

Bitdefender® ENTERPRISE

BITDEFENDER SMALL OFFICE SECURITY

Przewodnik Raportującego



Bitdefender Small Office Security

Przewodnik Raportującego

Data publikacji 2014.12.18

Copyright© 2014 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.

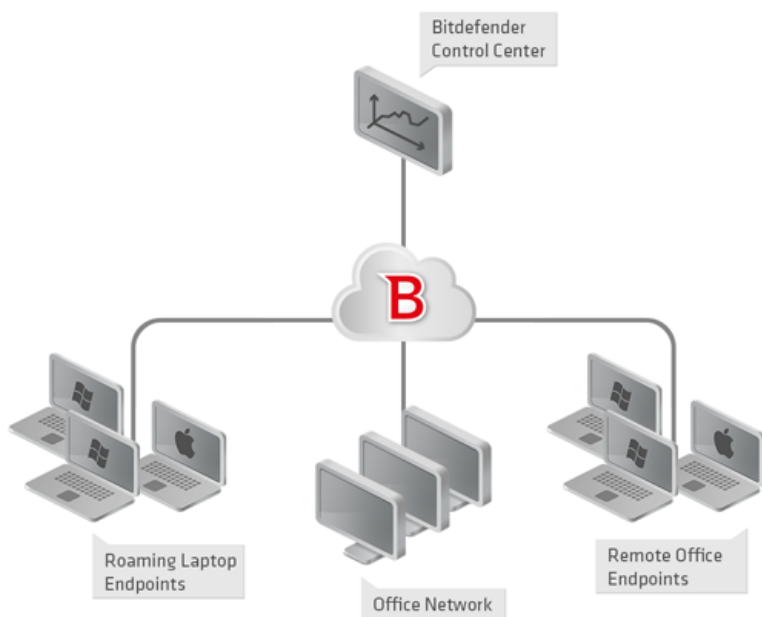


Spis treści

1. O Small Office Security	1
2. Pierwsze Kroki	3
2.1. Łączenie z Control Center	3
2.2. Control Center w skrócie	3
2.2.1. Tabela Danych	5
2.2.2. Paski narzędzi działań	6
2.2.3. Menu Kontekstowe	6
2.3. Zmiana hasła logowania	7
2.4. Zarządzanie kontem	7
3. Monitorowanie Panelu	9
3.1. Odświeżanie Danych Portletów	10
3.2. Edytowanie ustawień portletów	10
3.3. Dodawanie nowego portletu	10
3.4. usuwanie Portletu	11
3.5. Zmiana Układu Portletów	12
4. Powiadomienia	13
4.1. Rodzaje powiadomień	13
4.2. Zobacz powiadomienia	14
4.3. Usuwanie powiadomień	16
4.4. Konfiguracja ustawień powiadomień	16
5. Używanie raportów	19
5.1. Dostępne rodzaje raportów	19
5.2. Tworzenie raportów	22
5.3. Przeglądania i zarządzanie zaplanowanych raportów	24
5.3.1. Przeglądanie raportów	25
5.3.2. Edytowanie zaplanowanego raportu.	26
5.3.3. Usuwanie zaplanowanych raportów	27
5.4. Zapisywanie raportów	27
5.4.1. Eksportowanie raportów	27
5.4.2. Raporty pobierania	28
5.5. Raporty E-mailów	28
5.6. Drukowanie raportów	29
6. Dziennik Aktywności Użytkownika	30
7. Otrzymywanie pomocy	32
Słownik	33

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

Bitdefender Rozwiązania 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”.

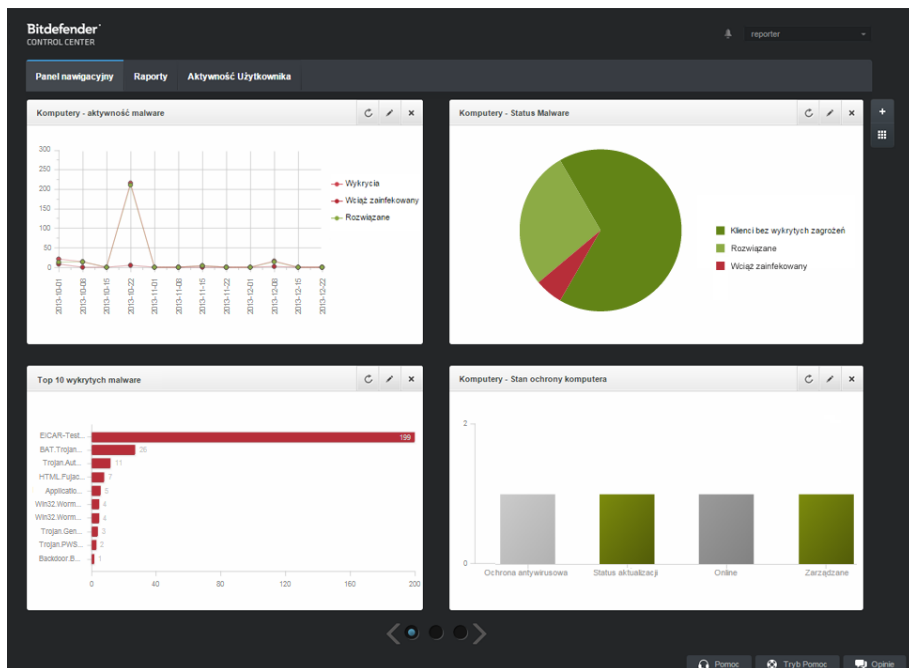


Notatka

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.



Panel

Reportery mają dostęp do poniższych sekcji w menu.

Panel nawigacyjny


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

Raporty

Pobierz raporty bezpieczeństwa dotyczące zarządzania klientami.

Aktywność Użytkownika

Sprawdź dziennik aktywności użytkownika.

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.
- **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.

2.2.1. Tabela Danych

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

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

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 nagłówek.

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

Sortowanie danych

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

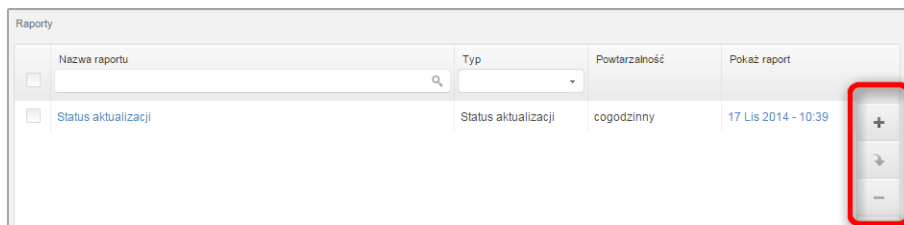
Odświeżanie Danych Tabele

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

2.2.2. 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.

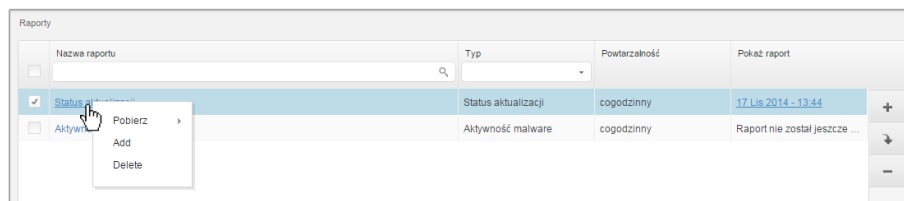


	Nazwa raportu	Typ	Powtarzalność	Pokaż raport
<input type="checkbox"/>	Status aktualizacji	Status aktualizacji	cogodzinny	17 Lis 2014 - 10:39

Strona raportów - Paski Narzędzi działań

2.2.3. 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.



	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. Zmiana hasła logowania

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

Zaleca się, aby wykonać następujące czynności:

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

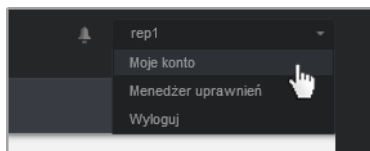
Aby zmienić hasło logowania:

1. 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.

2.4. 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 aktualizuj 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 wygasa.** Wybierz czas nieaktywności sesji zanim wygaśnie.
4. Naciśnij **Zapisz** aby zastosować zmiany.



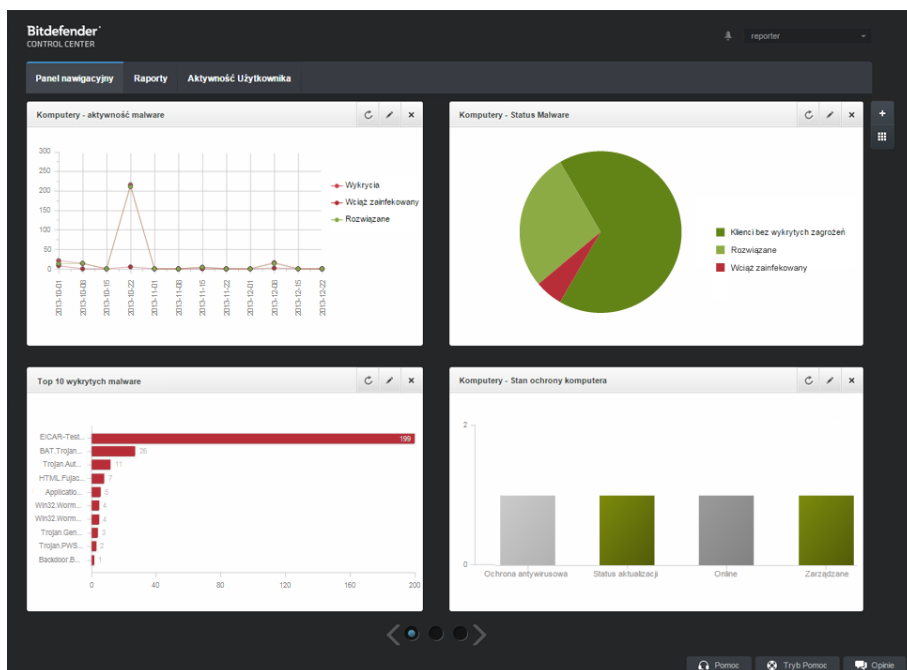
Notatka

Nie możesz usunąć swojego własnego konta.

3. 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. 19)


- 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, **dodać** dodatkowe portlety, **usuń** lub **zmień pozycję** istniejących portletów.

3.1. Odświeżanie Danych Portletów

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


3.2. 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.

3.3. 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. 19)


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

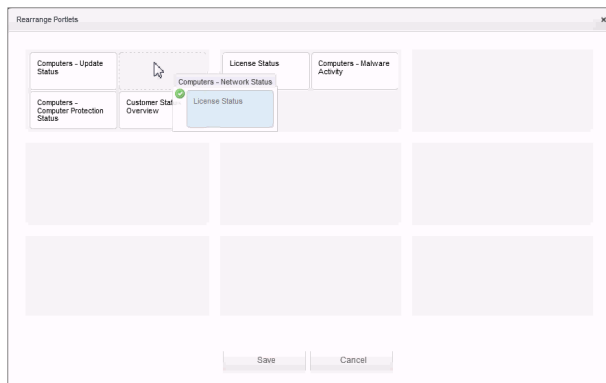
3.4. usuwanie Portletu

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.

3.5. Zmiana Układu Portletów

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

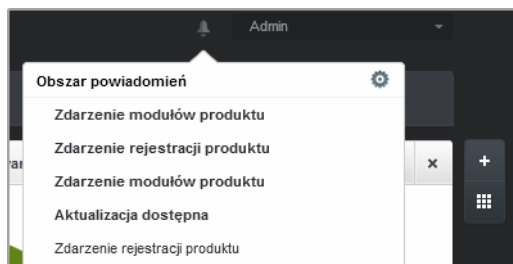
1. Przejdź do strony **Panel**.
2. Naciśnij przycisk  **Zmiana układu portletów** po prawej stronie panelu. Okno mapy portletów jest widoczne.
3. Przeciągnij i upuść portlet do żądanej pozycji.
4. Kliknij **Zapisz**.




Zmiana układu portletów w panelu

4. Powiadomienia

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

4.1. 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. 16).

Licencja wygasa

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

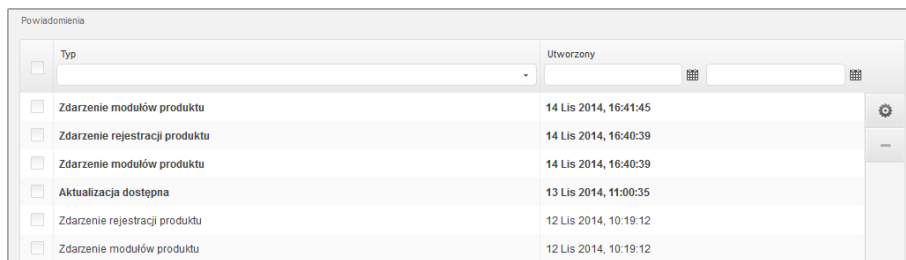
To powiadomienie jest wysyłane za każdym razem jak moduł bezpieczeństwa na zainstalowanym agencie zostanie zablokowany.

Zdarzenie rejestracji produktu

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

4.2. Zobacz powiadomienia

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

4.3. 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. 16).

4.4. 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. 13). 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**.

5. 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).

5.1. 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.

Using the available filters, you can easily find out which clients have updated or have not updated in the last 24 hours.

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.

5.2. 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. 19).
- 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 (godzinie 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**

5.3. Przeglądania i zarządzanie zaplanowanych raportów

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

Panel nawigacyjny			
Raporty		Aktywność Użytkownika	
Raporty			
<input type="checkbox"/>	Nazwa raportu <input type="text"/>	Typ <input type="text"/>	Powtarzalność <input type="text"/>
<input type="checkbox"/>	Rap1	Top 10 zainfekowanych komputerów	Miesięcznie
<input type="checkbox"/>	Rap2	Top 10 wykrytych malware	Miesięcznie
<input type="checkbox"/>	Rap3	Status aktualizacji	Codziennie
			Pokaż raport
			Raport nie został jeszcze wygenerowany
			Raport nie został jeszcze wygenerowany
			09 Gru 2014 - 00:00
Strona 1 z 1 10 3 elementów			

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.

5.3.1. 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.

5.3.2. 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.

5.3.3. 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.

5.4. 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.

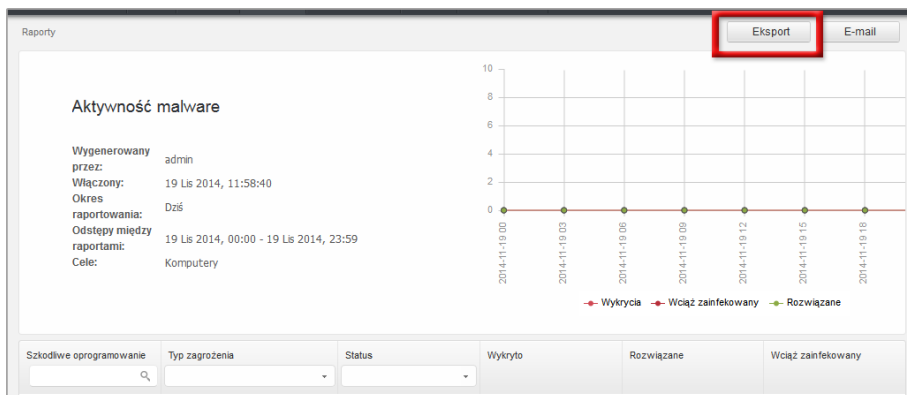
Masz dwie możliwości zapisywania raportów:

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

5.4.1. Eksportowanie raportów

Aby wyeksportować raport do twojego komputera:

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



Raporty - Opcje eksportu

2. Wybierz odpowiedni format raportu:


- Przenośny Format Dokumentu (PDF) lub
- Wartości oddzielone przecinkami (CSV)

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

5.4.2. Raporty pobierania

Archiwum Raport zawiera zarówno podsumowanie raportów i szczegółowych raportów.

Aby pobrać archiwum raportu:

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

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

5.5. Raporty E-mailów

Możesz wysłać raporty na e-mail używając poniższych opcji:

1. 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.

5.6. Drukowanie raportów

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

6. 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

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

Użytkownik	Rola	Akcja	Obszar	Cel	Utworzony
------------	------	-------	--------	-----	-----------


Strona aktywności użytkownika

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

Kolumny tabeli dostarczają przydatnych informacji na temat wymienionych wydarzeń:

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

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

Aby zobaczyć szczegółowe informacje o wydarzeniu, wybierz je i sprawdź sekcje pod tabelą. Aby upewnić się, że ostatnie informacje się wyświetlają naciśnij przycisk  **Odśwież** w lewym dolnym rogu tabeli.

7. Otrzymywanie pomocy

Dla każdego problemu lub pytania związanego z Control Center, skontaktuj się z administratorem.

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 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 błęd 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.