Klient ™ Symantec Endpoint Protection 14.3 RU1 dla systemu Mac – Pomoc

Listopad 2020 r.

W jaki sposób Symantec Endpoint Protection chroni komputer Mac

Program Symantec Endpoint Protection łączy w sobie kilka warstw ochrony w celu zabezpieczenia komputera przed atakami wirusów oraz programów typu spyware, a także przed próbami włamania.

Typy ochrony opisują poszczególne warstwy ochrony.

Table 1: Typy ochrony

Ochrona	Opis
Ochrona przed wirusami i programami typu spyware	Program Symantec Endpoint Protection obejmuje zaplanowane skanowania antywirusowe, skanowania na żądanie i funkcję Auto-Protect, która działa w tle, monitorując wirusy. W razie wykrycia wirusa program Symantec Endpoint Protection usuwa go. W jaki sposób Ochrona przed wirusami i programami typu spyware zapewnia ochronę komputerowi Mac
Ochrona przed zagrożeniami sieciowymi	Program Symantec Endpoint Protection przechwytuje dane w warstwie sieci. Skanuje pakiety lub strumienie pakietów przy użyciu sygnatur. Skanuje każdy pakiet z osobna, szukając wzorców odpowiadających atakom sieciowym lub atakom na przeglądarkę. Funkcja Ochrona przed zagrożeniami sieciowymi obejmuje następujące elementy: • Funkcja Zapobieganie, która wykrywa ataki na składniki systemu operacyjnego i warstwę aplikacji. Kiedy pogram Symantec Endpoint Protection wykryje zagrożenie sieciowe, zagrożenie jest blokowane. • Zapora, która zezwala lub blokuje ruch sieciowy na podstawie zasad i reguł zapory. (Począwszy od wersji 14.2.) W jaki sposób ochrona przed zagrożeniami sieciowymi chroni komputer Mac
Kontrola urządzeń	Administratorzy programu Symantec Endpoint Protection Manager mogą skonfigurować zasadę kontroli urządzeń. Urządzenia mogą być zablokowane lub odblokowane za pomocą zasad na podstawie nazwy urządzeń, dostawcy urządzeń, modelu urządzenia lub numeru seryjnego. Na kliencie zarządzanym można wyświetlić ustawienia dla kontroli urządzeń na karcie **Zaawansowane**. Kontrola urządzeń jest niedostępna dla klientów niezarządzanych. Kontrola urządzeń na kliencie Symantec Endpoint Protection dla systemu Mac – informacje
Wykrywanie zagrożeń i odpowiedzi dla systemu końcowego	Administratorzy programu Symantec Endpoint Protection Manager konfigurują zasadę modułu Activity Recorder, która zapewnia środki do wykrywania i ujawniania podejrzanych działań sieciowych.

Klient automatycznie pobiera definicje wirusów, definicje systemu zapobiegania włamaniom i aktualizacje produktów na komputer.

Aktualizowanie definicji wirusa, definicji zapobiegania włamaniom oraz oprogramowania klienta

W jaki sposób Ochrona przed wirusami i programami typu spyware zapewnia ochronę komputerowi Mac

Program Symantec Endpoint Protection korzysta z definicji wirusów do wykrywania znanych wirusów podczas skanowań planowanych i ręcznych. Funkcja Auto-Protect wykorzystuje definicje wirusów do ciągłego skanowania aktywności komputera.

Program Symantec Endpoint Protection wysyła powiadomienia o wykrytych wirusach i innych zagrożeniach bezpieczeństwa. Wirusy lub inne zagrożenia bezpieczeństwa są wykrywane, gdy wystąpi jedna z następujących sytuacji:

- Funkcja Auto-Protect znajdzie wirusa w trakcie monitorowania komputera.
- Funkcja Auto-Protect znajdzie wirusa na podstawie skanowania zaplanowanego lub uruchomionego ręcznie.

Przy ustawieniach domyślnych, program Symantec Endpoint Protection automatycznie próbuje naprawić wszystkie znalezione wirusy. Jeżeli naprawa pliku jest niemożliwa, klient w bezpieczny sposób poddaje plik kwarantannie, co chroni komputer. Zazwyczaj klient dokonuje wspomnianych napraw bez żadnego działania ze strony użytkownika. Gdy komputer znajdzie wirusa, można zdecydować o przesłaniu informacji o nim do firmy Symantec.

W pewnych sytuacjach klient przedstawia zapytanie czy zainfekowany plik ma zostać naprawiony, usunięty czy przywrócony na miejsce, gdzie został znaleziony. Odpowiedź użytkownika decyduje o tym, co klient zrobi z zainfekowanym plikiem.

Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Włączanie lub wyłączanie przesyłanie informacji dotyczących zabezpieczeń do Symantec

W jaki sposób ochrona przed zagrożeniami sieciowymi chroni komputer Mac

Funkcja Ochrona przed zagrożeniami sieciowymi obejmuje następujące technologie ochrony:

- Zapobieganie włamaniom
- Zapora

Zapobieganie włamaniom

System zapobiegania włamaniom automatycznie wykrywa ataki sieciowe i blokuje je. Funkcja Zapobieganie włamaniom to wewnętrzna warstwa ochrony komputerów klienckich. Funkcja Zapobieganie włamaniom jest zwana również systemem zapobiegania włamaniom (Intrusion Prevention System, IPS).

Funkcja Zapobieganie włamaniom przechwytuje dane w warstwie sieci. Skanuje pakiety lub strumienie pakietów przy użyciu sygnatur. Skanuje każdy pakiet z osobna, szukając wzorców odpowiadających atakom sieciowym lub atakom na przeglądarkę. Funkcja Zapobieganie wykrywa ataki na składniki systemu operacyjnego i warstwę aplikacji.

Funkcja Zapobieganie włamaniom sieciowym identyfikuje ataki na komputery klienckie za pomocą sygnatur. W przypadku znanych ataków system zapobiegania włamaniom automatycznie odrzuca pakiety dopasowane do sygnatur.

Zapora

Zapora monitoruje ruch sieciowy i blokuje potencjalnie szkodliwy ruch w celu ochrony komputera Mac. Zapora programu Symantec Endpoint Protection nie jest dostępna na kliencie niezarządzanym.

Zapora programu Symantec Endpoint Protection monitoruje ruch w warstwie Komunikacja i Internet. Wbudowana zapora dla komputerów Mac monitoruje ruch na wyższej warstwie aplikacji, po tym jak zapora programu Symantec Endpoint Protection ją monitoruje. W związku z tym można włączyć obie zapory jednocześnie do uruchamiania równoległego.

Do przepuszczania lub blokowania ruchu sieciowego zapora używa następujących typów reguł:

- Reguły domyślne
- Reguły niestandardowe
- Reguły wbudowane
- Reguły ochrony

Reguły te obejmują wykrywanie skanowania portu, wykrywanie ataków typu odmowa obsługi, mechanizm zapobiegania fałszowaniu adresów MAC, smart DHCP i smart DNS. Ustawienia zapory są całkowicie kontrolowane przez administratora programu Symantec Endpoint Protection Manager. Zaporę można włączyć lub wyłączyć tylko wtedy, gdy administrator zezwolił użytkownikowi na kontrolę klienta systemu Mac.

Ochrona zapory została dodana w wersji 14.2.

Zarządzanie systemem zapobiegania włamaniom

Zarządzanie ochroną za pomocą zapory dla klienta Mac

Zgodność systemu operacyjnego z programem Symantec Endpoint Protection dla komputerów Mac

Program Symantec Endpoint Protection dla komputerów Mac obsługuje następujące wersje systemu operacyjnego:

- macOS 10.15 do 10.15.5
- macOS 10.14
- macOS 10.13

Więcej informacji o obsłudze wcześniejszych wersji systemu operacyjnego Mac można znaleźć pod adresem Zgodność systemu Mac z klientem Endpoint Protection.

Autoryzacja rozszerzenia jądra w programie Symantec Endpoint Protection w systemie macOS 10.13 lub nowszym

Informacje o wersji, nowe poprawki i wymagania systemowe dla wszystkich wersji programu Endpoint Protection

Instalowanie klienta programu Symantec Endpoint Protection for Mac

Możliwe jest bezpośrednie zainstalowanie niezarządzanego lub zarządzanego klienta programu Symantec Endpoint Protection na komputerze Mac, jeśli użytkownik nie używa lub nie może używać funkcji Remote Push. Czynności instalacyjne są podobne zarówno w przypadku klienta niezarządzanego, jak i zarządzanego.

Jedynym sposobem zainstalowania klienta zarządzanego jest użycie pakietu utworzonego za pomocą programu Symantec Endpoint Protection Manager. Klienta niezarządzanego można w każdej chwili przekonwertować na klienta zarządzanego, importując ustawienia komunikacji klient-serwer do klienta systemu Mac.

> **NOTE**
> Informacje na temat przygotowywania klienta programu Symantec Endpoint Protection dla systemu Mac do obsługi oprogramowania innych firm do zdalnego wdrażania zawiera dokument Eksportowanie i wdrażanie klienta programu Symantec Endpoint Protection przy użyciu programu Apple Remote Desktop lub Casper.

Table 2: Metody instalowania klienta dla Mac

Jeśli plik instalacyjny został pobrany.	1. Wyodrębnij zawartość do folderu na komputerze Mac, a następnie otwórz folder. 2. Otwórz folder `SEP_MAC`. 3. Skopiuj plik `Symantec Endpoint Protection.dmg` na pulpit komputera z systemem Mac. 4. Kliknij dwukrotnie plik `Symantec Endpoint Protection.dmg`, aby zainstalować go jako dysk wirtualny. Następnie zainstaluj klienta programu Symantec Endpoint Protection dla systemu Mac.
W przypadku pakietu instalacyjnego klienta z rozszerzeniem .zip z serwisu Broadcom Support Portal.	1. Skopiuj plik na pulpit komputera Mac. Plik może mieć nazwę `Symantec Endpoint Protection.zip` lub `Symantec_Endpoint_Protection_wersja_Mac_Client.zip`, gdziewersjaoznacza wersję produktu. 2. Kliknij prawym przyciskiem myszy plik i wybierz polecenia **Otwórz za pomocą > Archive Utility**, aby wyodrębnić jego zawartość. 3. Przejdź do utworzonego folderu. Następnie zainstaluj klienta programu Symantec Endpoint Protection for Mac.

Utworzony wirtualny obraz dysku lub folder zawiera instalator aplikacji oraz folder o nazwie Dodatkowe zasoby. Aby instalacja została przeprowadzona pomyślnie, oba elementy muszą znajdować się w tej samej lokalizacji. Jeśli instalator został skopiowany do innej lokalizacji, należy skopiować również folder Dodatkowe zasoby.

Aby zainstalować klienta programu Symantec Endpoint Protection dla komputerów Mac:

1. Kliknij dwukrotnie pozycję `Instalator Symantec Endpoint Protection.`
2. Aby rozpocząć instalację, kliknij przycisk **Zainstaluj**.
3. Aby zainstalować narzędzie pomocnicze potrzebne do zainstalowania klienta programu Symantec Endpoint Protection, wprowadź administracyjną nazwę użytkownika Mac i hasło, a następnie kliknij przycisk **Zainstaluj pomocnika**.
4. Po ukończeniu instalacji kliknij przycisk **Kontynuuj**, aby zakończyć konfigurowanie klienta Symantec Endpoint Protection.
5. Aby skonfigurować klienta Symantec Endpoint Protection, należy wykonać następujące kroki:

Autoryzuj rozszerzenie systemu programu Symantec Endpoint Protection.	W oknie dialogowym **Ochrona i prywatność**, na karcie **Ogólne**, w obszarze **Oprogramowanie systemowe z aplikacji "Symantec Endpoint Protection" zostało zablokowane przed załadowaniem**, kliknij przycisk **Zezwalaj**. W razie potrzeby kliknij ikonę kłódki, aby wprowadzić zmiany. Należy autoryzować rozszerzenie systemu, aby program Symantec Endpoint Protection mógł działać poprawnie. Autoryzacja rozszerzenia systemu w programie Symantec Endpoint Protection w systemie macOS 10.15 lub nowszym
Zezwalaj na pełny dostęp do dysku.	W oknie dialogowym **Ochrona i prywatność**, na karcie **Prywatność** upewnij się, że **Rozszerzenie systemu Symantec** może uzyskać dostęp do danych i ustawień administracyjnych dla wszystkich użytkowników na urządzeniu Mac. W razie potrzeby kliknij ikonę kłódki, aby wprowadzić zmiany.
Zezwalaj na zmiany w profilu sieciowym.	Po wyświetleniu monitu programu **Symantec Endpoint Protection chce filtrować zawartość sieciową**, kliknij przycisk **Zezwalaj**.

6. Kliknij przycisk **Zakończ**.

Autoryzacja rozszerzenia systemu w programie Symantec Endpoint Protection w systemie macOS 10.15 lub nowszym

Wymóg autoryzacji rozszerzenia systemu stanowi nową funkcję bezpieczeństwa w systemie macOS 10.15Należy autoryzować rozszerzenie systemu, aby program Symantec Endpoint Protection mógł działać poprawnie.

Aby udzielić autoryzacji rozszerzenia systemu w programie Symantec Endpoint Protection, podczas konfiguracji klienta Symantec Endpoint Protection, w oknie dialogowym **Ochrona i prywatność**, na karcie **Ogólne**, w **Oprogramowanie systemowe z aplikacji „Symantec Endpoint Protection" zostało zablokowane przed załadowaniem**, kliknij przycisk **Zezwalaj**.

Instalowanie klienta programu Symantec Endpoint Protection dla komputerów Mac

Monit uaktualnienia dla klienta programu Symantec Endpoint Protection dla Mac

Administratorzy programu Symantec Endpoint Protection Manager mogą przypisać pakiet instalacyjny klienta, aby automatycznie zaktualizować zarządzane komputery kliencki z ustawieniami dla instalacji klienta.

Jeżeli użytkownik jest zalogowany na komputerze Mac, może ujrzeć monit o konieczności ponownego uruchamianie, aby zakończyć instalację. Można opóźnić ponowne uruchomienie w oparciu o ustawienia instalacji klienta.

Jeżeli użytkownik nie jest zalogowany na komputerze Mac, instalator automatycznie uruchomi ponownie komputer.

Rozpoczęcie pracy z klientem Symantec Endpoint Protection

Po otwarciu klienta programu Symantec Endpoint Protection, na górze strony wyświetlany jest komunikat **Jesteś chroniony**, o ile nie wystąpi problem, który trzeba rozwiązać. Kliknij **Napraw**, aby rozwiązać wszelkie problemy.

Klient Symantec Endpoint Protection przedstawia główne zadania, które można wykonać.

Table 3: strony klienta Symantec Endpoint Protection

Opcja	Opis
Zabezpieczenia	Wyświetla stan ochrony komputera.
Skanowania	Umożliwia skanowanie komputera. Można wybrać uruchomienie szybkiego skanowania lub skanowania pełnego. Można również upuścić plik lub folder do skanowania. Uruchomianie skanowania ręcznego
LiveUpdate	Uruchamia usługę LiveUpdate w celu aktualizacji definicje oraz plików produktów dla Symantec Endpoint Protection. Natychmiastowa aktualizacja treści w Symantec Endpoint Protection
Zaawansowane	Daje więcej różnych opcji dla ochrony przed wirusami i programami typu spyware, Ochrony przed zagrożeniami sieciowymi oraz usługi LiveUpdate.

Zarządzanie ochroną komputera Mac za pomocą Symantec Endpoint Protection

Ustawienia domyślne programu Symantec Endpoint Protection zapewniają ochronę komputera Mac przed wieloma typami destrukcyjnego oprogramowania. Klient albo automatycznie obsługuje destrukcyjne oprogramowanie, albo umożliwia użytkownikowi wybranie sposobu obsługi destrukcyjnego oprogramowania.

W zależności od ustawień nadanych przez administratora należy wykonać następujące zadania, aby pomóc w zachowaniu ochrony.

NOTE
Dostosowywanie tych ustawień wymaga przyznania kontroli nad tymi zadaniami.

Table 4: Zapewnienie ochrony komputera

Kroki	Opis
Krok 1: Sprawdzenie czy zarówno Ochrona przed wirusami i programami typu spyware, jak i Ochrona przed zagrożeniami sieciowymi są włączone.	Jeżeli włączone są zabezpieczenia, pojawi się strona **Bezpieczeństwo** z zielonym znacznikiem wyboru oraz komunikatem **Jesteś chroniony**. Włączanie i wyłączanie ochrony przed wirusami i programami typu spyware Włączanie i wyłączanie funkcji Ochrona przed zagrożeniami sieciowymi
Krok 2: Zapewnienie, że pliki definicji na komputerze są aktualne.	Strona **Bezpieczeństwo** wyświetla czas ostatniej aktualizacji definicji dla funkcji Ochrona przed wirusami i programami typu spyware oraz Ochrona przed zagrożeniami sieciowymi. W obszarze **LiveUpdate** pojawi się czas ostatniej aktualizacji produktu. Aby wyświetlić numer wersji oprogramowania, kliknij pozycję **Pomoc > Informacje**.
Krok 3: Aktualizacja oprogramowania lub definicji w razie potrzeby.	Na kliencie Symantec Endpoint Protection, kliknij pozycję **LiveUpdate**, aby od razu zaktualizować oprogramowanie oraz definicje. Aktualizowanie definicji wirusa, definicji zapobiegania włamaniom oraz oprogramowania klienta

Kroki	Opis
Krok 4: Uruchom skanowanie.	Można zaplanować skanowania, aby odbywały się w regularnych odstępach czasu, albo uruchomić skanowanie od razu. Ustawianie skanowań zaplanowanych Uruchomianie skanowania ręcznego

Zarządzania ustawieniami funkcji Ochrona przed wirusami i programami typu spyware:

Odnawianie licencji produktu

Możesz zobaczyć komunikat pod ikoną klienta programu Symantec Endpoint Protection na pasku menu, mówiący że licencja na program Symantec Endpoint Protection wygasła. Klient programu Symantec Endpoint Protection używa licencji do aktualizowania następujących elementów:

- Oprogramowanie klienckie
- Pliki definicji ochrony dla skanowania pod kątem wirusów i programów typu spyware oraz zapobiegania włamaniom.

Klient może używać licencji na wersję próbną lub płatną. Gdy którakolwiek z licencji wygaśnie, klient przestaje aktualizować wszelkie definicje i oprogramowanie klienckie.

W przypadku obu typów licencji należy skontaktować się z administratorem w celu zaktualizowania lub odnowienia licencji.

Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Włączanie lub wyłączanie kontroli urządzenia na kliencie programu Symantec Endpoint Protection dla systemu Mac

Administratorzy Symantec Endpoint Protection Manager mogą konfigurować klientów zarządzanych za pomocą zasady kontroli urządzeń. Urządzenia mogą być zablokowane lub odblokowane za pomocą zasad na podstawie nazwy urządzeń, dostawcy urządzeń, modelu urządzenia lub numeru seryjnego.

Można wyświetlić działania kontroli urządzeń na stronie **Zaawansowane**, klikając pozycję **Działania > Historia zabezpieczeń**.

Ustawienia klienta Symantec Endpoint Protection dla opcji **Kontrola urządzeń** pozwala włączyć lub wyłączyć kontrolę urządzeń. Jeżeli kontrola urządzeń jest włączona można opcjonalnie włączyć lub wyłączyć powiadomienia, gdy urządzenia są blokowane lub odblokowywane.

Aby zmienić ustawienia należy się uwierzytelnić za pomocą poświadczeń administratora systemu Mac. Jeżeli te ustawienia są przyciemnione, oznacza to, że administrator je zablokował, aby uniemożliwić włączanie i wyłączanie tej funkcji.

Nie można dodać ani dodawać urządzeń, które mają być blokowane lub odblokowane za pomocą interfejsu klienta Symantec Endpoint Protection.

NOTE
Zasada kontroli urządzeń z programu Symantec Endpoint Protection Manager kontroluje ustawienia kontroli urządzeń. Przy następnym pulsie, wszelkie zmiany wprowadzone w tych ustawieniach zostaną przywrócone do ustawień dyktowanych przez zasadę.

Kontrola urządzeń jest niedostępna dla klientów niezarządzanych.

Informacje o funkcji Przekierowanie ruchu sieciowego WSS na kliencie Mac

Funkcja Przekierowanie ruchu sieciowego WSS (WTR) umożliwia automatyzowanie przekierowywania ruchu internetowego do usługi Symantec Web Security i zapewnia ochronę ruchu sieciowego na każdym komputerze korzystającym z programu Symantec Endpoint Protection.

Administrator steruje ustawieniami funkcji Przekierowanie ruchu sieciowego WSS, co obejmuje adres URL konfiguracji serwera proxy oraz opcjonalny certyfikat główny usługi Symantec Web Security Service. Tylko administrator Symantec Endpoint Protection Manager może skonfigurować te ustawienia, które nie są dostępne w interfejsie klienta Symantec Endpoint Protection. Adres URL pliku konfiguracji serwera proxy można wyświetlić na komputerach Mac w sekcji **Preferencje systemu > Sieć** w obszarze **Proxy**. Certyfikat Usługi w chmurze jest dostępny w sekcji **Pęk kluczy**.

Przeglądarki internetowe Safari, Chrome oraz Firefox w wersji 65 i nowszych obsługują przekierowanie ruchu sieciowego WSS. Symantec Endpoint Protectionwersje wcześniejsze niż 14.2 RU1 obsługują tylko przeglądarki Safari i Chrome.

Odinstalowanie klienta Symantec Endpoint Protection w systemie Mac

Klienta Symantec Endpoint Protection dla systemu Mac można odinstalować za pomocą ikony klienta na pasku menu. Odinstalowanie klienta Symantec Endpoint Protection dla systemu Mac wymaga poświadczeń administratorskich użytkownika.

> **NOTE**
> Po odinstalowaniu klienta Symantec Endpoint Protection wyświetlany jest monit o ponowne uruchomienie komputera klienckiego w celu ukończenia odinstalowywania. Przed rozpoczęciem upewnij się, że wszystkie nieskończone zadania są zapisane a wszystkie otwarte aplikacje zamknięte.

Aby odinstalować klienta Symantec Endpoint Protection dla systemu Mac:

1. Na komputerze Mac otwórz klienta Symantec Endpoint Protection i kliknij przycisk **Symantec Endpoint Protection > Odinstaluj Symantec Endpoint Protection**.
2. Kliknij przycisk **Odinstaluj**, aby rozpocząć odinstalowywanie.
3. Aby zainstalować narzędzie pomocnicze potrzebne do odinstalowania klienta programu Symantec Endpoint Protection, wprowadź administracyjną nazwę użytkownika Mac i hasło, a następnie kliknij przycisk **Zainstaluj pomocnika**.
4. W oknie dialogowym **Symantec Endpoint Protection próbuje zmodyfikować Rozszerzenie systemu**, wprowadź administracyjną nazwę użytkownika Mac i hasło, a następnie kliknij przycisk **OK**.

   Dezinstalacja klienta może wymagać podania hasła. To hasło może być inne, niż hasło administracyjne systemu macOS.
5. Po zakończeniu odinstalowywania, należy kliknąć **Uruchom ponownie teraz**.

Jeśli odinstalowanie nie powiedzie się, konieczne może być użycie innej metody odinstalowywania. Patrz:

Odinstalowywanie programu Symantec Endpoint Protection

Aktualizowanie definicji wirusa, definicji zapobiegania włamaniom oraz oprogramowania klienta

Skuteczność ochrony zapewnianej przez produkty firmy Symantec jest uzależniona od aktualności informacji o nowych zagrożeniach. Symantec udostępnia te informacje programowi Symantec Endpoint Protection za pośrednictwem usługi LiveUpdate. Usługa LiveUpdate pobiera aktualizacje produktu i aktualizacje definicji, korzystając z połączenia internetowego użytkownika.

Aktualizacje definicji to pliki, dzięki którym produkty firmy Symantec są aktualne i korzystają z najnowszych technologii ochrony przed zagrożeniami. Usługa LiveUpdate pobiera nowe sygnatury zapobiegania włamaniom i pliki definicji wirusów z internetowej witryny firmy Symantec, a następnie zastępuje nimi stare pliki.

Aktualizacje produktu to ulepszenia zainstalowanego klienta. Aktualizacje produktu tworzy się zazwyczaj w celu zapewnienia zgodności oprogramowania z urządzeniami lub systemami operacyjnymi, zwiększenia wydajności lub usunięcia błędów produktu. Aktualizacje produktu ukazują się, gdy pojawi się taka potrzeba. Klienci mogą pobierać aktualizacje produktu bezpośrednio z serwera LiveUpdate. Aktualizacja produktu oraz aktualizacje definicji są zwane łącznie aktualizacjami treści.

Table 5: Sposoby aktualizowania składników oprogramowania na komputerze

Zadanie	Opis
Natychmiastowa aktualizacja składników oprogramowania	Natychmiastowe uruchomienie usługi LiveUpdate. Natychmiastowa aktualizacja treści w Symantec Endpoint Protection

Zarządzanie ochroną komputera Mac za pomocą Symantec Endpoint Protection

Natychmiastowa aktualizacja treści w Symantec Endpoint Protection

Pliki definicji i pliki produktu można aktualizować natychmiast za pomocą usługi LiveUpdate. Usługę LiveUpdate należy uruchamiać natychmiast w następujących sytuacjach:

- Po zainstalowaniu oprogramowania klienckiego.
- Po upływie długiego czasu od ostatniego skanowania.
- Gdy użytkownik podejrzewa, że na komputerze jest wirus lub inne destrukcyjne oprogramowanie.

Aby zaktualizować treści na klientach Symantec Endpoint Protection:

Uruchom program LiveUpdate w jeden z następujących sposobów:

- Kliknij prawym przyciskiem myszy ikonę Symantec Endpoint Protection na pasku narzędzi, a następnie kliknij polecenie **LiveUpdate**.
- Otwórz klienta Symantec Endpoint Protection, a następnie kliknij przycisk **LiveUpdate**.

Usługa LiveUpdate łączy się z serwerem LiveUpdate, sprawdza, czy są dostępne nowe aktualizacje, a następnie automatycznie je pobiera i instaluje. Pasek stanu pokazuje postęp pobierania.

Aktualizowanie definicji wirusa, definicji zapobiegania włamaniom oraz oprogramowania klienta

Aktualizacja treści w programie Symantec Endpoint Protection zgodnie z harmonogramem.

Harmonogramy na zarządzanych klientach systemu Mac

Domyślnie zarządzani klienci systemu Mac otrzymują harmonogram Symantec Endpoint Protection Manager, który uruchamia usługę LiveUpdate co cztery godziny. Administrator programu Symantec Endpoint Protection Manager kontroluje harmonogram. Zarządzani klienci nie mogą usuwać, modyfikować ani wyświetlac harmonogramu utworzonego przez administratora, ani tworzyć nowych harmonogramów.

Harmonogramy na niezarządzanych klientach systemu Mac

Użytkownik może utworzyć harmonogram automatycznego uruchamiania usługi LiveUpdate. Użytkownik może zaplanować uruchamianie usługi LiveUpdate na czas, w którym nie używa komputera.

Aby zaktualizować treści programu Symantec Endpoint Protection według harmonogramu:

1. Na kliencie programu Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ustawienia Produktu**, a następnie kliknij ikonę **Zaplanowane LiveUpdate**.

   Pojawi się aktualny harmonogram.

2. Wybierz przedział czasu z menu rozwijanego Harmonogram usługi LiveUpdate.

   Zgodnie z ustawieniami początkowymi usługa jest uruchamiana co **4** godziny. Można również wybrać uruchamianie usługi **Codziennie** lub **Co tydzień**, wybierając datę i godzinę.

3. Kliknij przycisk **Zastosuj zmiany**.

Natychmiastowa aktualizacja treści w Symantec Endpoint Protection

Aktualizowanie definicji wirusa, definicji zapobiegania włamaniom oraz oprogramowania klienta

Łączenie się z serwerem zarządzania za pośrednictwem serwera proxy – Informacje

Użytkownik może poproszony przez program Symantec Endpoint Protection o podanie poświadczeń, aby połączyć się z serwerem zarządzania za pośrednictwem serwera proxy. Otrzymasz komunikat z zapytaniem czy wyrażasz zgodę na dostęp procesu `symdaemon` do poświadczeń.

Należy kliknąć **Zawsze Dopuszczaj** w tym komunikacie. W przeciwnym wypadku będziesz otrzymywać ten sam komunikat za każdym razem, gdy klient będzie się komunikował z serwerem usługi LiveUpdate. Jeżeli klikniesz **Odmawiaj** klient nie będzie mógł otrzymywać aktualizacji oprogramowanie i definicji.

Aktualizowanie definicji wirusa, definicji zapobiegania włamaniom oraz oprogramowania klienta

Zarządzania ustawieniami funkcji Ochrona przed wirusami i programami typu spyware:

Domyślnie, program Symantec Endpoint Protection chroni przed wirusami i zagrożeniami bezpieczeństwa, w tym zagrożeniami sieciowymi od momentu uruchomienia komputera. Ochrona przed wirusami i spyware obejmuje Auto-Protect, która sprawdza programy pod kątem obecności wirusów przed uruchomieniem. Monitoruje także komputer w celu wykrycia jakichkolwiek operacji, które mogłyby wskazywać na obecność wirusa lub zagrożenia bezpieczeństwa. Przechwytywanie przez funkcję Auto-Protect uniemożliwia wirusom zainfekowanie komputera, dlatego funkcja Auto-Protect powinna być włączona.

W przypadku klientów zarządzanych zakres kontroli nad ustawieniami zależy od tego, jak administrator skonfigurował klienta. Co więcej, przy następnym pulsie, wszelkie zmiany wprowadzone w tych ustawieniach zostaną przywrócone do ustawień dyktowanych przez zasadę.

Zarządzanie ochroną przed wirusami i programami typu spyware opisuje zadania, które można wykonać w celu zarządzania Ochroną przed wirusami i programami typu spyware na komputerze Mac.

Table 6: Zarządzanie funkcją Ochrona przed wirusami i programami typu spyware

Kroki	Opis
Krok 1: Włączenie lub wyłączenie ochrony przed wirusami i programami typu spyware	Można z łatwością włączać lub wyłączać Ochronę przed wirusami i programami typu spyware. Firma Symantec zaleca pozostawienie tej usługi włączonej. Włączanie i wyłączanie ochrony przed wirusami i programami typu spyware
Krok 2: Dostosowanie ustawień funkcji Auto-Protect	Auto-Protect stanowi ważny element Ochrony przed wirusami i programami typu spyware. Można skonfigurować te opcje na stronie **Zaawansowane**. Konfigurowanie ustawień funkcji: Auto-Protect oraz Scan Zone
Krok 3: Skanowanie komputera w poszukiwaniu wirusów	Można ustawić, aby skanowanie antywirusowe było uruchamiane zgodnie z harmonogramem lub natychmiastowo. Ustawianie skanowań zaplanowanych Wstrzymywanie, odkładanie i zatrzymywanie skanowań Uruchomianie skanowania ręcznego
Krok 4: Reakcja po wykryciu wirusa przez program Symantec Endpoint Protection	Podczas gdy program Symantec Endpoint Protection skanuje komputer może on: • Powiadomić o działaniach, które możesz podjąć. • Poinformować o działaniach ochronnych, które podjął za Ciebie. Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Włączanie i wyłączanie ochrony przed wirusami i programami typu spyware

Domyślnie, Ochrona przed wirusami i spyware jest włączona wraz z usługą Auto-Protect.

Można bardziej szczegółowo kontrolować usługę Auto-Protect ustawiając konkretne opcje.

Jeżeli Ochrona przed wirusami i programami typu spyware jest wyłączona pojawia się czerwony „x” na stronie **Stan** z komunikatem **Ochrona przed wirusami i programami typu spyware jest wyłączona**. Jeżeli ochrona jest wyłączona należy włączyć ją jak najszybciej.

NOTE
Planowane skanowania będą nadal wykonywane niezależnie od tego, czy Ochrona przed wirusami i programami typu spyware jest włączona czy wyłączona. Administrator może ograniczyć dostęp do niektórych z ustawień programu Symantec Endpoint Protection. Możesz nie posiadać uprawnień do wyłączenia tych ustawień, planowania skanowań czy dostosowywania opcji ochrony.Może być wymagane podanie hasła administratora systemu Mac, aby zmienić którekolwiek z tych ustawień.

Aby włączyć lub wyłączyć ochronę przed wirusami i programami typu spyware:

1. Aby włączyć ochronę przed wirusami i programami typu spyware na kliencie Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ochrona systemu Mac**, a następnie włącz **Automatyczne skanowanie**.
2. Aby wyłączyć ochronę przed wirusami i programami typu spyware na kliencie Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ochrona systemu Mac**, a następnie wyłącz **Automatyczne skanowanie**.

Konfigurowanie ustawień funkcji: Auto-Protect oraz Scan Zone

Zarządzania ustawieniami funkcji Ochrona przed wirusami i programami typu spyware:

Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Konfigurowanie ustawień funkcji: Auto-Protect oraz Scan Zone

Na klientach zarządzanych, o ile administrator pozwoli, można dostosować sposób w jaki funkcja Auto-Protect monitoruje wirusy i naprawia zainfekowane pliki.

Ustawienia funkcji Auto-Protect wyświetlają się jako opcje w obszarze **Ochrona systemu Mac**. Aby włączyć funkcję Auto-Protect, należy włączyć **Automatyczne skanowanie**.

Ustawienia Scan Zone umożliwiają określenie plików, które mają być objęte skanowaniem i wykluczone ze skanowania.

Aby skonfigurować ustawienia funkcji Auto-Protect:

1. Na kliencie programu Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ochrona systemu Mac**, a następnie kliknij ikonę ustawień **Automatyczne skanowanie**.
2. Można zmienić jedną z następujących opcji:

Automatyczna kwarantanna	Umożliwia wybranie, czy wszelkie pliki, których nie można naprawić, mają być przenoszone do kwarantanny.
Automatyczna naprawa	Umożliwia włączenie automatycznej naprawy wszystkich zainfekowanych plików znalezionych przez funkcję Automatyczna ochrona.
Skanowanie	Można wybrać opcję **Dyski z danymi** i **Wszystkie inne dyski**.
Skanuj pliki skompresowane	Umożliwia wybranie, czy pliki skompresowane mają być uwzględniane w skanowaniu funkcji Automatyczna ochrona. Skanowanie obejmuje plik skompresowany i pliki wewnątrz pliku skompresowanego.

WARNING
W przypadku niewybrania opcji **Automatyczna naprawa** żadne zainfekowane pliki nie są przenoszone do kwarantanny, nawet jeśli wybrana została opcja **Poddaj kwarantannie pliki, których nie można naprawić**.Oprogramowanie pyta, czy ma naprawić zainfekowany plik. Jeśli plik nie zostanie naprawiony, pozostanie na komputerze. W przypadku wybrania opcji **Automatyczna naprawa** przy niewybraniu opcji **Automatyczna kwarantanna** wszystkie zainfekowane pliki są usuwane.

3. Kliknij przycisk **Gotowe**.

Aby skonfigurować ustawienia Scan Zone:

1. Na kliencie programu Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ochrona systemu Mac**, a następnie kliknij ikonę ustawień **Ustawienia Scan Zone**.
2. Można zmienić jedną z następujących opcji:

Skanuj wszędzie	Wszystkie pliki i procesy na komputerze są skanowane, gdy uzyskiwany jest do nich dostęp.
Skanuj tylko	Tylko określone pliki i foldery są objęte skanowaniem.
Nie skanuj	Wszystkie pliki i foldery są skanowane z wyjątkiem plików określonych jako wykluczone ze skanowania.
Użyj ustawień domyślnych	Ten wybór oznacza skanowanie wszędzie.

3. Kliknij przycisk **OK**.

W jaki sposób Ochrona przed wirusami i programami typu spyware zapewnia ochronę komputerowi Mac

Włączanie i wyłączanie ochrony przed wirusami i programami typu spyware

Zarządzanie plikami poddanymi kwarantannie

Ustawianie skanowań zaplanowanych

Program Symantec Endpoint Protection automatycznie uruchamia skanowanie domyślne, nawet jeżeli jest to klient zarządzany. Jeżeli administrator pozwala, można ustawić dodatkowe skanowania zaplanowane.

> **NOTE**
> W przypadku klienta niezarządzonego, trzeba samemu uruchamiać skanowania.Firma Symantec zaleca jak najszybsze przeprowadzenie pełnego skanowania ręcznego, a następnie konfigurowanie regularnych skanowań zaplanowanych. Można wstrzymać lub opóźnić każde skanowanie, niezależnie od tego czy to skanowanie zaplanowane czy ręczne.

Na kliencie zarządzanym, przy włączonej funkcji Automatycznej naprawy, domyślne skanowanie jest uruchamiane codziennie o godz. 8:00.

Uruchomianie skanowania ręcznego

Aby skonfigurować skanowania zaplanowane:

1. Na kliencie programu Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ochrona systemu Mac**, a następnie kliknij ikonę ustawień **Skanowania zaplanowane**.
2. W oknie dialogowym kliknij pozycję **Dodaj skanowania zaplanowane** lub kliknij pozycję **Edytuj**, aby zmienić ustawienia dla bieżących skanowań zaplanowanych.
3. W zakładce **Elementy skanowania** można ustawić następujące:

Dyski	Można wybrać czy skanować **Dyski twarde** oraz **Dyski wymienne**.
Foldery	Można wybrać skanowanie pliki w folderach **Folder główny (Aktywny użytkownik)**, **Aplikacje** oraz **Biblioteka**. Jeśli żaden użytkownik nie jest zalogowany w czasie planowanego skanowania folderu głównego, skanowanie nie zostanie uruchomione.
Opcje skanowania	Do wyboru dostępne są następujące opcje: • **Skanuj pliki skompresowane** • **Automatyczna naprawa** • **Automatyczna kwarantanna** • **Włącz skanowanie podczas bezczynności**

4. W zakładce **Harmonogram skanowania** można ustawić następujące opcje:

Harmonogram skanowania	Można skonfigurować skanowanie, które będzie uruchamiane w odstępach określonych w godzinach, dniach, tygodniach lub miesiącach. Opcja **Uruchamiaj w określonych odstępach czasu** jest wybrana domyślnie przy planowaniu nowego skanowania.
Uruchamiaj co	Dostępna jeżeli opcja **Uruchamiaj co określony czas** jest wybrana dla **Harmonogram skanowania**.
Godzina rozpoczęcia	Dostępny przy wyborze opcji **Codziennie**, **Co tydzień** lub **Co miesiąc** dla harmonogramu skanowania. Można wybrać porę dnia, o której będzie uruchamiane skanowanie. Najlepiej wybrać czas, kiedy nie jest się w pracy, ponieważ skanowanie może spowolnić pracę komputera.
Włączony	Dostępny przy wyborze opcji **Co tydzień`** lub **Co miesiąc** dla harmonogramu skanowania. Można wybrać dzień tygodnia lub miesiąca, w którym skanowanie ma być uruchamiane. Zalecamy wybranie terminu, kiedy nie jest się w pracy, ponieważ skanowanie może spowolnić pracę komputera.

5. Na karcie **Optymalizacja** można dostosować sposób optymalizacji wydajności skanowania.
6. Kliknij przycisk **OK**.
7. Kliknij przycisk **Gotowe**.

Wstrzymywanie, odkładanie i zatrzymywanie skanowań

Zarządzanie ochroną komputera Mac za pomocą Symantec Endpoint Protection

Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Włączanie lub wyłączanie przesyłanie informacji dotyczących zabezpieczeń do Symantec

Uruchomianie skanowania ręcznego

Może być konieczne przeskanowanie niektórych plików ręcznie. Na przykład: może być konieczne przeskanowanie plików zapisanych na komputerze przed instalacją programu Symantec Endpoint Protection. Możesz też zdecydować, że niektóre pliki wykluczone z planowanego skanowania powinny zostać przeskanowane.

> **NOTE**
> Można wstrzymać lub opóźnić każde skanowanie, niezależnie od tego czy to skanowanie zaplanowane czy ręczne.

Aby rozpocząć skanowanie ręczne:

W kliencie programu Symantec Endpoint Protection na stronie **Skany** wykonaj jedno z poniższych zadań:

- Aby rozpocząć szybkie skanowanie, kliknij pozycję **Szybkie skanowanie**, a następnie kliknij pozycję **Rozpocznij szybkie skanowanie**.
- Aby rozpocząć pełne skanowanie, kliknij pozycję **Pełne skanowanie**, a następnie kliknij pozycję **Rozpocznij pełne skanowanie**.
- Aby zeskanować plik lub folder, kliknij pozycję **Skanowanie pliku**, a następnie kliknij pozycję **Wybierz plik**.Okno Finder zostanie otwarte i będzie można wybrać opcje **Pokazuj pliki ukryte** oraz **Skanuj pliki skompresowane**. Można również włączyć opcję **Automatyczna naprawa** oraz **Automatyczna kwarantanna**.

Wstrzymywanie, odkładanie i zatrzymywanie skanowań

Ustawianie skanowań zaplanowanych

Włączanie lub wyłączanie przesyłanie informacji dotyczących zabezpieczeń do Symantec

Wstrzymywanie, odkładanie i zatrzymywanie skanowań

Funkcja wstrzymywania umożliwia zatrzymanie skanowania w i wznowienie go w późniejszym stosownym czasie. Można również zatrzymać i anulować skanowanie w dowolnym czasie. Nie potrzeba mieć uprawnień administratora, aby korzystać z tych funkcji.

Wznowione skanowanie rozpoczyna się od miejsca, w którym zostało przerwane.

> **NOTE**
> W przypadku wstrzymania skanowania w chwili, gdy klient skanuje plik skompresowany, klient może zareagować na żądanie wstrzymania dopiero po kilku minutach.

Jeśli odkładanie jest włączone, można także odłożyć skanowanie na później, ale tylko przed jego rozpoczęciem. Nie można odłożyć trwającego skanowania.

Aby wstrzymać lub zatrzymać uruchomione planowe skanowanie:

1. W oknie dialogowym postępu skanowania kliknij pozycję **Wstrzymaj**.
2. W oknie dialogowym postępu skanowania kliknij pozycję **Wznów skanowanie**, aby kontynuować skanowanie, albo kliknij pozycję **Zatrzymaj**, aby przerwać skanowanie. Można również kliknąć przycisk **Wykonano**, aby zamknąć okno.

Aby wstrzymać lub zatrzymać skanowanie ręczne:

1. W oknie dialogowym postępu skanowania kliknij pozycję **Wstrzymaj**, aby wstrzymać skanowanie.
2. Kliknij **Anuluj**, aby wstrzymać uruchomione ręczne skanowanie, lub kliknij **Wznów** aby kontynuować skanowanie.

Aby odłożyć skanowanie, które ma się wkrótce rozpocząć:

1. W wyświetlonym oknie kliknij menu rozwijane, aby wybrać wartość określającą, na jak długo zostanie odłożone skanowanie. Skanowanie można odłożyć na minimum 15 minut, a maksymalnie na jeden dzień.
2. Kliknij przycisk **OK**, aby odłożyć skanowanie.

   Jeśli skanowanie ma działać zgodnie z harmonogramem, to nie trzeba wykonywać żadnych czynności.

Ustawianie skanowań zaplanowanych

Uruchomianie skanowania ręcznego

Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Można sprawdzić, czy komputer jest zainfekowany i wykonać pewne dodatkowe zadania w celu zwiększenia poziomu bezpieczeństwa lub wydajności.

Administrator może zarządzać klientem lub może być to klient niezarządzany. Zadania ochrony, które można wykonać zależą od tego jak wysoki poziom kontroli nad klientem ma administrator.

Jeżeli produkt Symantec Endpoint Protection znajdzie wirusa lub zagrożenie bezpieczeństwa, możesz zostać poproszony o podjęcie działania. W oparciu o ustawienia, które wybrał administrator, możesz otrzymywać powiadomienia o działaniu, które klient podjął automatycznie.

Table 7: Reagowanie na komunikaty o infekcjach

Treść komunikatu	Wymagane działanie
Zainfekowany plik został naprawiony	Brak
Wymaga zatwierdzenia naprawy zainfekowanego pliku	Zatwierdzenie naprawy. Ta opcja zależy od ustawień preferencji usługi Auto-Protect. Zarządzania ustawieniami funkcji Ochrona przed wirusami i programami typu spyware: Jeżeli opcja automatycznej naprawy zainfekowanych plików nie jest zaznaczona, należy naprawić plik ręcznie. Naprawa zainfekowanych plików
Nie można naprawić zainfekowanego pliku	Skierować infekcję do kwarantanny Zarządzanie plikami poddanymi kwarantannie

W jaki sposób Ochrona przed wirusami i programami typu spyware zapewnia ochronę komputerowi Mac

Naprawa zainfekowanych plików

Jeżeli zainfekowany plik nie zostanie automatycznie zreperowany lub umieszczony w kwarantannie, można naprawić plik z listy wyników skanowania. Istnieje możliwość ręcznej naprawy pliku na twardym dysku komputera lub na nośniku wymiennym.

Aby naprawić zainfekowane pliki:

1. Z listy wyników skanowania należy wybrać plik do naprawy a następnie kliknąć **Naprawa**.

   Można również kliknąć prawym przyciskiem myszy dowolny plik z menu Maca **Znajdź** lub **Wyszukaj**
2. W razie potrzeby powtórzyć.
3. Uruchom kolejne skanowanie, aby sprawdzić inne zainfekowane pliki.
4. Sprawdź naprawione pliki, aby upewnić się, że działają prawidłowo.

Zarządzania ustawieniami funkcji Ochrona przed wirusami i programami typu spyware:

Zarządzanie plikami poddanymi kwarantannie

Zarządzanie plikami poddanymi kwarantannie

Domyślnie, jeżeli klient wykryje wirusa w pliku, próbuje usunąć wirusa. Jeśli usunięcie wirusa okaże się niemożliwe, plik jest poddawany kwarantannie na komputerze. Jeżeli program Symantec Endpoint Protection wykryje zagrożenie bezpieczeństwa w pliku, najpierw poddaje ten plik kwarantannie. Następnie naprawia wszelkie skutki uboczne zagrożenia.

Po aktualizacji definicji wirusów klient automatycznie sprawdza obszar kwarantanny. Elementy znajdujące się w obszarze kwarantanny można ponownie przeskanować. Najnowsze definicje mogą umożliwić oczyszczenie lub naprawienie plików poddanych kwarantannie.

Aby zarządzać plikami poddanymi kwarantannie:

1. W programie klienckim Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Działania > Historia zabezpieczeń > Kwarantanna**.
2. Wybierz pliki, którymi chcesz zarządzać, a następnie wybierz odpowiednią opcję:

Naprawa	Wybierz tę opcję, aby spróbować naprawić pliki poddane kwarantannie. Upewnij się, że definicje wirusa są późniejsze niż data poddania pliku kwarantannie.
Usuń	Wybierz tę opcję, aby usunąć wszelkie pliki, które nie są już potrzebne z obszaru kwarantanny.
Przywróć	Jeżeli jesteś pewien, że plik nie zawiera wirusa możesz przywrócić go do pierwotnej lokalizacji na komputerze. Ta opcja nie skanuje pliku, ani nie próbuje go naprawić.

Reagowanie na komunikaty o wykrytych infekcjach i zagrożeniach

Włączanie lub wyłączanie przesyłanie informacji dotyczących zabezpieczeń do Symantec

Program Symantec Endpoint Protection może przesyłać zamaskowane informacje o wykrytych zagrożeniach do centrum Symantec. Symantec używa tych informacji w celu zapewnienia komputerom klienckim ochrony przed nowymi, wyspecjalizowanymi i mutującymi zagrożeniami. Wszelkie dane przesyłane do firmy Symantec ułatwiają jej reagowanie na zagrożenia i dostosowywanie ochrony komputera użytkownika.

Dane telemetryczne firmy Symantec mogą zawierać zamaskowane elementy, które nie są bezpośrednio identyfikowalne. Firma Symantec nie potrzebuje wykorzystywać danych telemetrycznych do identyfikacji poszczególnych użytkowników i nie podejmuje takich prób

Domyślnie komputer kliencki wysyła informacje o wykryciach do centrum Symantec. Można wyłączyć przesyłanie, chociaż Symantec zaleca zostawić to ustawienie włączone.

Ta opcja przesyła jedynie informacje o wykrywanie wirusów.

NOTE
Firma Symantec zaleca pozostawienie tej opcji włączonej.

Aby włączyć lub wyłączyć przekazywanie zamaskowanych informacji dotyczących zabezpieczeń do firmy Symantec:

Na kliencie programu Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ustawienia produktu**, a następnie włącz lub wyłącz **Przesyłanie informacji zabezpieczających**.

Ustawianie skanowań zaplanowanych

Uruchomianie skanowania ręcznego

Zarządzanie systemem zapobiegania włamaniom

Domyślne ustawienia dla funkcji zapobieganie włamaniom chroniącej klienta z systemem Mac. Jeżeli jednak, chcesz zarządzać własną ochroną, możesz zarządzać funkcją zapobiegania włamaniom jako częścią funkcji Ochrona przed zagrożeniami sieciowymi.

Table 8: Zarządzanie systemem zapobiegania włamaniom

Kroki	Opis
Krok 1: Zapoznanie się z systemem zapobiegania włamaniom	Należy zapoznać się ze sposobem, w jaki system zapobiegania włamaniom wykrywa ataki sieciowe i blokuje je. W jaki sposób ochrona przed zagrożeniami sieciowymi chroni komputer Mac
Krok 2: Pobranie najnowszych sygnatur systemu zapobiegania włamaniom	Domyślnie najnowsze sygnatury są pobierane na klienta. Sygnatury można jednak pobrać natychmiast. Natychmiastowa aktualizacja treści w Symantec Endpoint Protection
Krok 3: Włączenie lub wyłączenie systemu zapobiegania włamaniom	Może pojawić się potrzeba wyłączenia funkcji zapobiegania włamaniom wyłączyć w celu rozwiązywania problemów lub gdy komputery klienckie zgłaszają nadmierną liczbę fałszywych alarmów. Zazwyczaj nie należy wyłączać funkcji zapobiegania włamaniom. Włączanie i wyłączanie funkcji Ochrona przed zagrożeniami sieciowymi
Krok 4: Włączenie powiadomień systemu zapobiegania włamaniom	Można skonfigurować powiadomienia, które będą wyświetlane, gdy program Symantec Endpoint Protection wykryje atak. Włączanie i wyłączanie powiadomień funkcji Ochrona przed zagrożeniami sieciowymi

Zarządzanie ochroną za pomocą zapory dla klienta Mac

Zapora Symantec Endpoint Protection dla komputerów Mac zapewnia ochronę z możliwością pełnej integracji w Symantec Endpoint Protection, co obejmuje zdarzenia, zasady i polecenia. Zapora Symantec Endpoint Protection jest dostępna tylko dla klientów zarządzanych.

NOTE
Zapora Symantec Endpoint Protection dla komputerów Mac nie integruje się z zaporą systemu operacyjnego. Obydwie zapory działają równolegle. Zapora systemu operacyjnego działa na poziomie warstwy aplikacji, a zapora Symantec Endpoint Protection zapewnia ochronę na niższych poziomach (IP i Transport).Zapora Symantec Endpoint Protection dla komputerów Mac nie pozwala na korzystanie z reguł blokowania typu peer-to-peer, ale reguły te można tworzyć w ramach niestandardowych reguł zapory.

Table 9: Zarządzanie ochroną za pomocą zapory

Kroki	Opis
Krok 1: Zapoznanie się z funkcją zapory	Należy poznać sposób, w jaki ochrona zapory monitoruje ruch i chroni przed typowymi wektorami ataków. W jaki sposób ochrona przed zagrożeniami sieciowymi chroni komputer Mac
Krok 2: Włączanie lub wyłączanie zapory.	Może pojawić się potrzeba wyłączenia zapory w celu rozwiązywania problemów, na przykład jeśli ruch jest zablokowany, podczas gdy ma być dozwolony. Zazwyczaj nie należy wyłączać zapory. Włączanie i wyłączanie funkcji Ochrona przed zagrożeniami sieciowymi

Włączanie i wyłączanie funkcji Ochrona przed zagrożeniami sieciowymi

Zazwyczaj po wyłączeniu składników Ochrony przed zagrożeniami sieciowymi na komputerze użytkownika, staje się on mniej bezpieczny. Wyłączenie funkcji zapobiegania włamaniom może być jednak konieczne, aby zapobiec fałszywym alarmom lub wyłączyć zaporę, aby rozwiązać problemy zablokowanego ruchu. System zapobiegania włamaniom i zapora są składnikami funkcji Ochrony przed zagrożeniami sieciowymi.

W przypadku klientów zarządzanych zakres kontroli nad ustawieniami zależy od tego, jak administrator skonfigurował klienta. Co więcej, przy następnym pulsie, wszelkie zmiany wprowadzone w tych ustawieniach zostaną przywrócone do ustawień dyktowanych przez zasadę.

W przypadku klientów niezarządzanych zapora jest niedostępna.

Włączanie i wyłączanie funkcji Ochrona przed zagrożeniami sieciowymi:

1. W programie klienckim Symantec Endpoint Protection, na stronie **Zaawansowane** kliknij pozycję **Ochrona przed zagrożeniami sieciowym**.
2. Aby włączyć lub wyłączyć funkcję zapobiegania włamaniom, włącz lub wyłącz **Zapobieganie włamaniom**.
3. Aby włączyć lub wyłączyć zaporę, włącz lub wyłącz opcję **Zapora**.
4. Aby włączyć lub wyłączyć powiadomienia dotyczące zapobiegania włamaniom i zapory, kliknij ikonę ustawień **Ochrona przed lukami**, a następnie w oknie dialogowym zaznacz lub wyczyść pole wyboru **Wyświetl powiadomienia ochrony przed lukami**.
5. Kliknij przycisk **Gotowe**.

W przypadku wyłączenia tych komponentów, należy włączyć ją jak najszybciej, aby zapewnić komputerowi najlepszą możliwą ochronę.

Zarządzanie systemem zapobiegania włamaniom

Zarządzanie ochroną za pomocą zapory dla klienta Mac


Symantec
A Division of Broadcom