każdy Twój ruch oraz

kliknięcie. Dlatego są one tematem publicznej dyskusji w kwestii prywatności. Wiele osób czuje się obrażonymi z powodu bycia obserwowanymi jako "Numer SKU" (kod kreskowy na opakowaniu, który jest skanowany przez sklepy przy zakupach). Mimo że ten ten punkt widzenia może się wydawać ekstremalny, w niektórych przypadkach ma swoje uzasadnienie.

Fałszywy alarm

Pojawia się, kiedy skaner identyfikuje plik jako zainfekowany, gdy w rzeczywistości nie jest zainfekowany.

Heurystyczny

Oparta na regułach metoda rozpoznawania nowych wirusów. Ta metoda skanowania nie polega na określonych sygnaturach wirusów. Zaletą skanowania heurystycznego jest to, że nie jest ono podatne na zmylenie przez nowy wariant znanych wirusów. Jednakże może czasami zgłaszać wykrycie podejrzanego kodu w normalnych programach generując tzw. "fałszywie alarmy".

IP

Protokół internetowy – protokół routingu w protokole TCP/IP który jest odpowiedzialny za adresowanie IP, fragmentację oraz ponowne składanie pakietów IP.

Keylogger

Keyloggery to aplikacje, które zapisują wszystkie naciśnięcia klawiszy.

Keyloggery nie są szkodliwe z założenia. Można ich używać dla celów zgodnych z prawem, np. po to, żeby legalnie monitorować aktywność pracowników lub dzieci. Jednak cyberprzestępcy coraz częściej używają ich w celu wyrządzenia szkody (np. do zbierania prywatnych danych, takich jak dane do logowania lub numer ubezpieczenia społecznego).

Makro wirus

Typ wirusa komputerowego, który jest zakodowany jako makro w danym dokumencie. Wiele aplikacji jak np. Microsoft Word i Excel wspiera makra.

Aplikacje te pozwalają Ci umiejscowić makro w dokumencie i wykonywać je za każdym razem, kiedy dokument jest otwierany.

Nie-heurystyczny

Ta metoda skanowania opiera się na określonych sygnaturach wirusów. Zaletą skanowania nieheurystycznego jest to, że nie jest ono podatne na wprowadzanie błąd przez obiekty wydające się być wirusem, a także nie generuje fałszywych alarmów.

Oprogramowanie szpiegujące (spyware)

Każde oprogramowanie, które zbiera dane o użytkowniku podczas połączenia z internetem bez jego wiedzy, zazwyczaj w celach reklamowych. Aplikacje spyware występują zazwyczaj jako ukryte komponenty programów freeware albo shareware,

które mogą być pobrane z internetu. Jednakże należy pamiętać że większość aplikacji shareware oraz freeware nie ma w sobie żadnego spyware. Po zainstalowaniu, spyware monitoruje aktywność użytkownika w internecie i przesyła informacje w tle do kogoś innego. Spyware może także zbierać informacje o adresach e-mail, a nawet hasła i numery kart kredytowych.

Spyware jest prostym programem podobnym do konia trojańskiego, którego użytkownicy instalują nieświadomie podczas instalacji innego programu. Pospolitym sposobem by zostać ofiarą spyware jest pobranie niektórych z obecnie dostępnych programów współdzielonych w sieciach typu peer-to-peer.

Abstrahując od kwestii etyki i prywatności, spyware okrada użytkownika używając pamięci komputera i także zużywając przepustowość łącza internetowego podczas wysyłania informacji z powrotem do swojej bazy drogą internetową. Ponieważ spyware zużywa pamięć i zasobów systemowych, aplikacje pracujące w tle mogą powodować zawieszenie się systemu lub jego ogólną niestabilność.

Phishing

Wysyłanie wiadomości e-mail do użytkownika przez osobę podającą się za przedstawiciela uprawnionego do tego przedsięwzięcia, będące próbą skłonienia użytkownika do podania informacji poufnych, wykorzystywanych w akcie kradzieży tożsamości. E-mail przekierowuje użytkownika na stronę internetową gdzie jest on proszony o zaktualizowanie informacji osobistych np. haseł, informacji dotyczących kart kredytowych, ubezpieczenia socjalnego i nr konta bankowego, które uprawniona organizacja już posiada. Strona internetowa jest fałszywa i umieszczona w internecie tylko po to, żeby wykraść informacje o użytkowniku.

Plik raportu

Plik, który zapisuje zaistniałe akcje. Bitdefender utrzymuje plik raportu udostępniając skanowaną ścieżkę dostępu, foldery, ilość archiwów i skanowanych plików, ilość zainfekowanych i podejrzanych plików jakie zostały znalezione.

Port

Interfejs komputera, do którego podłączasz urządzenie. Komputery osobiste mają różne rodzaje portów. Wewnątrz znajduje się kilka portów dla połączeń dyskowych, podłączania monitorów i klawiatur. Na zewnątrz komputery osobiste mają porty dla połączeń modemowych, drukarek, myszy i innych urządzeń peryferyjnych.

Natomiast w sieciach TCP/IP i UDP jest to punkt końcowy połączenia logicznego. Numer portu pokazuje, jakiego typu jest dany port. Np. port 80 jest używany dla ruchu HTTP.

Przeglądarka

Aplikacja używana do lokalizowania i wyświetlania stron internetowych. Dwoma najpopularniejszymi przeglądarkami są: Netscape Navigator i Microsoft Internet Explorer. Są graficznymi przeglądarkami, co oznacza, że mogą pokazywać grafikę oraz tekst. W dodatku większość nowoczesnych przeglądarek może pokazywać informacje

multimedialne wraz z dźwiękiem i obrazem video, jednak wymagają one wtyczek dla niektórych formatów.

Robak

Program, który propaguje się przez sieć mnożąc się w czasie poruszania. Nie może się podłączyć do innych programów.

Rootkit

Rootkit jest zestawem narzędzi programowych, który daje dostęp do systemu na poziomie administratora. Termin ten był początkowo używany dla systemów operacyjnych UNIX w odniesieniu do zrekompilowanych narzędzi, które udostępniały intruzom prawa administracyjne, pozwalając im ukryć ich obecność, żeby nie byli widoczni dla administratorów systemu.

Głównym zadaniem rootkitów jest ukrywanie procesów, plików, zdarzeń logowania i raportów. Mogą również przechwytywać dane z terminali, połączeń sieciowych lub urządzeń peryferyjnych, jeśli zawierają odpowiedni rodzaj oprogramowania.

Rootkity nie są zagrożeniem z założenia. Na przykład systemy, a nawet niektóre aplikacje ukrywają krytyczne pliki używające rootkitów. Jednak często są one używane do ukrywania złośliwego oprogramowania lub intruza w systemie. Gdy są połączone z wirusami, są wielkim zagrożeniem dla spójności działania i bezpieczeństwa systemu. Mogą monitorować ruch, tworzyć backdoory w systemie, zmieniać pliki i logi oraz unikać wykrycia.

Rozszerzenie pliku

Część nazwy pliku, która wskazuje na rodzaj danych przechowywanych w pliku.

Wiele systemów operacyjnych, np. Unix, VMS, i MS-DOS, używa rozszerzeń nazwy pliku. Zwykle składają się z jednego do trzech znaków (niektóre stare systemy operacyjne akceptują nie więcej niż trzy). Przykłady obejmują „c” jako kod źródłowy C, „ps” jako PostScript, „txt” jako tekst.

Sektor rozruchowy

Sektor na początku każdego dysku, który rozpoznaje budowę dysku (rozmiar sektora, rozmiar klastra itd.). Sektor rozruchowy zawiera również program uruchamiający system operacyjny.

Skrypt

Inna nazwa dla makr; skrypt jest listą komend, które mogą być wykonywane bez udziału użytkownika.

Spam

Elektroniczne śmieci lub komentarze grup dyskusyjnych. Ogólnie znane jako niechciane wiadomości e-mail.

Sygnatura malware

Sygnatury złośliwego oprogramowania to urywki kodu wypakowane z rzeczywistych próbek tego oprogramowania. Są one używane przez programy antywirusowe do dopasowywania wzorców i wykrywania złośliwego oprogramowania. Sygnatury są również użyte do usunięcia kodu malware z zainfekowanych plików.

Baza Danych Sygnatur Złośliwego Oprogramowania Bitdefender to zbiór sygnatur złośliwego oprogramowania uaktualniany co godzinę przez naukowców Bitdefender, zajmujących się złośliwym oprogramowaniem.

Szkodliwe oprogramowanie

Malware to ogólne określenie oprogramowania, które zostało stworzone do uszkodzenia za pomocą "złośliwego oprogramowania". Nie jest jeszcze w powszechnym użyciu, ale jego popularność jako główny produkt do określenia wirusów, koni trojańskich, robaków, i złośliwych kodów mobilnych rośnie.

TCP/IP

Protokół Kontroli Transmisji/Protokół internetowy – Zespół protokołów sieciowych szeroko używanych w internecie, zapewniający komunikację pomiędzy połączonymi sieciami komputerów z różną architekturą sprzętową i różnymi systemami operacyjnymi. TCP/IP zawierają standardy dotyczące komunikacji komputerów oraz połączeń sieciowych i ruchu.

Trojan

Niszczycielski program, który ukrywa się jako niegroźna aplikacja. W przeciwieństwie do wirusów, konie trojańskie nie powielają się, ale mogą być tak samo szkodliwe. Jednym z najmniejbezpiecznych typów koni trojańskich jest program zapewniający, że pozbędzie się wirusów z Twojego komputera, a który w rzeczywistości wprowadza wirusy do komputera.

Nazwa pochodzi z powieści Homera "Iliada", w której Grecy podarowali olbrzymiego konia swoim wrogom, Trojanom, pozornie jako znak pokoju. Gdy jednak Trojanie wprowadzili konia do miasta, greccy żołnierze wymknęli się z pustego wnętrza konia i otworzyli bramy miasta pozwalając pozostałym na wejście i podbicie Troi.

Wiersz poleceń

W interfejsie linii poleceń użytkownik wpisuje polecenia w przestrzeni znajdującej się na ekranie, używając języka poleceń.

Wirus

Program lub fragment kodu, który jest załadowany na Twoim komputerze bez Twojej wiedzy i uruchamia się wbrew Twojej woli. Większość wirusów może się również replikować. Wszystkie wirusy komputerowe są tworzone przez człowieka. Prosty wirus, który umie się skopiować kilka razy jest stosunkowo łatwy do utworzenia. Nawet tak prosty wirus jest niebezpieczny, ponieważ szybko wykorzysta całą dostępną pamięć i

przyczyni się do zatrzymania pracy systemu. Bardziej niebezpiecznym typem wirusa jest ten, który jest zdolny przenosić się przez sieci i łamać systemy bezpieczeństwa.

Wirus polimorficzny

Wirus, który zmienia swoją formę za każdym razem, kiedy zainfekuje kolejny plik. Ponieważ nie mają one stałego wzoru binarnego, są trudne do rozpoznania.

Wirus sektora rozruchowego

Wirus, który infekuje boot sektor dysku stałego lub stację dyskietek. Próba uruchomienia systemu z dyskietki zainfekowanej wirusem tego typu spowoduje, że wirus uaktywni się w pamięci. Od tego momentu za każdym razem, kiedy będziesz uruchamiał system, wirus będzie aktywny w pamięci.

Zasobnik systemowy

Wprowadzony w systemie Windows 95 zasobnik systemowy znajduje się na pasku zadań Windows (zwykle u dołu obok zegara) i zawiera miniaturowe ikony zapewniające łatwy dostęp do funkcji systemowych, takich jak faks, drukarka, modem, głośność i nie tylko. Aby wyświetlić informacje szczegółowe i sterowniki, kliknij dwukrotnie ikonę lub kliknij ją prawym przyciskiem myszy.

Zdarzenia

Działanie lub wydarzenie wykryte przez program. Zdarzenia mogą być czynnościami użytkownika takimi jak: kliknięcie myszą lub naciśnięcie klawisza albo zdarzeniami systemowymi takimi, jak kończenie się pamięci.