SOPHOS

Cybersecurity made simple.

Sophos Endpoint dla Windows

Pomoc

Spis treści

1 Sophos Endpoint dla Windows — informacje

Ten plik pomocy zawiera informacje o programie Sophos Endpoint dla Windows oraz szczegółowe omówienie procedur.

2 Sophos Endpoint

Aplikacja Sophos Endpoint jest uruchomiona na chronionych komputerach i serwerach.

Ograniczenie
Możliwe, że nie masz dostępu do niektórych opisanych tutaj funkcji. Zależy to od posiadanej licencji.

Aplikacja Sophos Endpoint jest konfigurowana i zarządzana centralnie z poziomu konsoli Sophos Central Admin.

Pewne zadania można jednak wykonywać na komputerze lub serwerze:

- Sprawdzanie stanu komputera.
- Skanowanie pliku, komputera lub serwer lub wyszukiwanie zagrożeń.
- Przeglądanie szczegółów zdarzeń na komputerze lub serwerze, takich jak na przykład informacje o wykrytych zagrożeniach.
- Czyszczenie zagrożeń.
- Zmiana ustawień zabezpieczeń. Możesz na przykład wyłączyć niektóre funkcje w celu rozwiązania problemów.
- Aktualizowanie.
- Rozwiązywanie problemów.

Uwaga
Aby wyczyścić zagrożenia lub zmienić ustawienia, musisz użyć opcji **Logowanie** i wprowadzić hasło ochrony przed naruszeniami.

Informacje pokrewne

Pojęcia pokrewne

Stan na stronie 4
Użytkownik może sprawdzić stan zabezpieczeń i przeskanować komputer lub serwer.

Zdarzenia na stronie 6
Na stronie **Zdarzenia** znajdują się zdarzenia z komputera lub serwera, na przykład zdarzenie wykrycia zagrożenia.

Zadania pokrewne

Skanowanie plików na stronie 10
Użytkownik może skanować poszczególne pliki.

Skanowanie komputera lub serwera na stronie 10
Aby przeskanować komputer lub serwer, postępuj zgodnie z instrukcjami podanymi poniżej.

Czyszczenie zagrożeń na stronie 10
Aby usunąć wykryte zagrożenia, należy postępować zgodnie z instrukcjami podanymi poniżej.

Zmiana ustawień zabezpieczeń na stronie 10
Aby zmienić ustawienia zabezpieczeń, postępuj zgodnie z instrukcjami podanymi poniżej.

Aktualizuj teraz na stronie 11
Aby zaktualizować definicje wirusów, należy postępować zgodnie z poniższymi instrukcjami.

Rozwiązywanie problemów na stronie 11
W celu rozwiązania problemów należy postępować zgodnie z poniższymi instrukcjami.

3 Stan

Użytkownik może sprawdzić stan zabezpieczeń i przeskanować komputer lub serwer.

Ograniczenie
Możliwe, że nie masz dostępu do niektórych opisanych tutaj funkcji. Zależy to od posiadanej licencji.

Strona **Stan** pozwala:

- Obserwować stan bezpieczeństwa komputera lub serwera.
- Skanować komputer lub serwer w poszukiwaniu zagrożeń.
- Zobacz zainstalowane funkcje i stan ich zabezpieczeń.

Uwaga
Łącze **Informacje** w dolnym prawym rogu strony pozwala zaktualizować definicje wirusów lub rozwiązać ewentualne problemy z produktem.

Stan bezpieczeństwa

O stanie bezpieczeństwa informuje ikona w górnej części strony.

Ustawienie	Opis
 Zielona.	Nie ma żadnych alertów albo występują wyłącznie alerty o niskim priorytecie.
 Czerwona.	Występują alerty o wysokim priorytecie.
 Żółty.	Występują alerty o średnim priorytecie.
 Szara.	Stan jest nieznany.

Poniżej wyświetlane są wszystkie zainstalowane funkcje wraz z ich indywidualnym stanem zabezpieczeń.

Skanowanie komputera

Kliknij opcję **Skanuj**, aby przeskanować wszystkie pliki na komputerze lub serwerze w poszukiwaniu zagrożeń.

Po zakończeniu skanowania zostanie wyświetlone podsumowanie wyników skanowania. Jeśli zostały wykryte zagrożenia, możesz przejść na stronę **Zdarzenia**, aby zobaczyć szczegółowe informacje.

4 Zdarzenia

Na stronie **Zdarzenia** znajdują się zdarzenia z komputera lub serwera, na przykład zdarzenie wykrycia zagrożenia.

Ograniczenie
Możliwe, że nie masz dostępu do niektórych opisanych tutaj funkcji. Zależy to od posiadanej licencji.

Zdarzenia można filtrować, aby na przykład wyświetlić tyko te, które wymagają podjęcia działania. Można również szukać konkretnych typów zdarzeń.

Lista Zdarzenia

Informacje widoczne na liście:

- Istotność. Skrajna ikona z lewej strony listy informuje, czy zdarzenie ma wysoki priorytet, średni priorytet czy status powiadomienia.
- Źródło. Ikona z lewej strony listy informuje, która funkcja Sophos zgłosiła zdarzenie.
- Data i godzina wystąpienia zdarzenia.
- Opis zdarzenia.
- Łącze umożliwiające podjęcie działania (jeśli jest wymagane jakiekolwiek działanie). Ta informacja jest widoczna tylko wtedy, gdy użytkownik jest zalogowany jako administrator.

Aby wyświetlić szczegóły każdego zdarzenia, kliknij strzałkę po prawej stronie, aby je rozwinąć.

Działania, które można wykonać, są takie same, jak te dostępne w konsoli Sophos Central Admin. Patrz lista na stronie **Alarmy** w Sophos Central Admin pomoc.

Zdarzenia można filtrować według następujących typów:

Typ zdarzenia	Opis
Malware i PUA	Złośliwe oprogramowanie to ogólny termin określający oprogramowanie o złośliwym działaniu. Obejmuje wirusy, robaki, konie trojańskie oraz oprogramowanie szpiegujące. Potencjalnie niechciane aplikacje (PUA) to programy, które nie są złośliwe, takie jak dialery, zdalne narzędzia administracyjne i narzędzia do hakowania, ale ogólnie są uznawane za nieodpowiednie dla większości sieci firmowych.

Typ zdarzenia	Opis
Zagrożenia sieciowe	Zagrożenia sieciowe obejmują złośliwe witryny internetowe, witryny bez przypisanej kategorii oraz ryzykowne treści dostępne do pobrania. Niektóre witryny internetowe są zwykle uważane za nieodpowiednie dla sieci firmowych, na przykład witryny dla dorosłych czy portale społecznościowe. Można je zablokować.
Szkodliwe zachowanie	Szkodliwe zachowanie to podejrzane zachowanie wykryte w oprogramowaniu uruchomionym obecnie na komputerze lub serwerze. Oprogramowanie ransomware to złośliwe oprogramowanie, które blokuje dostęp do plików i domaga się zapłaty okupu.
Kontrolowane elementy	Kategoria ta obejmuje: • Aplikacje, które nie stanowią zagrożenia bezpieczeństwa, ale które według użytkownika nie nadają się do użytku firmowego • Urządzenia peryferyjne i nośniki wymienne • Ryzykowne treści do pobrania oraz witryny internetowe, które są nieodpowiednie w środowisku firmowym • Pliki zawierające wrażliwe informacje (na przykład dane osobowe lub finansowe), które powinny pozostać w firmie
Szkodliwy ruch	Szkodliwy ruch to ruch między komputerami, który wskazuje na potencjalną próbę przejęcia kontroli nad komputerem lub serwerem (atak typu „command and control”).
Programy wykorzystujące luki	Programy wykorzystujące luki, którym mogą zapobiec produkty Sophos, obejmują programy przejmujące kontrolę nad aplikacjami oraz programy wykorzystujące luki w przeglądarkach, wtyczkach przeglądarek, aplikacjach Java, aplikacjach multimedialnych i aplikacjach pakietu Microsoft Office.

5 Ustawienia

Możesz tymczasowo zmienić ustawienia bezpieczeństwa na bieżącym komputerze lub serwerze.

Może to być potrzebne podczas rozwiązywania problemów. Możesz na przykład wyłączyć jedną z funkcji, aby sprawdzić, czy nie wywołuje ona problemów z komputerem.

Ograniczenie
Możliwe, że nie masz dostępu do niektórych opisanych tutaj funkcji. Zależy to od posiadanej licencji.

Ograniczenie
Strona **Ustawienia** jest dostępna wyłącznie po uprzednim wprowadzeniu hasła ochrony przed naruszeniami (dostępne u administratora platformy Sophos Central).

Zmiana ustawień

Zaznacz pole wyboru **Pomijaj zasadę Sophos Central przez 4 godziny w celu rozwiązania problemu**.

Teraz możesz zmienić ustawienia na tej stronie. Wprowadzone zmiany tymczasowo zastąpią ustawienia zasady, która została wdrożona przez Ciebie (lub innego administratora) z poziomu konsoli Sophos Central Admin.

Po czterech godzinach ustawienia automatycznie zmienią się z powrotem na ustawienia zasady wymuszane centralnie.

W razie potrzeby możesz później ponownie zmienić ustawienia. Aby zrobić to dla poszczególnych funkcji, nie możesz korzystać z suwaków. Zamiast tego, wyłącz opcję **Pomijaj zasadę Sophos Central przez 4 godziny w celu rozwiązania problemu**.

Uczenie głębokie

Uczenie głębokie wykrywa zagrożenia, wykorzystując zaawansowane uczenie maszynowe. Może identyfikować złośliwe oprogramowanie i potencjalnie niechciane aplikacje bez wykorzystywania żadnych sygnatur.

Skanowanie w czasie rzeczywistym

Skanowanie w czasie rzeczywistym skanuje elementy w momencie, gdy użytkownik próbuje uzyskać do nich dostęp. Zezwala na dostęp tylko wtedy, gdy stwierdzi, że nie stanowią one zagrożenia. Możliwe opcje:

- **Pliki**: Ta funkcja skanuje lokalne pliki i dane udostępnione w sieci (jeśli zdefiniowano tak w zasadzie).
- **Internet**: Ta funkcja skanuje zasoby internetowe. Może skanować pobierane pliki, blokować dostęp do złośliwych witryn internetowych oraz wykrywać witryny o niskiej reputacji.

Kontrola użytkowników

- Funkcja **Kontrola urządzeń peryferyjnych** pozwala kontrolować dostęp do urządzeń peryferyjnych i nośników wymiennych.
- Funkcja **Kontrola aplikacji** pozwala wykrywać i blokować aplikacje, które nie stanowią zagrożenia bezpieczeństwa, ale które według użytkownika nie nadają się do użytku firmowego.
- Funkcja **Kontrola sieci** chroni przed pobieraniem ryzykownych treści, decyduje, które witryny mogą odwiedzać użytkownicy, oraz zapobiega utracie danych.
- Funkcja **Zapobieganie utracie danych** pozwala monitorować i ograniczać transfer plików zawierających wrażliwe dane.
- **Ochrona przed naruszeniami** umożliwia ograniczenie zmian. Jeśli opcja ta jest włączona, administrator lokalny potrzebuje hasła, aby zmienić ustawienia zabezpieczeń lub odinstalować Sophos Endpoint.

Ochrona środowiska wykonawczego

Funkcja ochrony środowiska wykonawczego chroni przed zagrożeniami poprzez wykrywanie podejrzanego i złośliwego zachowania lub ruchu na komputerach końcowych. Możliwe opcje:

- **Wykrywanie oprogramowania ransomware**: Ta funkcja chroni przed złośliwym oprogramowaniem, które ogranicza dostęp do plików, a następnie wymaga okupu w celu przywrócenia dostępu.
- **Bezpieczne przeglądanie**: Ta funkcja chroni przeglądarki internetowe przed atakami ze strony złośliwego oprogramowania.
- **Unikanie programów wykorzystujących luki**: Ta funkcja chroni aplikacje najbardziej narażone na ataki złośliwego oprogramowania, takie jak aplikacje Java.
- **Ochrona przed zagrożeniami sieciowymi**: Ta funkcja wykrywa ruch między komputerem końcowym i serwerem, który może wskazywać na próbę przejęcia kontroli nad komputerem. Obejmuje ona kontrolę pakietów, która polega na skanowaniu komunikacji w sieci, identyfikowaniu i blokowaniu zagrożeń, zanim zdołają uszkodzić system operacyjny lub aplikacje.

  Uwaga
  Wyłączenie funkcji **Ochrona przed zagrożeniami sieciowymi** spowoduje wyłączenie funkcji EDR, izolowania oraz blokowania komunikacji.

- **Wykrywanie szkodliwych zachowań**: Ta funkcja wykrywa i blokuje zachowanie, które jest uważane za złośliwe lub podejrzane.

Kontrola komputera

Można monitorować Zaporę systemu Windows (albo inną zarejestrowaną zaporę) na używanych komputerach i serwerach.

6 Jak to zrobić...?

6.1 Skanowanie plików

Użytkownik może skanować poszczególne pliki.

Aby przeskanować plik, wykonaj następujące czynności:

- W Eksploratorze plików kliknij plik prawym przyciskiem myszy i wybierz opcje **Skanuj**.

6.2 Skanowanie komputera lub serwera

Aby przeskanować komputer lub serwer, postępuj zgodnie z instrukcjami podanymi poniżej.

Aby przeskanować wszystkie pliki na komputerze lub serwerze:

1. Przejdź do strony **Status** lub **Wykrycia**.
2. Kliknij przycisk **Skanuj**.
   Po zakończeniu skanowania zostanie wyświetlone podsumowanie wyników skanowania.
3. Jeśli zostały wykryte zagrożenia, możesz przejść na stronę **Zdarzenia**, aby zobaczyć szczegółowe informacje.

6.3 Czyszczenie zagrożeń

Aby usunąć wykryte zagrożenia, należy postępować zgodnie z instrukcjami podanymi poniżej.

Aby usunąć zagrożenie, wykonaj następujące czynności:

1. Kliknij opcję **Logowanie administratora** i wprowadź hasło ochrony przed naruszeniami (dostępne u administratora platformy Sophos Central).
2. Przejdź na stronę **Zdarzenia**, aby wyświetlić szczegóły wykrytego zagrożenia.
3. Znajdź łącze działania obok szczegółów zagrożenia.

Działania możliwe do wykonania są takie same jak w konsoli Sophos Central Admin. Zobacz listę na stronie **Alerty** w sekcji pomoc Sophos Central Admin.

6.4 Zmiana ustawień zabezpieczeń

Aby zmienić ustawienia zabezpieczeń, postępuj zgodnie z instrukcjami podanymi poniżej.

Aby zmienić ustawienia zabezpieczeń:

1. Kliknij opcję **Logowanie** w prawym górnym rogu interfejsu.
2. Wprowadź hasło ochrony przed naruszeniami (dostępne u administratora platformy Sophos Central).
   Teraz na pasku menu znajduje się pozycja **Ustawienia**.
3. Przejdź na stronę **Ustawienia**.

4. Zaznacz pole wyboru **Pomijaj zasadę Sophos Central przez 4 godziny w celu rozwiązania problemu**.
5. Wyłącz funkcje zabezpieczeń za pomocą suwaków widocznych na stronie.

Po czterech godzinach ustawienia automatycznie zmienią się z powrotem na ustawienia zasady wymuszane centralnie.

Uwaga
W razie potrzeby możesz później ponownie zmienić ustawienia. Aby zrobić to dla poszczególnych funkcji, nie możesz korzystać z suwaków. Zamiast tego, usuń zaznaczenie pola **Pomijaj zasadę Sophos Central przez 4 godziny w celu rozwiązania problemu**.

6.5 Aktualizuj teraz

Aby zaktualizować definicje wirusów, należy postępować zgodnie z poniższymi instrukcjami.

Aby dokonać aktualizacji, wykonaj następujące czynności:

1. Kliknij opcję **Informacje**.
2. Kliknij opcję **Aktualizuj teraz**.

6.6 Rozwiązywanie problemów

W celu rozwiązania problemów należy postępować zgodnie z poniższymi instrukcjami.

Aby rozwiązać problemy, wykonaj następujące czynności:

1. Kliknij opcję **Informacje**.
2. Kliknij opcję **Otwórz narzędzie Endpoint Self Help Tool**, aby zebrać dane o problemie, albo skorzystaj z łącza do **Forum społeczności**.

6.7 Szyfrowanie komputera

Aby zaszyfrować komputer, postępuj zgodnie z instrukcjami podanymi poniżej.

Ograniczenie
Funkcja Device Encryption jest dostępna tylko na komputerach końcowych.

Funkcja Device Encryption szyfruje dysk twardy komputera za pomocą technologii Windows BitLocker. Administrator decyduje, czy przy każdym dostępie do komputera należy wprowadzać dane uwierzytelniające.

Jeśli uwierzytelnianie nie jest wymagane, szyfrowanie dysku twardego rozpoczyna się automatycznie w momencie ponownego uruchomienia komputera, po odebraniu zasady Sophos Central. W tym przypadku nie trzeba nic robić.

W przypadku konieczności uwierzytelnienia należy wykonać następujące czynności:

1. Gdy pojawi się okno **Sophos Device Encryption**, wykonaj instrukcje widoczne na ekranie. Konkretne instrukcje zależą od używanego systemu operacyjnego i zdefiniowanych przez administratora ustawień zasady.

- Jeśli zasada Device Encryption wymaga uwierzytelnienia za pomocą kodu PIN lub hasła, wykonaj instrukcje widoczne na ekranie, aby utworzyć kod PIN lub hasło.

  Uwaga
  Tworząc kod PIN lub hasło, zachowaj ostrożność. Środowisko uruchomieniowe obsługuje wyłącznie angielski (amerykański) układ klawiatury. Jeśli kod PIN lub hasło zostanie utworzone z użyciem znaków specjalnych, podczas późniejszego wprowadzania hasła w celu zalogowania się może być konieczne użycie całkiem innych klawiszy.

- Jeśli zasada Device Encryption wymaga uwierzytelniania za pomocą klucza USB, musisz podłączyć do komputera dysk flash USB. Dysk flash USB musi być sformatowany za pomocą systemu NTFS, FAT lub FAT32.

2. Kliknięcie opcji **Uruchom ponownie i zaszyfruj** spowoduje ponowne uruchomienie komputera i zaszyfrowanie dysków twardych. Możesz pracować tak, jak zwykle.

   Uwaga
   Aby zamknąć okno dialogowe, możesz wybrać opcję **Zrób to później**. Okno dialogowe pojawi się jednak ponownie podczas następnego logowania.

Gdy platforma Sophos Central zaszyfruje wolumin systemowy, rozpocznie się szyfrowanie woluminów danych. Wymienne woluminy danych, takie jak dyski USB, nie są szyfrowane.

Przy logowaniu do komputera, w celu odblokowania woluminu systemowego, może być konieczne wpisanie kodu PIN lub hasła albo podłączenie klucza USB. Woluminy danych są odblokowywane automatycznie.

6.8 Dostęp do komputera w przypadku zapomnienia hasła

Aby uzyskać dostęp do komputera, wykonaj następujące czynności.

Jeśli nie możesz zalogować się do komputera z powodu utraty kodu PIN, hasła lub klucza USB, musisz użyć klucza odzyskiwania.

Jeśli używasz funkcji Sophos Device Encryption, klucz odzyskiwania jest przechowywany na platformie Sophos Central. Aby uzyskać klucz odzyskiwania, wykonaj jedną z następujących czynności:

- Zaloguj się do portalu Sophos Self Service Portal i wykonaj instrukcje podane w części pomoc.
- Poproś administratora o pobranie dla Ciebie klucza odzyskiwania. Zrób tak, jeśli nie masz dostępu do portalu Self Service Portal.

Informacje pokrewne

Zadania pokrewne

Korzystanie z funkcji odzyskiwania BitLocker na stronie 13
W celu przywrócenia komputera do normalnego stanu, postępuj zgodnie z instrukcjami podanymi poniżej.

6.8.1 Korzystanie z funkcji odzyskiwania BitLocker

W celu przywrócenia komputera do normalnego stanu, postępuj zgodnie z instrukcjami podanymi poniżej.

Aby przywrócić komputer do normalnego stanu, wykonaj następujące czynności:

1. Uruchom ponownie komputer i naciśnij klawisz Esc na ekranie logowania **BitLocker**.
2. Na ekranie **Odzyskiwanie funkcji BitLocker** znajdź pozycję **Identyfikator klucza odzyskiwania**. Na krótki czas pojawi się **Identyfikator klucza odzyskiwania**. Aby ponownie go wyświetlić, musisz ponownie uruchomić komputer.
3. Skontaktuj się z administratorem i przekaż mu **Identyfikator klucza odzyskiwania**. Administrator musi znaleźć klucz odzyskiwania komputera w platformie Sophos Central, a następnie Ci go przekazać.
4. Wprowadź klucz odzyskiwania na ekranie **Odzyskiwanie funkcji BitLocker**. Możesz teraz uruchomić komputer.
5. Wykonaj instrukcje widoczne na ekranie, aby utworzyć nowy kod PIN lub hasło funkcji BitLocker.

   Na komputerach z systemem Windows 7 nie zostaną wyświetlone żadne instrukcje. Musisz ręcznie zresetować kod PIN lub hasło.

Teraz możesz ponownie uzyskać dostęp do komputera.

Uwaga
Z klucza odzyskiwania można skorzystać tylko jeden raz. W przypadku konieczności ponownego odzyskania komputera konieczne jest pobranie nowego klucza odzyskiwania.

7 Dlaczego mój transfer pliku został zablokowany?

Możesz pojawić się komunikat z informacją, że transfer plików (na przykład kopiowanie, przenoszenie lub wysyłanie w wiadomości e-mail) został zablokowany.

Może to wynikać z faktu skonfigurowania firmowej zasady zabezpieczającej przed niezamierzonym wysyłaniem wrażliwych informacji do użytkowników, którzy nie powinni mieć do nich dostępu.

Są dostępne dwa rodzaje komunikatów.

Komunikat	Opis
Zablokowano transfer	Jeśli pojawi się komunikat „zablokowano transfer pliku”, transfer pliku nie jest możliwy. Być może administrator dodał do komunikatu pewne wskazówki.
Transfer jest dozwolony	Jeśli pojawi się komunikat „Zablokowano żądanie przesyłania pliku”, możesz zdecydować, czy chcesz przesłać pliki. Być może administrator dodał do komunikatu pewne wskazówki. Kliknij opcję **Zezwól**, jeśli masz pewność, że działanie jest bezpieczne.

8 Wsparcie

Z pomocy technicznej dotyczącej produktów Sophos można skorzystać na kilka sposobów:

- Odwiedź Społeczność Sophos pod adresem community.sophos.com/ i znajdź innych użytkowników, którzy mają ten sam problem.
- Odwiedź bazę wiedzy technicznej Sophos pod adresem www.sophos.com/en-us/support.aspx.
- Pobierz dokumentację produktu pod adresem www.sophos.com/en-us/support/documentation.aspx.
- Wyślij zgłoszenie do naszego zespołu ds. obsługi klienta pod adresem https://secure2.sophos.com/support/contact-support/support-query.aspx.

9 Informacje prawne