System Center

Endpoint Protection dla systemu Mac

Podręcznik instalacji i Podręcznik użytkownika

Microsoft

Spis treści

System Center Endpoint Protection

W związku z rosnącą popularnością systemów operacyjnych opartych na platformie Unix autorzy szkodliwego oprogramowania przygotowują coraz więcej aplikacji wymierzonych w użytkowników komputerów Mac. Program System Center Endpoint Protection udostępnia zaawansowaną i skuteczną ochronę przed takimi zagrożeniami. Program System Center Endpoint Protection potrafi ponadto blokować szkodliwe programy przeznaczone dla systemu Windows, chroniąc komputery Mac wchodzące w interakcje z komputerami z systemem Windows i na odwrót. Mimo iż szkodliwe oprogramowanie przygotowane dla systemu Windows nie stanowi bezpośredniego zagrożenia dla systemu Mac, dezaktywacja oprogramowania, które zaraziło komputer z systemem Mac, zapobiegnie jego rozprzestrzenianiu na komputery z systemem Windows przez sieć lokalną lub Internet.

Wymagania systemowe

Aby zapewnić optymalne działanie programu System Center Endpoint Protection, komputer powinien spełniać następujące wymagania dotyczące sprzętu i oprogramowania:

System Center Endpoint Protection:

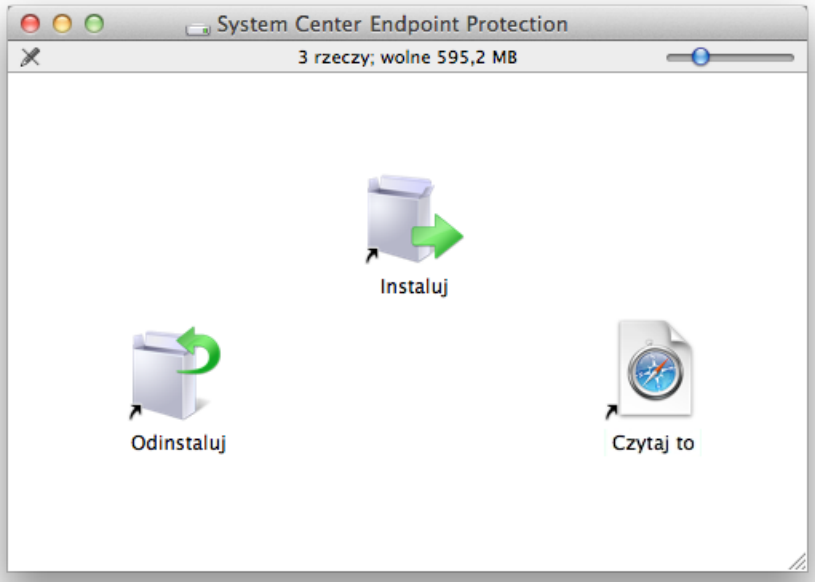
	Wymagania systemowe
Architektura procesora	32- lub 64-bitowy procesor Intel®
System operacyjny	Mac OS X 10.6 lub nowszy
Pamięć	512 MB
Wolne miejsce na dysku	100 MB

Instalacja

Przed rozpoczęciem procesu instalacji zamknij wszystkie otwarte programy. System Center Endpoint Protection zawiera komponenty, które mogą wchodzić w konflikt z innymi programami antywirusowymi zainstalowanymi na komputerze. Zaleca się usunięcie innych programów antywirusowych w celu uniknięcia potencjalnych problemów. Aby zainstalować program System Center Endpoint Protection, użyj płyty instalacyjnej CD/DVD lub pliku pobranego z naszej witryny internetowej.

Aby uruchomić kreatora instalacji, wykonaj jeden z następujących kroków:

- W przypadku instalacji z płyty instalacyjnej CD/DVD włóż płytę do napędu komputera, otwórz ją z poziomu pulpitu lub okna programu Finder i kliknij dwukrotnie ikonę **Instaluj**.
- Jeśli wykonujesz instalację za pomocą pobranego pliku, otwórz pobrany plik i kliknij dwukrotnie ikonę **Instaluj**.



Po uruchomieniu programu instalacyjnego kreator instalacji poprowadzi użytkownika przez podstawowe kroki konfiguracji. Po zaakceptowaniu Umowy licencyjnej oprogramowania i przeczytaniu Zasad zachowania poufności informacji można wybrać jeden z następujących typów instalacji:

- Typowa 4
- Zaawansowana 4

Instalacja typowa

Tryb instalacji typowej obejmuje opcje konfiguracyjne odpowiednie dla większości użytkowników. Ustawienia te stanowią najlepszy kompromis między maksymalnym bezpieczeństwem a najwyższą wydajnością. Instalacja typowa jest trybem domyślnym i zaleca się ją w przypadku, gdy użytkownik nie ma specjalnych wymagań w kwestii określonych ustawień.

Po wybraniu trybu instalacji **Typowa** skonfiguruj opcję **Wykrywanie potencjalnie niepożądanych aplikacji**. Potencjalnie niepożądane aplikacje nie są z założenia tworzone w złych intencjach, ale mogą negatywnie wpływać na działanie systemu operacyjnego. Aplikacje te są często dołączane do innych programów i mogą być trudne do zauważenia podczas instalacji. W trakcie instalowania tych aplikacji zazwyczaj wyświetlane jest powiadomienie, jednak mogą one zostać łatwo zainstalowane bez zgody użytkownika.

Po zainstalowaniu programu System Center Endpoint Protection należy przeskanować komputer w poszukiwaniu złośliwego kodu. W głównym oknie programu należy kliknąć opcję **Skanowanie komputera**, a następnie opcję **Skanowanie inteligentne**. Więcej informacji o skanowaniu komputera na żądanie można znaleźć w sekcji Skanowanie komputera na żądanie 11.

Instalacja zaawansowana

Instalacja zaawansowana jest przeznaczona dla doświadczonych użytkowników, którzy chcą modyfikować zaawansowane ustawienia podczas instalacji.

Po wybraniu trybu instalacji **Zaawansowana** pojawi się monit o wprowadzenie ustawień opcji **Serwer proxy**. Jeśli używasz serwera proxy, możesz zaznaczyć opcję **Korzystam z serwera proxy** i określić jego ustawienia. W polu **Adres** wprowadź adres IP lub URL serwera proxy. W polu Port wprowadź numer portu, na którym serwer proxy przyjmuje połączenia (domyślnie 3128). W przypadku, gdy serwer proxy wymaga uwierzytelniania, należy w polach **Nazwa użytkownika** i **Hasło** podać poprawne dane umożliwiające

dostęp do serwera. Jeśli wiadomo na pewno, że serwer proxy nie jest używany, zaznacz opcję **Nie korzystam z serwera proxy**. W razie braku pewności można użyć bieżących ustawień systemowych, zaznaczając opcję **Użyj ustawień systemowych (zalecane)**.

W następnym kroku można w oknie **Zdefiniuj uprawnionych użytkowników** wskazać użytkowników mających pozwolenie na edytowanie konfiguracji programu. Na liście użytkowników z lewej strony zaznacz żądane osoby, a następnie kliknij przycisk **Dodaj**. Osoby te zostaną dodane do listy **Użytkownicy uprzywilejowani**. Aby byli widoczni wszyscy użytkownicy zdefiniowani w systemie, zaznacz opcję **Pokaż wszystkich użytkowników**.

Następnym etapem procesu instalacji jest skonfigurowanie opcji **Wykrywanie potencjalnie niepożądanych aplikacji**. Potencjalnie niepożądane aplikacje nie są z założenia tworzone w złych intencjach, ale mogą negatywnie wpływać na działanie systemu operacyjnego. Aplikacje te są często dołączane do innych programów i mogą być trudne do zauważenia podczas instalacji. W trakcie instalowania tych aplikacji zazwyczaj wyświetlane jest powiadomienie, jednak mogą one zostać łatwo zainstalowane bez zgody użytkownika.

Po zainstalowaniu programu System Center Endpoint Protection należy przeskanować komputer w poszukiwaniu złośliwego kodu. W głównym oknie programu należy kliknąć opcję **Skanowanie komputera**, a następnie opcję **Skanowanie inteligentne**. Więcej informacji o skanowaniu komputera na żądanie można znaleźć w sekcji Skanowanie komputera na żądanie 11.

Odinstalowanie

Aby odinstalować program System Center Endpoint Protection z komputera, wykonaj jedną z następujących czynności:

- Włóż płytę instalacyjną CD/DVD z programem System Center Endpoint Protection do napędu komputera, otwórz ją z poziomu pulpitu lub okna programu Finder i kliknij dwukrotnie ikonę **Odinstaluj**.
- Otwórz plik instalacyjny programu System Center Endpoint Protection (*.dmg*) i kliknij dwukrotnie ikonę **Odinstaluj**.
- Uruchom program **Finder**, otwórz folder **Aplikacje** znajdujący się na dysku twardym komputera, naciśnij klawisz Ctrl i kliknij ikonę programu System Center Endpoint Protection, a następnie wybierz opcję **Pokaż zawartość pakietu**. Otwórz folder **Contents > Helpers** i kliknij dwukrotnie ikonę **Uninstaller**.

Przewodnik dla początkujących

Niniejszy rozdział zawiera ogólny opis programu System Center Endpoint Protection i jego podstawowych ustawień.

Interfejs użytkownika

Główne okno programu System Center Endpoint Protection jest podzielone na dwie podstawowe części. W głównym oknie z prawej strony są wyświetlane informacje dotyczące opcji zaznaczonej w menu głównym z lewej strony.

Poniżej opisano opcje dostępne w menu głównym:

- **Stan ochrony** — wyświetla informacje o stanie ochrony programu System Center Endpoint Protection. W przypadku aktywowania opcji **Tryb zaawansowany** jest wyświetlane podmenu **Statystyki**.
- **Skanowanie komputera** — pozwala skonfigurować i uruchomić funkcję Skanowanie komputera na żądanie.
- **Aktualizacja** — tutaj są wyświetlane informacje o aktualizacjach bazy sygnatur wirusów.
- **Ustawienia** — umożliwia dostosowanie poziomu zabezpieczeń komputera. W przypadku aktywowania opcji **Tryb zaawansowany** jest wyświetlane podmenu **Antywirus i antyspyware**.
- **Narzędzia** — zapewnia dostęp do modułów **Pliki dziennika**, **Kwarantanna** i **Harmonogram**. Opcja jest wyświetlana wyłącznie po aktywowaniu opcji **Tryb zaawansowany**.
- **Pomoc** — informacje o programie oraz dostęp do plików pomocy.

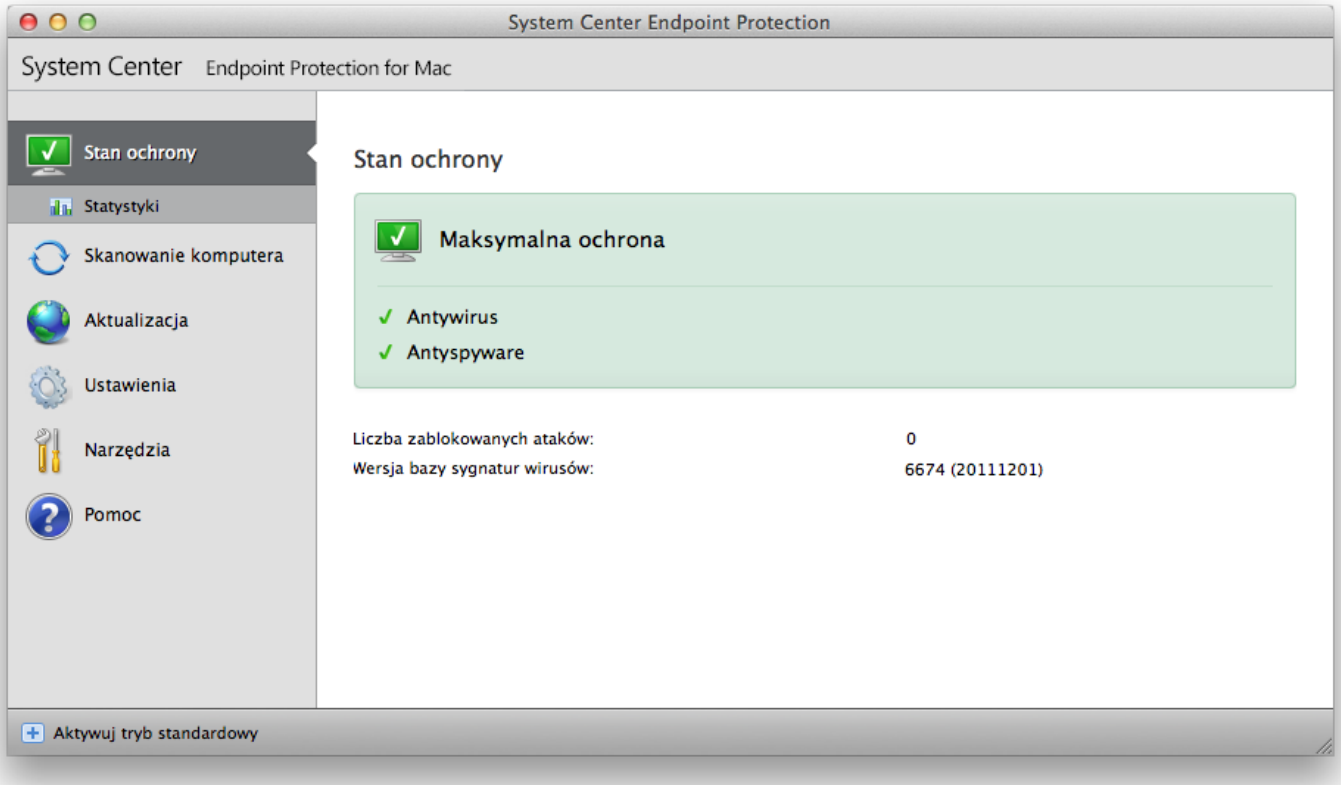
Interfejs użytkownika programu System Center Endpoint Protection pozwala na przełączanie między trybem standardowym i zaawansowanym. Tryb standardowy zapewnia dostęp do funkcji wymaganych do wykonywania typowych operacji. Żadne zaawansowane opcje nie są wyświetlane. W celu przełączenia z jednego trybu do drugiego należy kliknąć ikonę plusa (**+**) widoczną obok nagłówka **Aktywuj tryb zaawansowany**/**Aktywuj tryb standardowy** w lewym dolnym rogu głównego okna programu lub nacisnąć kombinację klawiszy cmd+M.

Przełączenie do trybu zaawansowanego powoduje dodanie do menu głównego opcji **Narzędzia**. Opcja **Narzędzia** umożliwia dostęp do podmenu modułów **Pliki dziennika**, **Kwarantanna** i **Harmonogram**.

UWAGA: Wszystkie pozostałe instrukcje w niniejszym podręczniku dotyczą **trybu zaawansowanego**.

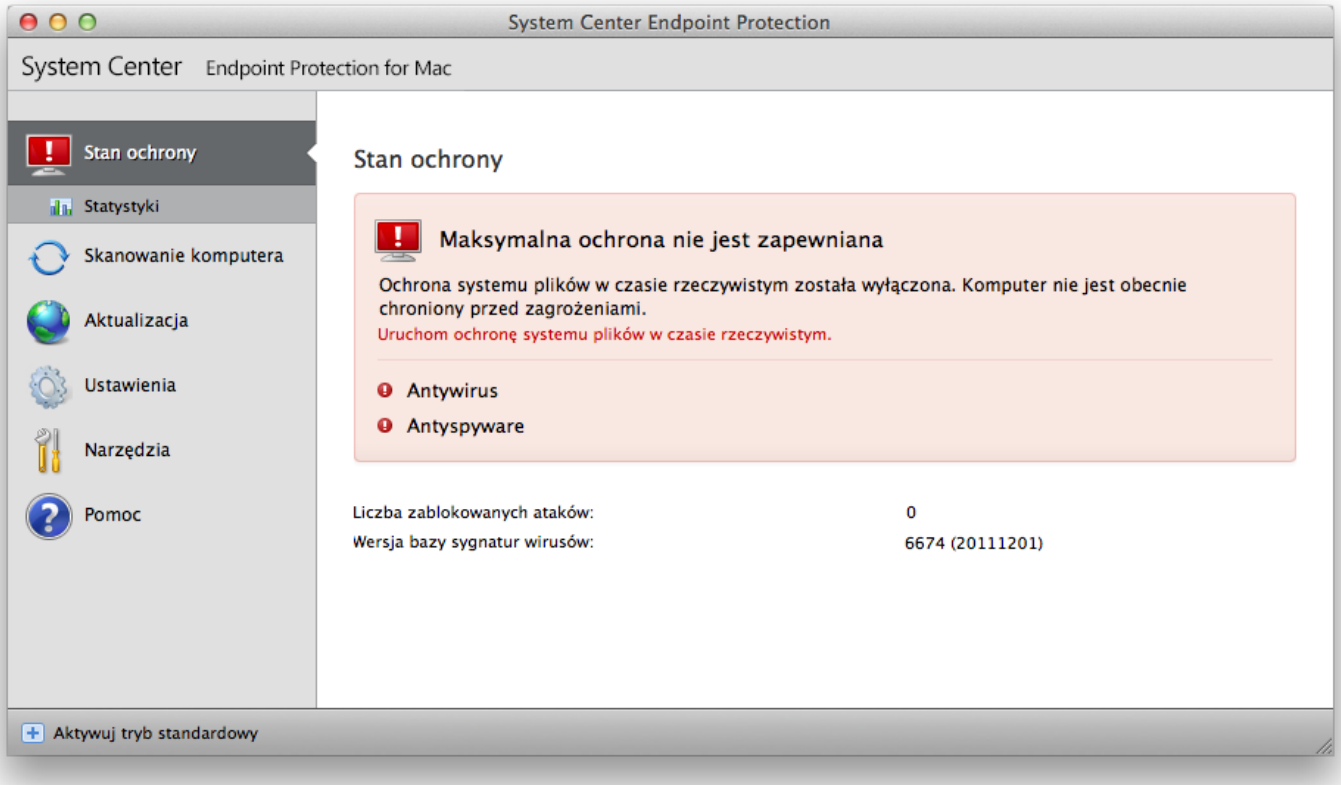
Sprawdzanie działania systemu

Aby wyświetlić okno **Stan ochrony**, należy kliknąć górną opcję w menu głównym. W głównym oknie zostanie wyświetlone podsumowanie stanu informujące o działaniu programu System Center Endpoint Protection. Pojawi się także podmenu z opcją **Statystyki**. Po kliknięciu tej opcji można obejrzeć dokładniejsze informacje i statystyki dotyczące operacji skanowania komputera wykonanych w danym systemie. Okno Statystyki jest dostępne wyłącznie w trybie zaawansowanym.



Postępowanie w przypadku, gdy program nie działa poprawnie

Jeśli włączone moduły działają poprawnie, są oznaczone zieloną ikoną znacznika wyboru. W przeciwnym razie jest wyświetlana czerwona ikona wykrzyknika lub pomarańczowa ikona powiadomienia, a w górnej części okna pojawiają się dodatkowe informacje dotyczące modułu. Wyświetlany jest również proponowany sposób przywrócenia działania modułu. Aby zmienić stan poszczególnych modułów, w menu głównym należy kliknąć opcję **Ustawienia**, a następnie kliknąć wybrany moduł.



Praca z programem System Center Endpoint Protection

Ochrona antywirusowa i antyspyware

Ochrona antywirusowa zabezpiecza system przed złośliwymi atakami, modyfikując potencjalnie niebezpieczne pliki. W przypadku wykrycia zagrożenia zawierającego złośliwy kod moduł antywirusowy może je wyeliminować przez zablokowanie, a następnie wyleczyć, usunąć lub przenieść do kwarantanny.

Ochrona systemu plików w czasie rzeczywistym

Ochrona systemu plików w czasie rzeczywistym zapewnia kontrolę nad wszystkimi zdarzeniami związanymi z ochroną antywirusową systemu. Wszystkie pliki w momencie otwarcia, utworzenia lub uruchomienia na komputerze są skanowane w poszukiwaniu złośliwego kodu. Ochrona systemu plików w czasie rzeczywistym jest włączana przy uruchamianiu systemu.

Ustawienia ochrony w czasie rzeczywistym

Funkcja ochrony systemu plików w czasie rzeczywistym sprawdza wszystkie typy nośników i wywołuje skanowanie po wystąpieniu różnych zdarzeń. Działanie tej funkcji może się różnić w odniesieniu do nowo tworzonych i istniejących plików. W przypadku nowo tworzonych plików można stosować głębszy poziom sprawdzania.

Ochrona w czasie rzeczywistym jest domyślnie włączana przy uruchamianiu systemu i zapewnia nieprzerwane skanowanie. W szczególnych przypadkach (np. jeśli wystąpi konflikt z innym skanerem działającym w czasie rzeczywistym) ochronę w czasie rzeczywistym można wyłączyć, klikając ikonę System Center Endpoint Protection dostępną na pasku menu (u góry ekranu), a następnie zaznaczając opcję **Wyłącz ochronę systemu plików w czasie rzeczywistym**. Ochrona w czasie rzeczywistym może również zostać wyłączona w oknie głównym programu (**Ustawienia** > **Antywirus i antyspyware** > **Wyłącz**).

Aby zmodyfikować zaawansowane ustawienia ochrony w czasie rzeczywistym, należy przejść do opcji **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ochrona** > **Ochrona w czasie rzeczywistym** i kliknąć przycisk **Ustawienia...** umieszczony obok pozycji **Opcje zaawansowane** (opisano to w sekcji Zaawansowane opcje skanowania 9).

Skanowanie po wystąpieniu zdarzenia

Domyślnie wystąpienie następujących zdarzeń powoduje skanowanie każdego pliku: **Otwieranie pliku**, **Tworzenie pliku** oraz **Wykonywanie pliku**. Zaleca się zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalny poziom ochrony komputera w czasie rzeczywistym.

Zaawansowane opcje skanowania

W tym oknie można wskazać typy obiektów, które mają być skanowane przez aparat skanowania, włączyć lub wyłączyć funkcję **Zaawansowana heurystyka**, a także zmodyfikować ustawienia archiwizacji i pamięci podręcznej plików.

Nie zaleca się zmieniania domyślnych wartości w części **Domyślne ustawienia archiwów**, chyba że jest to niezbędne do rozwiązania konkretnego problemu, ponieważ większa liczba poziomów zagnieżdżania archiwów może spowodować obniżenie wydajności systemu.

Funkcję skanowania z wykorzystaniem zaawansowanej heurystyki można włączać osobno dla plików uruchamianych, nowo tworzonych i modyfikowanych. W tym celu należy zaznaczyć pole wyboru **Zaawansowana heurystyka** w odpowiednich sekcjach parametrów technologii.

Aby zminimalizować obciążenie systemu podczas korzystania z ochrony w czasie rzeczywistym, można ustawić rozmiar pamięci podręcznej optymalizacji. Funkcja ta jest dostępna w przypadku korzystania z opcji **Włącz pamięć podręczną leczenia plików**. Po jej wyłączeniu wszystkie pliki są skanowane za każdym razem, gdy uzyskuje się do nich dostęp. Po umieszczeniu w pamięci podręcznej zeskanowane pliki nie będą ponownie skanowane (chyba że ulegną modyfikacji), aż do osiągnięcia zdefiniowanego rozmiaru pamięci podręcznej. Pliki są niezwłocznie skanowane ponownie po każdej aktualizacji bazy sygnatur wirusów.

Aby włączyć lub wyłączyć tę funkcję, należy kliknąć opcję **Włącz pamięć podręczną leczenia plików**. W celu określenia liczby plików, jakie można umieścić w pamięci podręcznej, wystarczy wprowadzić żądaną wartość w polu **Rozmiar pamięci podręcznej**.

Dodatkowe parametry skanowania można skonfigurować w oknie **Ustawienia technologii**. W części **Obiekty** można wskazać obiekty, które mają być skanowane. W części **Opcje** można wybrać opcje skanowania, a w części **Poziom leczenia** — zakres leczenia plików. Można także określić typy (część **Rozszerzenia**) i rozmiar (część **Limity**) plików skanowanych przez funkcję ochrony systemu plików w czasie rzeczywistym. Aby przejść do okna ustawień technologii, należy kliknąć przycisk **Ustawienia...** widoczny obok nagłówka **Technologia** w oknie Ustawienia zaawansowane. Więcej informacji o parametrach technologii można znaleźć w sekcji Ustawienia parametrów technologii 14.

Wyłączenia ze skanowania

W tej części można wyłączyć ze skanowania wybrane pliki i foldery.

- **Ścieżka** — ścieżka do wyłączonych plików i folderów.
- **Zagrożenie** — gdy obok wyłączonego pliku widać nazwę zagrożenia, oznacza to, że plik będzie pomijany tylko przy wyszukiwaniu tego zagrożenia, a nie całkowicie. W związku z tym, jeśli później plik zostanie zarażony innym szkodliwym oprogramowaniem, moduł antywirusowy go wykryje.
- **Dodaj...** — pozwala dodać obiekty, które mają być pomijane podczas wykrywania. Należy wprowadzić ścieżkę do obiektu (można używać symboli wieloznacznych *i ?) albo zaznaczyć folder lub plik w strukturze drzewa.
- **Edytuj...** — pozwala zmodyfikować zaznaczone elementy.
- **Usuń** — służy do usuwania zaznaczonych elementów.
- **Domyślne** — anuluje wszystkie wyłączenia.

Modyfikowanie ustawień ochrony w czasie rzeczywistym

Ochrona w czasie rzeczywistym jest najbardziej istotnym elementem zapewniającym bezpieczeństwo systemu. Dlatego modyfikowanie parametrów tej funkcji należy przeprowadzać z dużą ostrożnością. Zmienianie ustawień ochrony jest zalecane tylko w określonych przypadkach, na przykład jeśli występuje konflikt z określoną aplikacją lub działającym w czasie rzeczywistym skanerem należącym do innego programu antywirusowego.

Po zainstalowaniu programu System Center Endpoint Protection wszystkie ustawienia są optymalizowane w celu zapewnienia maksymalnego poziomu bezpieczeństwa systemu. Aby przywrócić ustawienia domyślne, należy kliknąć przycisk **Domyślne** znajdujący się w prawej dolnej części okna **Ochrona w czasie rzeczywistym** (otwieranego po wybraniu kolejno opcji **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ochrona** > **Ochrona w czasie rzeczywistym**).

Sprawdzanie skuteczności ochrony w czasie rzeczywistym

Aby sprawdzić, czy funkcja ochrony w czasie rzeczywistym działa i wykrywa wirusy, należy użyć pliku testowego eicar.com. Jest to specjalny nieszkodliwy plik wykrywany przez wszystkie programy antywirusowe. Został on utworzony przez instytut EICAR (ang. European Institute for Computer Antivirus Research) w celu testowania działania programów antywirusowych.

Aby sprawdzić stan ochrony w czasie rzeczywistym, należy podłączyć komputer kliencki za pomocą okna **Terminal** i wykonać następujące polecenie:
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

Stan skanera działającego w czasie rzeczywistym zostanie wyświetlony jako `RTPStatus=Enabled` lub `RTPStatus=Disabled`.

Dane wynikowe polecenia BASH w oknie Terminal obejmują również następujące informacje:

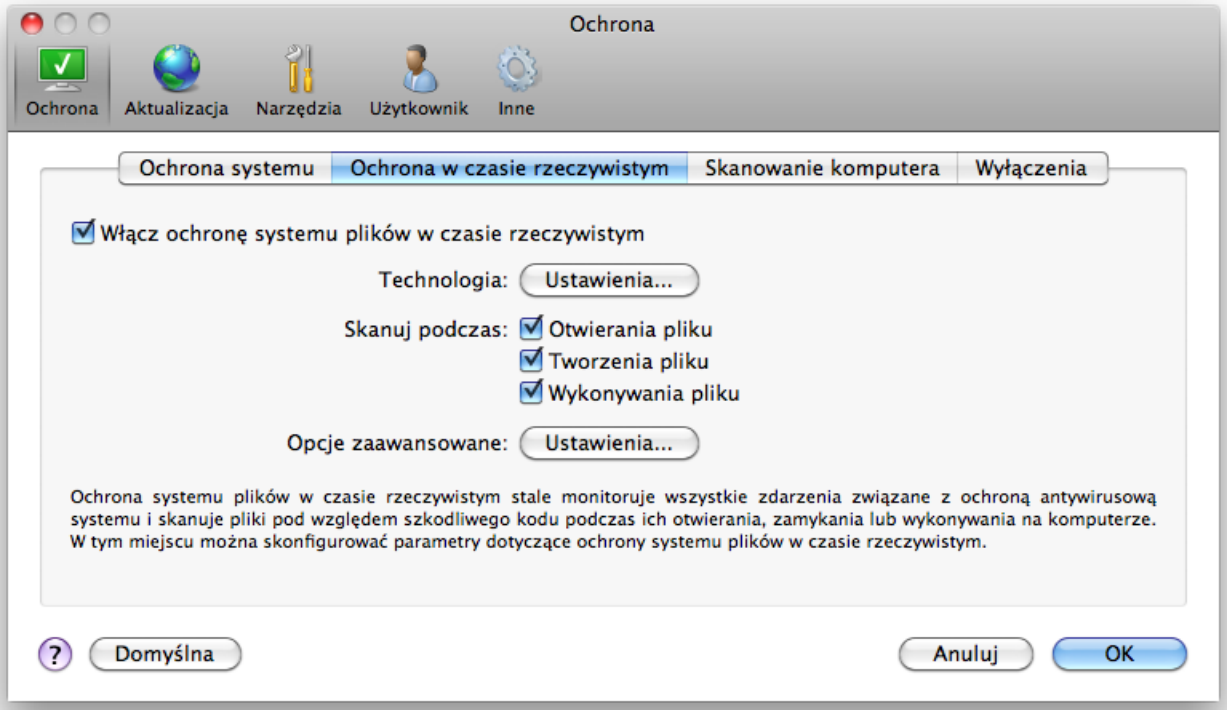
- wersja programu System Center Endpoint Protection zainstalowanego na komputerze klienckim
- data i wersja bazy sygnatur wirusów
- ścieżka do serwera aktualizacji

UWAGA: Korzystanie z okna Terminal jest zalecane wyłącznie w przypadku użytkowników zaawansowanych.

Co należy zrobić, jeśli ochrona w czasie rzeczywistym nie działa

W tym rozdziale opisano problemy, które mogą wystąpić podczas korzystania z ochrony w czasie rzeczywistym, oraz sposoby ich rozwiązywania.

Ochrona w czasie rzeczywistym jest wyłączona
Jeśli ochrona w czasie rzeczywistym została przypadkowo wyłączona przez użytkownika, należy ją włączyć ponownie. Aby ponownie aktywować ochronę w czasie rzeczywistym, w głównym oknie programu należy wybrać kolejno opcje **Ustawienia** > **Antywirus i antyspyware**, a następnie kliknąć łącze **Włącz ochronę systemu plików w czasie rzeczywistym** (z prawej strony). Ochronę systemu plików w czasie rzeczywistym można też włączyć w oknie Ustawienia zaawansowane (otwieranym po wybraniu kolejno opcji **Ochrona** > **Ochrona w czasie rzeczywistym**), zaznaczając pole wyboru **Włącz ochronę systemu plików w czasie rzeczywistym**.



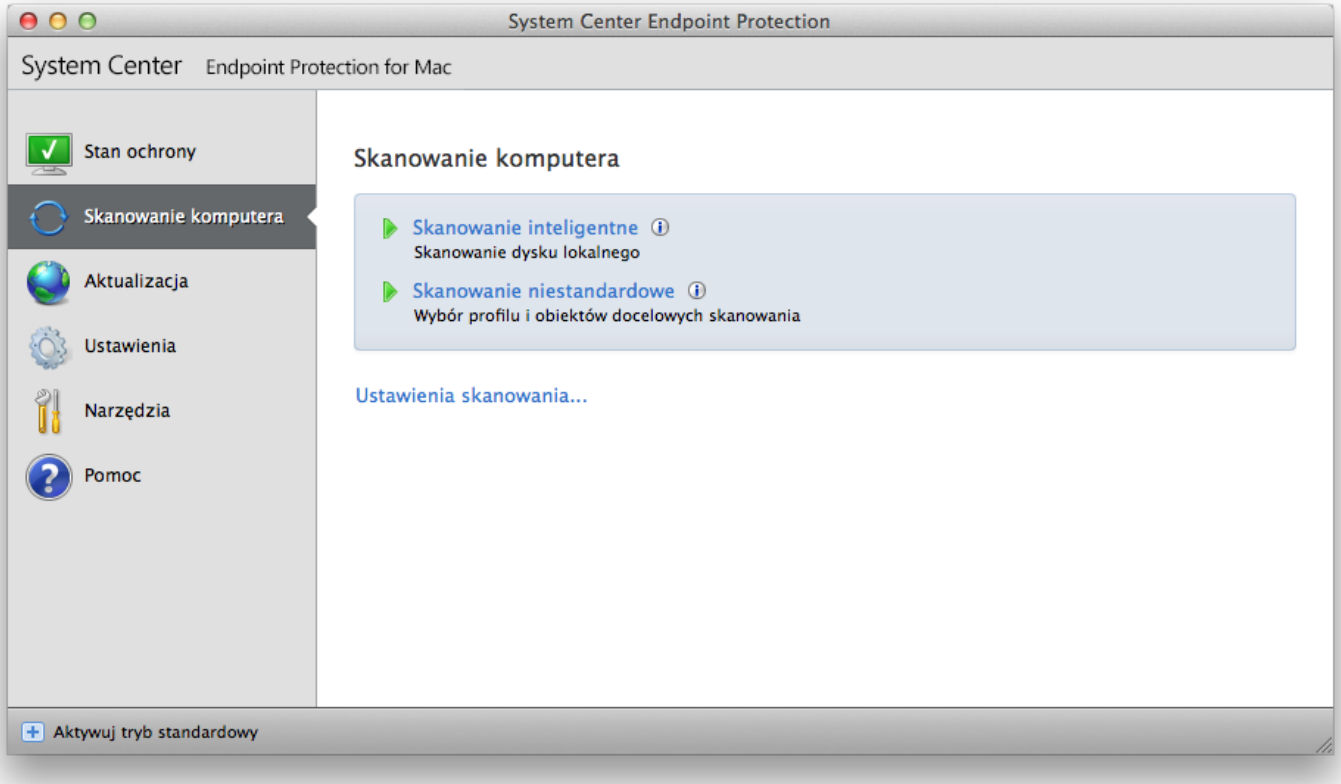
Ochrona w czasie rzeczywistym nie wykrywa ani nie leczy infekcji
Należy się upewnić, że na komputerze nie ma zainstalowanych innych programów antywirusowych. Jednoczesne włączenie dwóch modułów ochrony w czasie rzeczywistym może powodować ich konflikt. Zaleca się odinstalowanie innych programów antywirusowych znajdujących się w systemie.

Ochrona w czasie rzeczywistym nie jest uruchamiana
Jeśli funkcja ochrony w czasie rzeczywistym nie jest inicjowana podczas uruchamiania systemu, być może jest to spowodowane konfliktami z innymi programami. W takim przypadku należy skonsultować się z Działem obsługi klienta.

Skanowanie komputera na żądanie

Jeśli istnieje podejrzenie, że komputer jest zarażony (działa w sposób nieprawidłowy), należy wybrać kolejno opcje **Skanowanie komputera** > **Skanowanie inteligentne** w celu sprawdzenia komputera w poszukiwaniu infekcji. Aby zapewnić maksymalny poziom bezpieczeństwa, skanowanie komputera powinno być uruchamiane regularnie w ramach rutynowych działań związanych z bezpieczeństwem, a nie tylko w przypadku podejrzenia wystąpienia infekcji. Regularne skanowanie umożliwia wykrywanie zagrożeń, które podczas zapisywania zarażonych plików na dysku nie zostały wykryte przez skaner działający w czasie rzeczywistym. Jest to możliwe, jeśli w momencie wystąpienia infekcji skaner działający w czasie rzeczywistym był wyłączony lub baza sygnatur wirusów była nieaktualna.

Zaleca się uruchamianie skanowania komputera na żądanie co najmniej raz w miesiącu. Skanowanie można skonfigurować jako zaplanowane zadanie za pomocą opcji **Narzędzia** > **Harmonogram**.



Można również przeciągnąć wybrane pliki i foldery z pulpitu lub okna programu Finder i upuścić je na głównym ekranie programu System Center Endpoint Protection, na ikonie doku, ikonie paska menu (w górnej części ekranu) lub ikonie aplikacji (znajdującej się w folderze */Aplikacje*).

Typ skanowania

Dostępne są dwa typy skanowania komputera na żądanie. Opcja **Skanowanie inteligentne** umożliwia szybkie przeskanowanie systemu bez konieczności dodatkowego konfigurowania parametrów skanowania. **Skanowanie niestandardowe** umożliwia wybranie jednego ze wstępnie zdefiniowanych profilów skanowania oraz określenie obiektów skanowania.

Skanowanie inteligentne

Tryb skanowania inteligentnego umożliwia szybkie uruchomienie skanowania komputera i wyleczenie zarażonych plików bez konieczności podejmowania dodatkowych działań przez użytkownika. Jego główną zaletą jest łatwa obsługa i brak szczegółowej konfiguracji skanowania. W ramach skanowania inteligentnego sprawdzane są wszystkie pliki we wszystkich folderach, a wykryte infekcje są automatycznie leczone lub usuwane. Automatycznie ustawiany jest też domyślny poziom leczenia. Szczegółowe informacje na temat typów leczenia można znaleźć w sekcji Leczenie 15.

Skanowanie niestandardowe

Skanowanie niestandardowe stanowi optymalne rozwiązanie, jeśli użytkownik chce określić parametry skanowania, takie jak skanowane obiekty i metody skanowania. Zaletą skanowania niestandardowego jest możliwość szczegółowej konfiguracji parametrów. Konfiguracje można zapisywać w zdefiniowanych przez użytkownika profilach skanowania, które mogą być przydatne, jeśli skanowanie jest wykonywane wielokrotnie z zastosowaniem tych samych parametrów.

Aby wybrać skanowane obiekty, należy użyć opcji **Skanowanie komputera** > **Skanowanie niestandardowe**, a następnie zaznaczyć określone **Skanowane obiekty** w strukturze drzewa. Obiekty do skanowania można również wskazać bardziej precyzyjnie, wprowadzając ścieżkę do folderu lub plików, które mają zostać objęte skanowaniem. Jeśli użytkownik chce tylko przeskanować system bez wykonywania dodatkowych czynności związanych z leczeniem, należy wybrać opcję **Skanuj bez leczenia**. Ponadto można wybrać jeden z trzech poziomów leczenia, klikając kolejno opcje **Ustawienia...** > **Leczenie**.

Skanowanie komputera w trybie skanowania niestandardowego jest przeznaczone dla zaawansowanych użytkowników, którzy mają już doświadczenie w posługiwaniu się programami antywirusowymi.

Skanowane obiekty

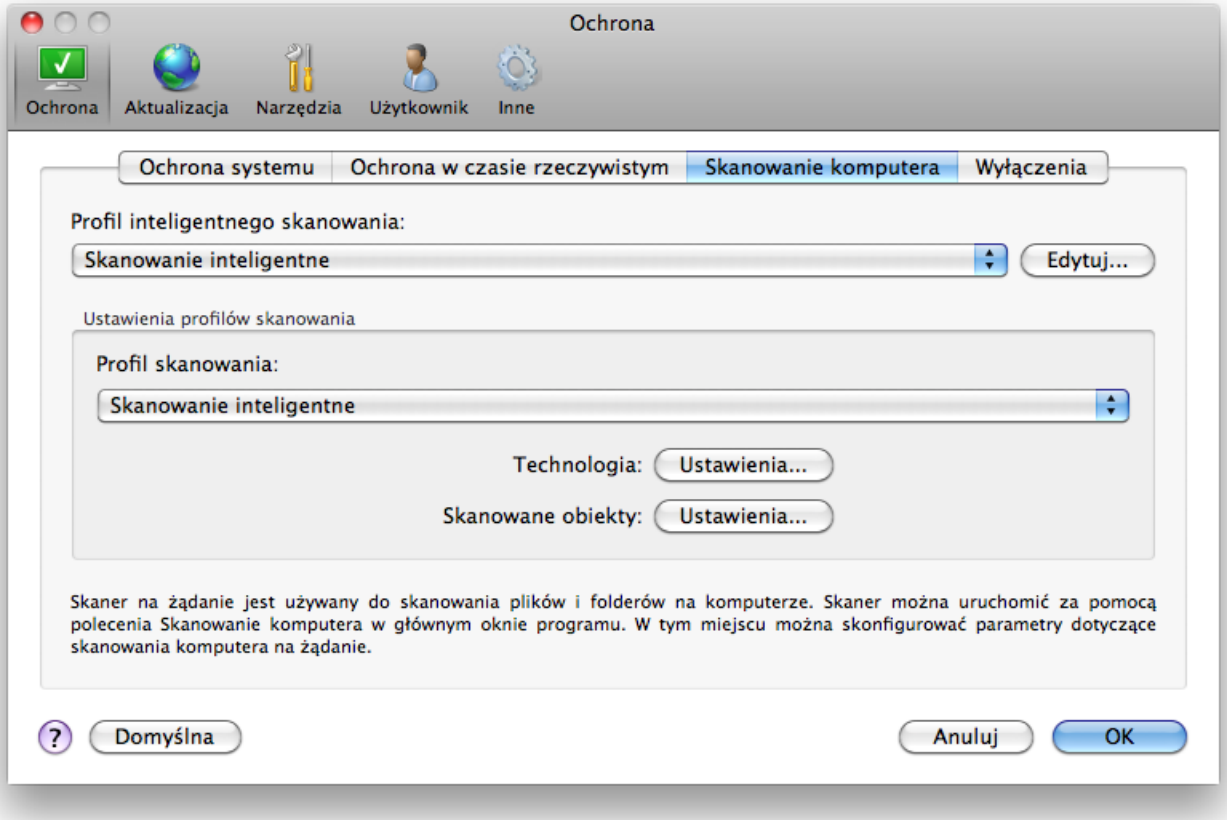
Struktura drzewa skanowanych obiektów umożliwia wybór plików i folderów, które mają być skanowane w poszukiwaniu wirusów. Foldery mogą również zostać zaznaczone zgodnie z ustawieniami profilu.

Skanowany obiekt można również dokładniej określić, wprowadzając ścieżkę do folderu lub plików, które mają zostać objęte skanowaniem. Skanowane obiekty można wybrać w strukturze drzewa zawierającej wszystkie foldery dostępne na komputerze.

Profile skanowania

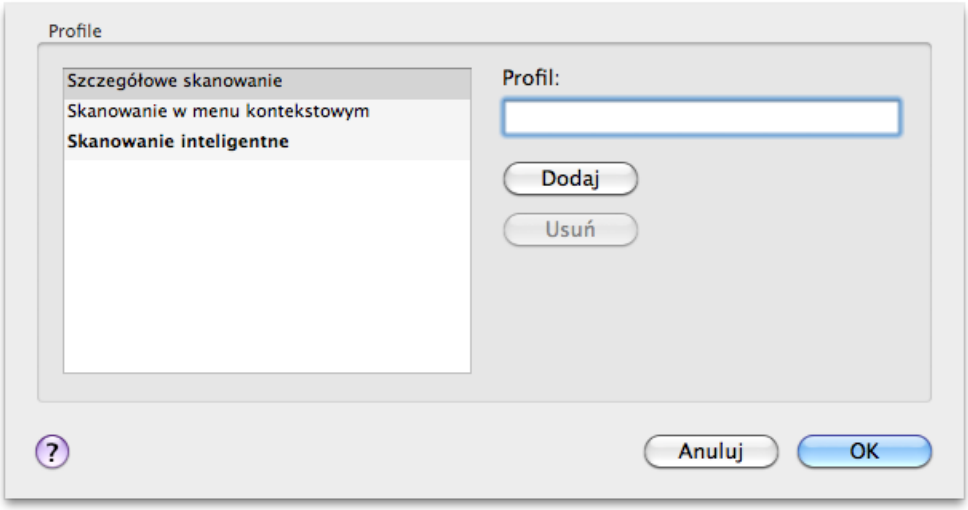
Preferowane ustawienia skanowania mogą zostać zapisane i użyte w przyszłości. Zalecane jest utworzenie osobnego profilu (z ustawionymi różnymi obiektami i metodami skanowania oraz innymi parametrami) dla każdego regularnie przeprowadzanego skanowania.

Aby utworzyć nowy profil, należy przejść do opcji **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ochrona** > **Skanowanie komputera** i kliknąć przycisk **Edytuj...** obok listy bieżących profilów.



Informacje na temat tworzenia profilu skanowania dostosowanego do indywidualnych potrzeb można znaleźć w sekcji Ustawienia parametrów technologii 14, w której opisano poszczególne parametry ustawień skanowania.

Przykład: załóżmy, że użytkownik chce utworzyć własny profil skanowania, a żądana konfiguracja częściowo pokrywa się z konfiguracją w profilu Skanowanie inteligentne. Użytkownik nie chce jednak skanować plików spakowanych lub potencjalnie niebezpiecznych aplikacji oraz chce zastosować poziom leczenia Leczenie dokładne. W oknie **Lista profilów skanera na żądanie** należy wpisać nazwę profilu, kliknąć przycisk **Dodaj** i potwierdzić, klikając przycisk **OK**. Następnie należy dostosować parametry do własnych potrzeb, konfigurując opcje **Technologia** oraz **Skanowane obiekty**.



Ustawienia parametrów technologii

Technologia skanowania używana w programie System Center Endpoint Protection działa w sposób proaktywny, co oznacza, że zapewnia ochronę już od pierwszych godzin rozprzestrzeniania się nowego zagrożenia. Stosowana jest w niej kombinacja kilku metod (analiza kodu, emulacja kodu, sygnatury rodzajowe, sygnatury wirusów), które razem znacznie zwiększają bezpieczeństwo systemu. Technologia skanowania może kontrolować kilka strumieni danych jednocześnie, co zwiększa do maksimum skuteczność i wskaźnik wykrywalności. Ponadto technologia ta skutecznie chroni przed programami typu rootkit.

Za pomocą ustawień technologii można określić kilka parametrów skanowania:
- typy i rozszerzenia plików, które mają być skanowane;
- kombinacje różnych metod wykrywania;
- poziomy leczenia itp.

Aby otworzyć okno konfiguracji, należy wybrać kolejno opcje **Ustawienia** > **Antywirus i antyspyware** > **Zaawansowane ustawienia ochrony antywirusowej i antyspyware**, a następnie kliknąć przycisk **Ustawienia...** umieszczony na kartach funkcji **Ochrona systemu**, **Ochrona w czasie rzeczywistym** i **Skanowanie komputera**. Różne scenariusze zabezpieczeń mogą wymagać różnych konfiguracji. Parametry technologii można więc konfigurować indywidualnie dla następujących modułów ochrony:
- **Ochrona systemu** > Automatyczne sprawdzanie plików wykonywanych podczas uruchamiania
- **Ochrona w czasie rzeczywistym** > Ochrona systemu plików w czasie rzeczywistym
- **Skanowanie komputera** > Skanowanie komputera na żądanie

Parametry technologii są specjalnie zoptymalizowane dla poszczególnych modułów i ich modyfikacja może znacząco wpłynąć na działanie systemu. Na przykład ustawienie opcji każdorazowego skanowania programów spakowanych lub włączenie zaawansowanej heurystyki w module ochrony systemu plików w czasie rzeczywistym może powodować spowolnienie działania systemu. Dlatego zalecane jest pozostawienie niezmienionych parametrów domyślnych technologii dla wszystkich skanerów z wyjątkiem modułu Skanowanie komputera.

Obiekty

Część **Obiekty** pozwala określić, które pliki komputera będą skanowane w poszukiwaniu infekcji.

- **Pliki** — skanowane są najczęściej używane typy plików (programy, obrazy, pliki audio, pliki wideo, pliki baz danych itd.).
- **Łącza symboliczne** — (tylko skaner na żądanie) skanowane są specjalne typy plików zawierających ciąg tekstowy interpretowany i otwierany przez system operacyjny jako ścieżka do innego pliku lub katalogu.
- **Pliki poczty** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są specjalne pliki zawierające wiadomości e-mail.
- **Skrzynki pocztowe** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są skrzynki pocztowe użytkowników znajdujące się w systemie. Niewłaściwe stosowanie tej opcji może prowadzić do konfliktu z używanym programem poczty e-mail.
- **Archiwa** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki skompresowane w archiwach (. rar, .zip, .arj, .tar itd.).
- **Archiwa samorozpakowujące** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki znajdujące się w archiwach samorozpakowujących.
- **Pliki spakowane** — oprócz standardowych statycznych spakowanych plików skanowane są pliki, które (inaczej niż w przypadku standardowych typów archiwów) są rozpakowywane w pamięci (UPX, yoda, ASPack, FGS itp.).

Opcje

W części **Opcje** można wybrać metody, które mają być stosowane podczas skanowania systemu w poszukiwaniu infekcji. Dostępne są następujące opcje:

- **Heurystyka** — heurystyka wykorzystuje algorytm analizujący szkodliwe działania podejmowane przez programy. Główną zaletą heurystyki jest możliwość wykrywania nowego złośliwego oprogramowania, które wcześniej nie istniało lub nie zostało umieszczone na liście znanych wirusów (w bazie sygnatur wirusów).
- **Zaawansowana heurystyka** — zaawansowana heurystyka jest oparta na unikatowym algorytmie heurystycznym. Został on zoptymalizowany pod kątem wykrywania robaków i koni trojańskich napisanych w językach programowania wysokiego poziomu. Zaawansowana heurystyka znacznie zwiększa możliwości programu w zakresie wykrywania zagrożeń.
- **Potencjalnie niepożądane aplikacje** — nie muszą one być tworzone w złych intencjach, ale mogą negatywnie wpływać na wydajność komputera. Zainstalowanie takiej aplikacji zazwyczaj wymaga zgody użytkownika. Po zainstalowaniu tego rodzaju programu działanie systemu zmienia się w porównaniu z wcześniejszym stanem. Najbardziej widoczne zmiany to wyświetlanie wyskakujących okienek, aktywowanie i uruchamianie ukrytych procesów, zwiększone użycie zasobów systemowych, zmiany w wynikach wyszukiwania oraz komunikowanie się aplikacji ze zdalnymi serwerami.
- **Potencjalnie niebezpieczne aplikacje** — do aplikacji tych zaliczane są niektóre legalne programy komercyjne, które mogą zostać wykorzystane przez intruzów do prowadzenia niebezpiecznych działań, jeśli zostały zainstalowane bez wiedzy użytkownika. Są to między innymi narzędzia do dostępu zdalnego, dlatego ta opcja jest domyślnie wyłączona.

Leczenie

Ustawienia leczenia określają sposób czyszczenia zarażonych plików przez skaner. Dostępne są 3 poziomy leczenia:

- **Brak leczenia** — zarażone pliki nie są automatycznie leczone. Wyświetlane jest okno z ostrzeżeniem, a użytkownik może wybrać czynność do wykonania.
- **Leczenie standardowe** — program próbuje automatycznie wyleczyć lub usunąć zarażony plik. Jeśli automatyczny wybór właściwej czynności nie jest możliwy, program umożliwia wybranie dostępnej czynności. Dostępne czynności są wyświetlane również wtedy, gdy wykonanie wstępnie zdefiniowanej czynności nie jest możliwe.
- **Leczenie dokładne** — program leczy lub usuwa wszystkie zarażone pliki (w tym archiwa). Jedyny wyjątek stanowią pliki systemowe. Jeśli ich wyleczenie nie jest możliwe, użytkownik jest monitowany o wybranie odpowiedniej czynności w oknie z ostrzeżeniem.

Ostrzeżenie: W domyślnym trybie Leczenie standardowe cały plik archiwum jest usuwany tylko wtedy, gdy wszystkie pliki w archiwum są zarażone. Jeśli zawiera również niezarażone pliki, nie jest usuwany. Jeśli zarażony plik archiwum zostanie wykryty w trybie Leczenie dokładne, od razu usuwane jest całe archiwum, nawet jeśli zawiera również niezarażone pliki.

Rozszerzenia

Rozszerzenie jest częścią nazwy pliku oddzieloną kropką. Określa ono typ i zawartość pliku. Ta część ustawień parametrów technologii umożliwia określanie typów plików, które mają być wyłączone ze skanowania.

Domyślnie skanowane są wszystkie pliki niezależnie od rozszerzenia. Do listy plików wyłączonych ze skanowania można dodać dowolne rozszerzenie. Przy użyciu przycisków **Dodaj** i **Usuń** można włączyć lub wyłączyć skanowanie określonych rozszerzeń.

Wyłączenie plików ze skanowania jest czasami konieczne, jeśli skanowanie pewnych typów plików uniemożliwia prawidłowe działanie programu. Na przykład wskazane może być wykluczenie rozszerzeń *.log*, *.cfg* i *.tmp*.

Limity

W części **Limity** można określić maksymalny rozmiar obiektów i poziomy zagnieżdżenia archiwów, które mają być skanowane:

- **Maksymalny rozmiar:** Określa maksymalny rozmiar obiektów do skanowania. Moduł antywirusowy będzie skanować tylko obiekty o rozmiarze mniejszym niż określony. Nie zaleca się zmieniania wartości domyślnej, ponieważ zazwyczaj nie ma ku temu powodu. Do modyfikowania tej opcji powinni przystępować tylko zaawansowani użytkownicy, mający określone powody do wyłączenia większych obiektów ze skanowania.
- **Maksymalny czas skanowania:** Określa maksymalny czas przyznany na skanowanie obiektu. Jeśli użytkownik określi taką wartość, moduł antywirusowy zatrzyma skanowanie danego obiektu po upływie tego czasu niezależnie od tego, czy skanowanie zostało zakończone.
- **Maksymalny poziom zagnieżdżania:** Określa maksymalną głębokość skanowania archiwów. Nie zaleca się zmieniania wartości domyślnej (równej 10); w normalnych warunkach nie powinno być powodów do jej modyfikacji. Jeśli skanowanie zostanie przedwcześnie zakończone z powodu liczby zagnieżdżonych archiwów, archiwum pozostanie niesprawdzone.
- **Maksymalny rozmiar pliku:** Opcja ta pozwala określić maksymalny rozmiar plików znajdujących się w archiwach (po ich rozpakowaniu), które mają być skanowane. Jeśli wskutek narzucenia tego limitu skanowanie zostanie przedwcześnie zakończone, archiwum pozostanie niesprawdzone.

Inne

Po włączeniu opcji Inteligentna optymalizacja używane są optymalne ustawienia, zapewniające połączenie maksymalnej skuteczności z największą szybkością skanowania. Poszczególne moduły ochrony działają w sposób inteligentny, stosując różne metody skanowania do konkretnych typów plików. Funkcja inteligentnej optymalizacji dostępna w produkcie nie ma ostatecznej postaci. Nasi programiści stale wprowadzają zmiany, które są następnie integrowane z programem System Center Endpoint Protection za pomocą regularnych aktualizacji. Jeśli opcja Inteligentna optymalizacja jest wyłączona, podczas skanowania są wykorzystywane jedynie ustawienia określone przez użytkownika w aparacie danego modułu.

Skanuj alternatywny strumień danych (tylko skaner na żądanie)
Alternatywne strumienie danych (rozwidlenia zasobów/danych) używane w systemie plików to skojarzenia plików i folderów, których nie można sprawdzić za pomocą standardowych technik skanowania. Wiele infekcji stara się uniknąć wykrycia, udając alternatywne strumienie danych.

Wykrycie infekcji

Infekcje mogą przedostawać się do systemu różnymi drogami, np. za pośrednictwem: stron internetowych, folderów udostępnionych, poczty e-mail lub wymiennych urządzeń komputerowych (USB, dysków zewnętrznych, dysków CD i DVD, dyskietek itd.).

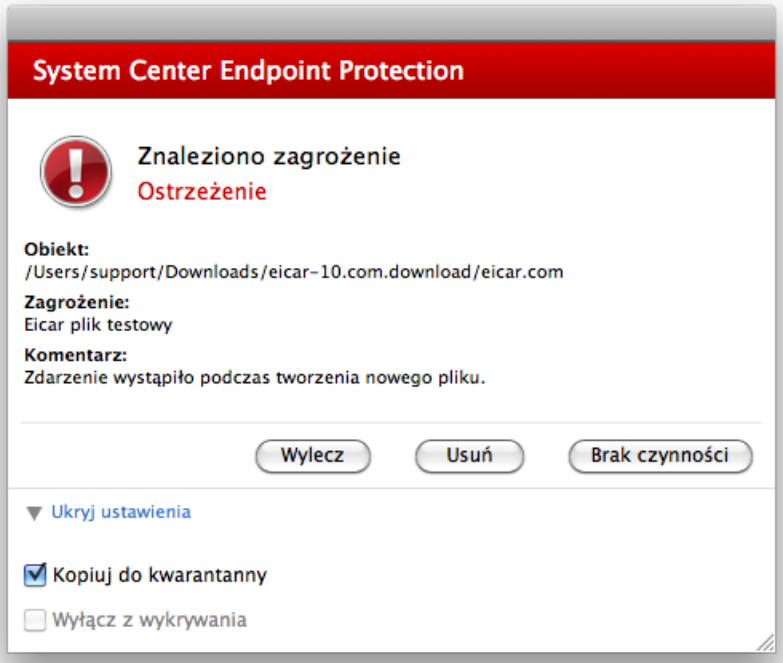
Jeśli komputer wykazuje symptomy zarażenia szkodliwym oprogramowaniem, np. działa wolniej lub często przestaje odpowiadać, zaleca się wykonanie następujących czynności:

1. Uruchom program System Center Endpoint Protection i kliknij opcję **Skanowanie komputera**.
2. Kliknij opcję **Skanowanie inteligentne** (więcej informacji znajduje się w sekcji Skanowanie inteligentne 12).
3. Po zakończeniu skanowania przejrzyj dziennik, aby sprawdzić liczbę przeskanowanych, zarażonych i wyleczonych plików.

Aby przeskanować tylko określoną część dysku, kliknij opcję **Skanowanie niestandardowe** i wybierz obiekty, które mają zostać przeskanowane w poszukiwaniu wirusów.

Ogólnym przykładem sposobu działania programu System Center Endpoint Protection w momencie infekcji może być sytuacja, w której infekcja zostaje wykryta przez działający w czasie rzeczywistym monitor systemu plików z ustawionym domyślnym poziomem leczenia. Następuje wtedy próba wyleczenia lub usunięcia pliku. W przypadku braku wstępnie zdefiniowanej czynności, którą ma wykonywać moduł ochrony w czasie rzeczywistym, zostanie wyświetlony monit o wybranie opcji w oknie alertu. Zazwyczaj dostępne są opcje **Wylecz**, **Usuń** i **Brak czynności**. Nie zaleca się wybierania opcji **Brak czynności**, ponieważ powoduje to pozostawienie zarażonych plików bez zmian. Jedyny wyjątek stanowi sytuacja, w której użytkownik ma pewność, że dany plik jest nieszkodliwy i został błędnie wykryty.

Leczenie i usuwanie — leczenie należy stosować w przypadku zarażonego pliku, do którego wirus dołączył złośliwy kod. Należy najpierw podjąć próbę wyleczenia zarażonego pliku w celu przywrócenia go do stanu pierwotnego. Jeśli plik zawiera wyłącznie złośliwy kod, zostanie usunięty w całości.



Usuwanie plików w archiwach — w domyślnym trybie leczenia całe archiwum jest usuwane tylko wtedy, gdy zawiera wyłącznie zarażone pliki i nie zawiera żadnych niezarażonych plików. Oznacza to, że archiwa nie są usuwane, jeśli zawierają również nieszkodliwe, niezarażone pliki. Podczas skanowania w trybie **Leczenie dokładne** należy jednak zachować ostrożność — każde archiwum zawierające co najmniej jeden zarażony plik jest usuwane bez względu na stan pozostałych zawartych w nim plików.

Aktualizowanie programu

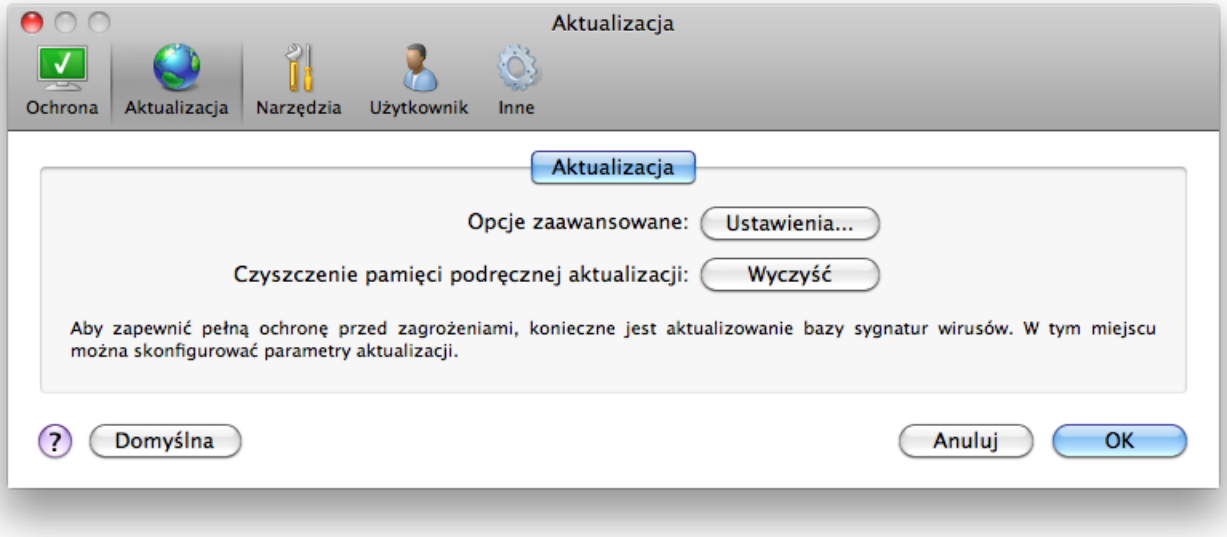
Regularne aktualizowanie programu System Center Endpoint Protection jest niezbędne dla utrzymania maksymalnego poziomu bezpieczeństwa. Moduł aktualizacji zapewnia aktualność programu przez pobieranie najnowszej wersji bazy sygnatur wirusów.

Klikając w menu głównym opcję **Aktualizacja**, można sprawdzić bieżący stan aktualizacji, w tym datę i godzinę ostatniej pomyślnej aktualizacji, oraz ustalić, czy w danej chwili należy przeprowadzić aktualizację. Aby ręcznie rozpocząć proces aktualizacji, kliknij przycisk **Aktualizuj bazę danych sygnatur wirusów**.

W normalnych okolicznościach, po prawidłowym pobraniu aktualizacji w oknie Aktualizacja pojawia się komunikat *Aktualizacja nie jest konieczna — zainstalowana baza sygnatur wirusów jest aktualna*.

W oknie Aktualizacja wyświetlane są też informacje na temat wersji bazy sygnatur wirusów. Ten liczbowy wskaźnik stanowi aktywne łącze do witryny internetowej zawierającej listę wszystkich sygnatur dodanych podczas określonej aktualizacji.

Ustawienia aktualizacji



Aby włączyć używanie trybu testowego (testowania aktualizacji), kliknij przycisk **Ustawienia...** znajdujący się obok nagłówka **Opcje zaawansowane**, a następnie zaznacz pole wyboru **Włącz tryb testowania aktualizacji**. Aby wyłączyć wyświetlanie na pasku zadań powiadomienia po każdej udanej aktualizacji, zaznacz pole wyboru **Nie wyświetlaj powiadomienia o pomyślnej aktualizacji**.

Aby usunąć wszystkie tymczasowo przechowywane dane aktualizacji, kliknij przycisk **Wyczyść** umieszczony obok nagłówka **Czyszczenie pamięci podręcznej aktualizacji**. Opcji tej należy użyć w razie problemów z wykonaniem aktualizacji.

Tworzenie zadań aktualizacji

Aktualizacje można uruchamiać ręcznie, klikając opcję **Aktualizuj bazę sygnatur wirusów** w oknie głównym, które jest wyświetlane po kliknięciu polecenia **Aktualizacja** w menu głównym.

Inną możliwością jest wykonywanie aktualizacji jako zaplanowanych zadań. Aby skonfigurować zaplanowane zadanie, kliknij kolejno opcje **Narzędzia** > **Harmonogram**. Domyślnie w programie System Center Endpoint Protection aktywne są następujące zadania:

- **Regularna aktualizacja automatyczna**
- **Automatyczna aktualizacja po zalogowaniu użytkownika**

Każde z tych zadań aktualizacji można zmodyfikować zgodnie z potrzebami użytkownika. Oprócz domyślnych zadań aktualizacji można tworzyć nowe zadania z konfiguracją zdefiniowaną przez użytkownika. Więcej szczegółowych informacji na temat tworzenia i konfigurowania zadań aktualizacji można znaleźć w sekcji Harmonogram 19.

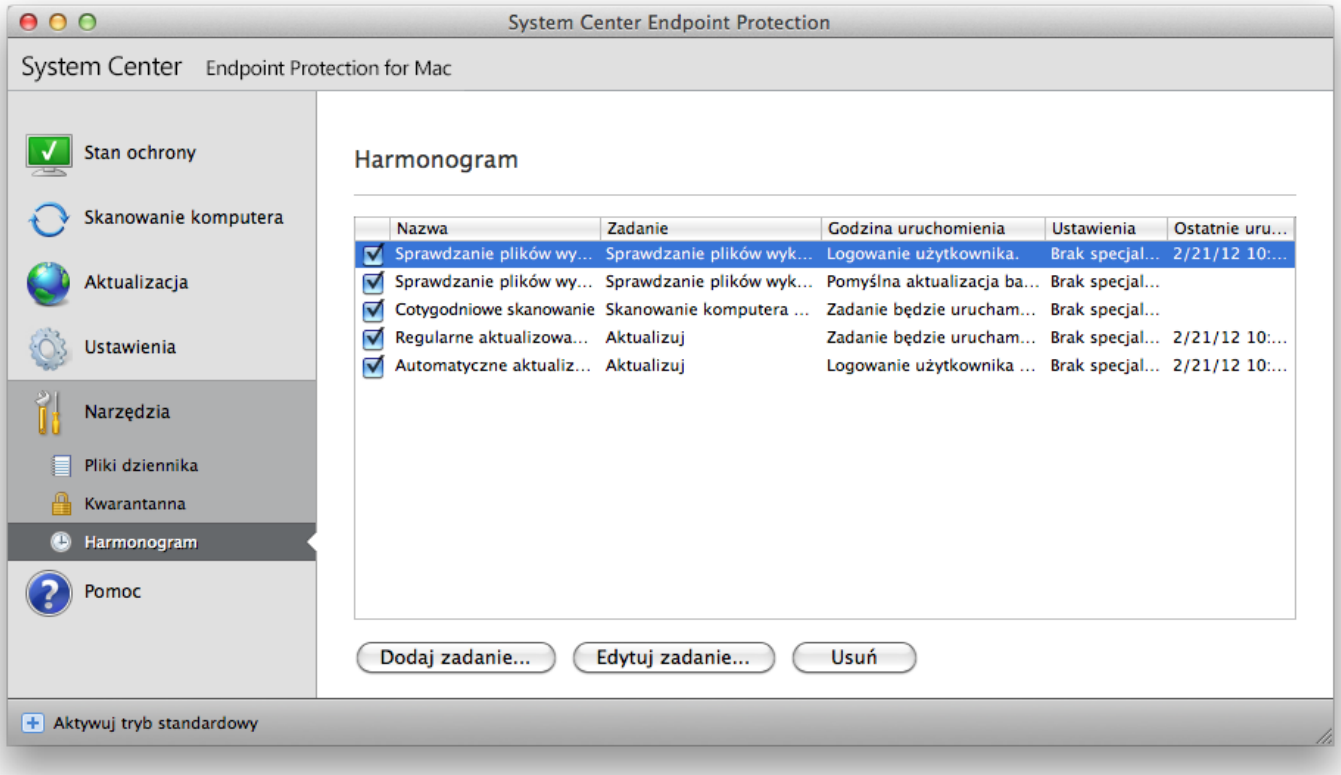
Uaktualnianie do nowej kompilacji

Używanie najnowszej kompilacji programu System Center Endpoint Protection gwarantuje maksymalne bezpieczeństwo. Aby sprawdzić dostępność nowej wersji, kliknij opcję **Aktualizacja** dostępną w menu głównym po lewej stronie. W przypadku dostępności nowej kompilacji u dołu okna pojawi się komunikat *Dostępna jest nowa wersja programu!* Aby wyświetlić okno z informacją o numerze wersji nowej kompilacji oraz dziennikiem zmian, kliknij przycisk **Więcej informacji...**

Aby pobrać najnowszą kompilację, kliknij przycisk **Pobierz**. Jeśli chcesz zamknąć okno i pobrać uaktualnienie później, kliknij przycisk **Zamknij**.

Harmonogram

Moduł **Harmonogram** jest dostępny, gdy w programie System Center Endpoint Protection włączono tryb zaawansowany. Opcja Harmonogram znajduje się w menu głównym programu System Center Endpoint Protection, w kategorii **Narzędzia**. Okno **Harmonogram** zawiera listę wszystkich zaplanowanych zadań oraz właściwości konfiguracyjne, takie jak wstępnie zdefiniowany dzień, godzina i używany profil skanowania.



Domyślnie w oknie Harmonogram są wyświetlane następujące zaplanowane zadania:

- Regularna aktualizacja automatyczna
- Automatyczna aktualizacja po zalogowaniu użytkownika
- Sprawdzanie plików przy uruchamianiu po zalogowaniu użytkownika
- Sprawdzanie plików przy uruchamianiu po pomyślnej aktualizacji bazy sygnatur wirusów
- Administracja dziennikami (po włączeniu opcji **Pokaż zadania systemowe** w ustawieniach modułu Harmonogram)
- Skanowanie cotygodniowe

Aby zmodyfikować konfigurację istniejącego zaplanowanego zadania (zarówno domyślnego, jak i zdefiniowanego przez użytkownika), naciśnij klawisz Ctrl, kliknij zadanie, które ma zostać zmodyfikowane, i wybierz opcję **Edytuj** lub wybierz zadanie i kliknij przycisk **Edytuj zadanie**.

Cel planowania zadań

Harmonogram służy do zarządzania zaplanowanymi zadaniami oraz uruchamiania ich ze wstępnie zdefiniowaną konfiguracją i właściwościami. Konfiguracja i właściwości zawierają takie informacje, jak data i godzina oraz określone profile używane podczas wykonywania zadania.

Tworzenie nowych zadań

Aby utworzyć nowe zadanie w harmonogramie, kliknij przycisk **Dodaj zadanie...** lub naciśnij klawisz Ctrl, kliknij puste pole i z menu kontekstowego wybierz opcję **Dodaj...** Dostępnych jest pięć typów zaplanowanych zadań:

- **Uruchamianie aplikacji**
- **Aktualizacja**
- **Administracja dziennikami**
- **Skanowanie komputera na żądanie**
- **Sprawdzanie plików przy uruchamianiu systemu**

Ponieważ jednym z najczęściej planowanych zadań jest aktualizacja, zostanie przedstawiony sposób dodawania nowego zadania

aktualizacji.

Z menu rozwijanego **Zaplanowane zadanie** wybierz opcję **Aktualizacja**. W polu **Nazwa zadania** wprowadź nazwę zadania. W menu rozwijanym **Uruchom zadanie** wybierz częstotliwość, z jaką ma być wykonywane zadanie. Dostępne są następujące opcje: **Zdefiniowane przez użytkownika**, **Jednorazowo**, **Wielokrotnie**, **Codziennie**, **Co tydzień** i **Po wystąpieniu zdarzenia**. Zależnie od wybranej częstotliwości zostaną wyświetlone różne parametry aktualizacji.

W przypadku wybrania opcji **Zdefiniowane przez użytkownika** zostanie wyświetlony monit o określenie daty/godziny w formacie narzędzia cron (więcej szczegółów zawiera sekcja Tworzenie zadań zdefiniowanych przez użytkownika 20).

W następnym kroku zdefiniuj czynność podejmowaną w przypadku, gdy nie można wykonać lub zakończyć zadania w zaplanowanym czasie. Dostępne są następujące trzy opcje:

- **Czekaj do następnego zaplanowanego terminu**
- **Uruchom zadanie jak najszybciej**
- **Uruchom zadanie natychmiast, jeśli od ostatniego wykonania upłynął określony czas** (upływ czasu można określić za pomocą opcji **Minimalny odstęp między zadaniami**)

W następnym kroku zostanie wyświetlone okno z podsumowaniem informacji o bieżącym zaplanowanym zadaniu. Kliknij przycisk **Zakończ**.

Nowe zaplanowane zadanie zostanie dodane do listy aktualnie zaplanowanych zadań.

W systemie istnieją wstępnie zdefiniowane zadania zaplanowane istotne dla prawidłowego działania produktu. Są one domyślnie ukryte i nie należy ich zmieniać. Aby zmodyfikować tę opcję i sprawić, by zadania były widoczne, kliknij kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Narzędzia** > **Harmonogram**, a następnie wybierz opcję **Pokaż zadania systemowe**.

Tworzenie zadań zdefiniowanych przez użytkownika

Datę i godzinę zadania typu **Zdefiniowane przez użytkownika** należy wprowadzić w formacie narzędzia cron z rozszerzonym rokiem (ciąg składający się z 6 pól oddzielonych znakiem odstępu):

```
minuta(0-59) godzina(0-23) dzień miesiąca(1-31) miesiąc(1-12) rok(1970-2099) dzień tygodnia(0-7)(Niedziela =
```

Przykład:

```
30 6 22 3 2012 4
```

Znaki specjalne obsługiwane w wyrażeniach programu cron:

- gwiazdka (`*`) — wyrażenie będzie dopasowane do wszystkich wartości pola, na przykład gwiazdka w trzecim polu (dzień miesiąca) oznacza każdy dzień;
- łącznik (`-`) — umożliwia zdefiniowanie zakresu, na przykład `3-9`
- przecinek (`,`) — oddziela elementy listy, na przykład `1,3,7,8`
- ukośnik (`/`) — umożliwia zdefiniowanie przyrostu w zakresie, na przykład `3-28/5` w trzecim polu (dzień miesiąca) oznacza trzeci dzień miesiąca oraz co piąty kolejny dzień.

Nazwy dni (poniedziałek-niedziela) i miesięcy (styczeń-grudzień) nie są obsługiwane.

UWAGA: W przypadku zdefiniowania zarówno dnia miesiąca, jak i dnia tygodnia polecenie zostanie wykonane tylko wtedy, gdy wartości obu pól będą dopasowane.

Kwarantanna

Głównym zadaniem kwarantanny jest bezpieczne przechowywanie zarażonych plików. Pliki należy poddawać kwarantannie w przypadku, gdy nie można ich wyleczyć, gdy ich usunięcie nie jest bezpieczne lub zalecane albo gdy są one nieprawidłowo wykrywane przez program System Center Endpoint Protection.

Kwarantanną można objąć dowolny plik. Takie działanie jest zalecane, jeśli plik zachowuje się w podejrzany sposób, ale nie jest wykrywany przez skaner antywirusowy.

Pliki przechowywane w folderze kwarantanny mogą być wyświetlane w tabeli zawierającej datę i godzinę przeniesienia do kwarantanny, ścieżkę do pierwotnej lokalizacji zarażonego pliku, rozmiar pliku w bajtach, powód (np. dodanie przez użytkownika) oraz liczbę zagrożeń (np. jeśli plik jest archiwum zawierającym wiele infekcji). Folder kwarantanny z plikami poddanymi kwarantannie (*/Library/Application Support/Microsoft/scep/cache/quarantine*) pozostanie w systemie nawet po odinstalowaniu programu System Center Endpoint Protection. Pliki poddane kwarantannie są przechowywane w bezpiecznej, zaszyfrowanej postaci. Można je przywrócić po ponownym zainstalowaniu programu System Center Endpoint Protection.

Poddawanie plików kwarantannie

Program System Center Endpoint Protection automatycznie poddaje kwarantannie usunięte pliki (jeśli nie anulowano tej opcji w oknie alertu). W razie potrzeby można ręcznie poddać kwarantannie dowolny podejrzany plik, klikając przycisk **Kwarantanna...**. W tym celu można również skorzystać z menu kontekstowego — naciśnij klawisz Ctrl, kliknij puste pole, wybierz opcję **Kwarantanna...**, wybierz plik, który chcesz poddać kwarantannie, i kliknij przycisk **Otwórz**.

Przywracanie plików z kwarantanny

Pliki poddane kwarantannie można przywrócić do ich pierwotnej lokalizacji. Służy do tego przycisk **Przywróć**. Funkcja przywracania jest również dostępna w menu kontekstowym — w tym celu należy nacisnąć klawisz Ctrl, kliknąć wybrany plik w oknie **Kwarantanna** i wybrać polecenie **Przywróć**. Menu kontekstowe zawiera także opcję **Przywróć do...** umożliwiającą przywrócenie pliku do lokalizacji innej niż ta, z której został usunięty.

Pliki dziennika

Pliki dziennika zawierają informacje o wszystkich ważnych zdarzeniach, jakie miały miejsce w programie, oraz przegląd wykrytych zagrożeń. Zapisywanie informacji w dzienniku pełni istotną rolę przy analizie systemu, wykrywaniu zagrożeń i rozwiązywaniu problemów. Dziennik jest aktywnie tworzony w tle i nie wymaga żadnych działań ze strony użytkownika. Informacje są zapisywane zgodnie z bieżącymi ustawieniami szczegółowości dziennika. Możliwe jest przeglądanie komunikatów tekstowych i dzienników bezpośrednio w programie System Center Endpoint Protection, jak również archiwizowanie dzienników.

Pliki dziennika są dostępne z poziomu menu głównego programu System Center Endpoint Protection po kliknięciu kolejno opcji **Narzędzia** > **Pliki dziennika**. Żądany typ dziennika należy wybrać w menu rozwijanym **Dziennik** znajdującym się u góry okna. Dostępne są następujące dzienniki:

1. **Wykryte zagrożenia** — po wybraniu tej opcji można zapoznać się ze wszystkimi informacjami na temat zdarzeń związanych z wykryciem infekcji.
2. **Zdarzenia** — ta opcja pomaga administratorom systemu i użytkownikom w rozwiązywaniu problemów. Wszystkie ważne czynności podejmowane przez program System Center Endpoint Protection są zapisywane w dziennikach zdarzeń.
3. **Skanowanie komputera** — w tym oknie są wyświetlane wyniki wszystkich ukończonych operacji skanowania. Dwukrotne kliknięcie dowolnego wpisu powoduje wyświetlenie szczegółowych informacji na temat danej operacji skanowania komputera na żądanie.

Informacje wyświetlane w każdym obszarze okna można skopiować bezpośrednio do schowka, wybierając żądaną pozycję i klikając przycisk **Kopiuj**.

Administracja dziennikami

Dostęp do konfiguracji zapisywania w dziennikach w programie System Center Endpoint Protection można uzyskać z poziomu okna głównego. Kliknij kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Narzędzia** > **Pliki dziennika**. Można określić następujące opcje plików dziennika:

- **Automatycznie usuwaj starsze rekordy dzienników** — wpisy dziennika starsze niż podana liczba dni są usuwane automatycznie.
- **Automatycznie optymalizuj pliki dzienników** — umożliwia automatyczną defragmentację plików dzienników w przypadku przekroczenia określonego procentu nieużywanych rekordów.

Wszystkie istotne informacje wyświetlane w graficznym interfejsie użytkownika, komunikaty o zagrożeniach i zdarzeniach mogą być zapisywane w formatach tekstowych czytelnych dla człowieka, takich jak zwykły tekst lub CSV (wartości rozdzielane przecinkami). Jeśli pliki mają być dostępne do przetwarzania za pomocą narzędzi innych firm, należy zaznaczyć pole wyboru obok pozycji **Włącz zapisywanie w plikach tekstowych**.

Aby zdefiniować folder docelowy, w którym zapisywane będą pliki dziennika, należy kliknąć **Ustawienia...**, a następnie **Ustawienia zaawansowane**.

W zależności od opcji wybranych w ustawieniu **Pliki dziennika tekstowego: Edytuj** można zapisywać dzienniki z następującymi informacjami:

- Zagrożenia wykryte przez funkcję Skaner przy uruchamianiu, Ochrona w czasie rzeczywistym lub Skanowanie komputera są zapisywane w pliku o nazwie threatslog.txt.
- Takie zdarzenia, jak *Nieprawidłowa nazwa użytkownika i hasło*, *Nie można zaktualizować bazy sygnatur wirusów* itp. są zapisywane w pliku eventslog.txt.
- Wyniki wszystkich ukończonych skanów są zapisywane w formacie scanlog.NUMBER.txt.

Aby skonfigurować filtry w opcji **Domyślne rekordy dziennika skanowania komputera**, należy kliknąć znajdujący się obok tej opcji przycisk **Edytuj...**, a następnie zaznaczyć lub usunąć zaznaczenie żądanych typów dzienników. Dodatkowe objaśnienia dotyczące typów dzienników można znaleźć w tym rozdziale 22.

Filtrowanie dziennika

W dziennikach przechowywane są informacje o ważnych zdarzeniach systemowych. Funkcja filtrowania dziennika pozwala wyświetlać rekordy na temat określonego typu zdarzeń.

Najczęściej używane typy dzienników wymieniono poniżej:

- **Ostrzeżenia krytyczne** — krytyczne błędy systemowe (np. „Uruchomienie ochrony antywirusowej nie powiodło się").
- **Błędy** — komunikaty o błędach, np. „*Błąd podczas pobierania pliku*", oraz błędy krytyczne.
- **Ostrzeżenia** — komunikaty ostrzegawcze.
- **Rekordy informacyjne** — komunikaty informacyjne, w tym powiadomienia o pomyślnych aktualizacjach, alerty itp.
- **Rekordy diagnostyczne** — informacje potrzebne do ulepszenia konfiguracji programu i wszystkie rekordy wymienione powyżej.

Interfejs użytkownika

Opcje konfiguracji interfejsu użytkownika w programie System Center Endpoint Protection umożliwiają dostosowanie środowiska pracy do potrzeb użytkownika. Można uzyskać do nich dostęp, klikając kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Użytkownik** > **Interfejs**.

Znajduje się tutaj między innymi opcja Tryb zaawansowany, pozwalająca na przejście do trybu zaawansowanego. W trybie zaawansowanym są wyświetlane bardziej szczegółowe ustawienia i dodatkowe formanty programu System Center Endpoint Protection.

Jeśli podczas uruchamiania programu ma być wyświetlany ekran powitalny, zaznacz opcję **Pokaż ekran powitalny przy uruchamianiu**.

W części **Użyj standardowego menu** można wybrać opcję **W trybie standardowym** lub **W trybie zaawansowanym**, która spowoduje, że w głównym oknie programu w wybranym trybie wyświetlania będzie używane standardowe menu.

Aby włączyć wyświetlanie etykiet narzędzi, zaznacz opcję **Pokaż etykiety narzędzi**. Z kolei opcja **Pokaż ukryte pliki** umożliwia wyświetlanie i zaznaczanie ukrytych plików w części **Skanowane obiekty** znajdującej się w oknie **Skanowanie komputera**.

Alerty i powiadomienia

Sekcja **Alerty i powiadomienia** umożliwia konfigurowanie sposobu obsługi alertów o zagrożeniach i powiadomień systemowych w programie System Center Endpoint Protection.

Wyłączenie opcji **Wyświetlaj alerty** spowoduje anulowanie wyświetlania wszystkich okien alertów, dlatego należy jej używać tylko w szczególnych sytuacjach. W przypadku większości użytkowników zaleca się pozostawienie ustawienia domyślnego tej opcji (włączona).

Zaznaczenie opcji **Wyświetlaj powiadomienia na pulpicie** spowoduje wyświetlanie na pulpicie komputera okien alertów niewymagających interwencji ze strony użytkownika (domyślnie — w prawym górnym rogu ekranu). Za pomocą ustawienia **Automatycznie zamykaj powiadomienia po** X **s** można określić czas, przez jaki powiadomienia są widoczne.

Zaawansowane ustawienia alertów i powiadomień

Wyświetlaj tylko powiadomienia wymagające działania użytkownika
Ta opcja pozwala włączyć lub wyłączyć wyświetlanie komunikatów wymagających interwencji użytkownika.

Wyświetlaj tylko powiadomienia wymagające działania użytkownika podczas korzystania z aplikacji w trybie pełnego ekranu
Ta opcja jest przydatna w trakcie wyświetlania prezentacji lub wykonywania innych czynności wymagających użycia całego ekranu.

Uprawnienia

Ustawienia programu System Center Endpoint Protection mogą odgrywać dużą rolę w całościowej polityce bezpieczeństwa firmy. Nieautoryzowane modyfikacje mogą rodzić zagrożenie dla stabilności i ochrony systemu. Dlatego administrator może zezwalać na modyfikowanie konfiguracji programu tylko wybranym użytkownikom.

Aby wyznaczyć uprzywilejowanych użytkowników, kliknij kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Użytkownik** > **Uprawnienia**.

Aby zapewnić maksymalny poziom ochrony systemu, program musi być prawidłowo skonfigurowany. Nieautoryzowane modyfikacje mogą powodować utratę ważnych danych. Aby utworzyć listę uprzywilejowanych użytkowników, wystarczy zaznaczyć ich na liście **Użytkownicy** znajdującej się z lewej strony, a następnie kliknąć przycisk **Dodaj**. Aby usunąć użytkownika, należy zaznaczyć jego nazwę na liście **Użytkownicy uprzywilejowani** po prawej stronie, a następnie kliknąć przycisk **Usuń**.

UWAGA: Jeśli lista uprzywilejowanych użytkowników jest pusta, wszyscy użytkownicy zdefiniowani w systemie mogą zmieniać ustawienia programu.

Menu kontekstowe

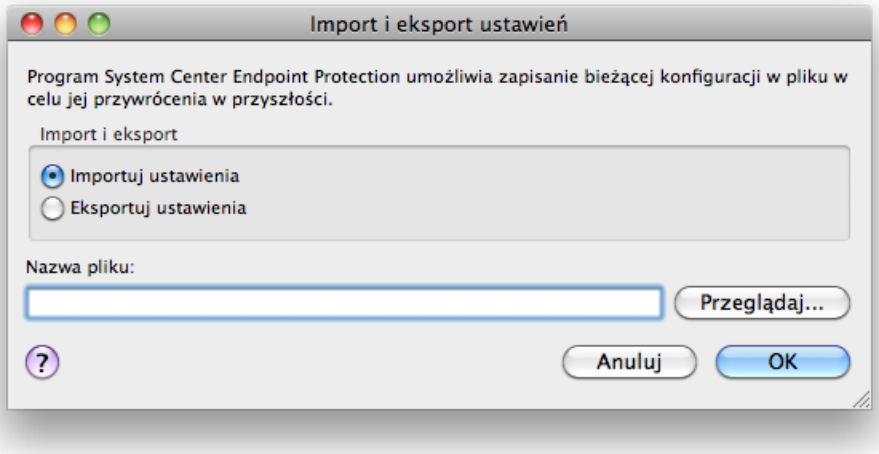
Integrację menu kontekstowego można włączyć, wybierając kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Użytkownik** > **Menu kontekstowe** i zaznaczając pole wyboru **Zintegruj z menu kontekstowym**.

Użytkownik zaawansowany

Import i eksport ustawień

Importowanie i eksportowanie konfiguracji programu System Center Endpoint Protection jest dostępne w trybie zaawansowanym w menu **Ustawienia**.

Do przechowywania konfiguracji podczas importowania i eksportowania są stosowane pliki archiwów. Funkcja importu i eksportu jest przydatna, gdy konieczne jest utworzenie kopii zapasowej bieżącej konfiguracji programu System Center Endpoint Protection w celu jej użycia w późniejszym czasie. Funkcja eksportu ustawień jest również przydatna dla użytkowników, którzy chcą używać preferowanej konfiguracji programu System Center Endpoint Protection w wielu systemach — plik konfiguracyjny można łatwo zaimportować w celu przeniesienia żądanych ustawień.



Import ustawień

Importowanie konfiguracji jest bardzo łatwe. W menu głównym kliknij kolejno opcje **Ustawienia** > **Import i eksport ustawień...**, a następnie wybierz opcję **Importuj ustawienia**. Wprowadź nazwę pliku konfiguracyjnego lub kliknij przycisk **Przeglądaj...**, aby wyszukać plik konfiguracyjny do zaimportowania.

Eksport ustawień

Czynności wykonywane podczas eksportu konfiguracji są bardzo podobne. W menu głównym kliknij kolejno opcje **Ustawienia** > **Import i eksport ustawień...** Wybierz opcję **Eksportuj ustawienia** i wprowadź nazwę pliku konfiguracyjnego. Wybierz za pomocą przeglądania lokalizację na komputerze, w której ma zostać zapisany plik konfiguracyjny.

Ustawienia serwera proxy

Ustawienia serwera proxy można skonfigurować, wybierając kolejno opcje **Inne** > **Serwer proxy**. Określenie serwera proxy na tym poziomie powoduje zdefiniowanie globalnych ustawień serwera proxy dla wszystkich funkcji programu System Center Endpoint Protection. Wprowadzone w tym miejscu parametry będą używane przez wszystkie moduły, które wymagają połączenia internetowego.

Aby określić ustawienia serwera proxy na tym poziomie, zaznacz pole wyboru **Użyj serwera proxy**, a następnie wprowadź w polu **Serwer proxy** adres IP lub adres URL serwera proxy. W polu Port wprowadź numer portu, na którym serwer proxy przyjmuje połączenia (domyślnie 3128). Jeśli komunikacja z serwerem proxy wymaga uwierzytelniania, zaznacz pole wyboru **Serwer proxy wymaga uwierzytelniania** i w odpowiednich polach wprowadź prawidłową **nazwę użytkownika** i **hasło**.

Blokowanie nośników wymiennych

Na nośnikach wymiennych (CD, USB itd.) może znajdować się szkodliwy kod stwarzający zagrożenie dla komputera. Aby zablokować nośniki wymienne, zaznacz pole wyboru obok opcji **Włącz blokowanie nośników wymiennych**. Aby umożliwić dostęp do nośników określonego typu, odznacz pola wyboru obok typów nośników, które mają być dozwolone.

Zaznacz pole wyboru obok opcji **Inne**, jeśli chcesz zastosować te ustawienia do typów nośników innych niż CD, DVD, FireWire lub USB. To ustawienie ma zastosowanie w szczególności do urządzeń peryferyjnych podłączonych do komputera za pośrednictwem interfejsu Thunderbolt.

Słowniczek

Typy infekcji

Infekcja oznacza atak złośliwego oprogramowania, które usiłuje uzyskać dostęp do komputera użytkownika i (lub) uszkodzić jego zawartość.

Wirusy

Wirus komputerowy to program, który zaraża system i uszkadza pliki znajdujące się na komputerze. Nazwa tego typu programów pochodzi od wirusów biologicznych, ponieważ stosują one podobne techniki przenoszenia się z jednego komputera na drugi.

Wirusy komputerowe atakują głównie pliki wykonywalne, skrypty i dokumenty. W celu powielenia wirus dokleja swój kod na końcu zaatakowanego pliku. Działanie wirusa komputerowego w skrócie przedstawia się następująco. Po uruchomieniu zarażonego pliku wirus aktywuje się (przed właściwą aplikacją) i wykonuje zadanie określone przez jego twórcę. Dopiero wtedy następuje uruchomienie właściwej aplikacji. Wirus nie może zarazić komputera, dopóki użytkownik — przypadkowo lub rozmyślnie — nie uruchomi lub nie otworzy złośliwego programu.

Wirusy komputerowe różnią się pod względem celu działania i stopnia stwarzanego zagrożenia. Niektóre z nich są bardzo niebezpieczne, ponieważ mogą celowo usuwać pliki z dysku twardego. Część wirusów nie powoduje jednak żadnych szkód — ich celem jest tylko zirytowanie użytkownika i zademonstrowanie umiejętności programistycznych ich twórców.

Warto zauważyć, że w porównaniu z końmi trojańskimi lub oprogramowaniem spyware wirusy stają się coraz rzadsze, ponieważ nie przynoszą autorom żadnych dochodów. Ponadto termin „wirus” jest często błędnie używany w odniesieniu do wszystkich typów programów zarażających system. Taka interpretacja powoli jednak zanika i stosowane jest nowe, ściślejsze określenie „szkodliwe (lub złośliwe) oprogramowanie” (ang. malware, malicious software).

Jeśli komputer został zaatakowany przez wirusa, konieczne jest przywrócenie zarażonych plików do pierwotnego stanu, czyli wyleczenie ich przy użyciu programu antywirusowego.

Przykłady wirusów: *OneHalf*, *Tenga* i *Yankee Doodle*.

Robaki

Robak komputerowy jest programem zawierającym złośliwy kod, który atakuje komputery hosty. Robaki rozprzestrzeniają się za pośrednictwem sieci. Podstawowa różnica między wirusem a robakiem polega na tym, że ten ostatni potrafi się samodzielnie powielać i przenosić — nie musi w tym celu korzystać z plików nosicieli ani z sektorów rozruchowych dysku. Robaki rozpowszechniają się przy użyciu adresów e-mail z listy kontaktów oraz wykorzystują luki w zabezpieczeniach aplikacji sieciowych.

Robaki są przez to znacznie bardziej żywotne niż wirusy komputerowe. Ze względu na powszechność dostępu do Internetu mogą one rozprzestrzenić się na całym świecie w ciągu kilku godzin po opublikowaniu, a w niektórych przypadkach nawet w ciągu kilku minut. Możliwość szybkiego i niezależnego powielania się powoduje, że są one znacznie groźniejsze niż inne rodzaje szkodliwego oprogramowania.

Robak aktywowany w systemie może być przyczyną wielu niedogodności: może usuwać pliki, obniżać wydajność komputera, a nawet blokować działanie programów. Natura robaka komputerowego predestynuje go do stosowania w charakterze „środka transportu” dla innych typów infekcji.

Jeśli komputer został zarażony przez robaka, zaleca się usunięcie zarażonych plików, ponieważ prawdopodobnie zawierają one złośliwy kod.

Przykłady popularnych robaków: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* i *Netsky*.

Konie trojańskie

Komputerowe konie trojańskie uznawano dotychczas za klasę wirusów, które udają pożyteczne programy, aby skłonić użytkownika do ich uruchomienia. Obecnie konie trojańskie już nie muszą się maskować. Ich jedynym celem jest jak najłatwiejsze przeniknięcie do systemu i wyrządzenie w nim szkód. Określenie „koń trojański” stało się ogólnym terminem używanym w odniesieniu do każdego wirusa, którego nie można zaliczyć do infekcji innego typu.

W związku z tym, że jest to bardzo pojemna kategoria, dzieli się ją często na wiele podkategorii:

- Program pobierający (ang. downloader) — złośliwy program, który może pobierać inne wirusy z Internetu.
- Program zakażający (ang. dropper) — rodzaj konia trojańskiego, którego działanie polega na umieszczaniu na zaatakowanych komputerach innych typów szkodliwego oprogramowania.
- Program otwierający furtki (ang. backdoor) — aplikacja, która komunikuje się ze zdalnymi intruzami, umożliwiając im uzyskanie dostępu do systemu i przejęcie nad nim kontroli.

- Program rejestrujący znaki wprowadzane na klawiaturze (ang. keylogger, keystroke logger) — program, który rejestruje znaki wprowadzane przez użytkownika i wysyła informacje o nich zdalnym intruzom.
- Program nawiązujący kosztowne połączenia (ang. dialer) — program mający na celu nawiązywanie połączeń z kosztownymi numerami telefonicznymi. Zauważenie przez użytkownika nowego połączenia jest prawie niemożliwe. Programy takie mogą przynosić straty użytkownikom modemów telefonicznych, które nie są już regularnie eksploatowane.
- Konie trojańskie występują zwykle w postaci plików wykonywalnych. Jeśli na komputerze zostanie wykryty plik rozpoznany jako koń trojański, zaleca się jego usunięcie, ponieważ najprawdopodobniej zawiera złośliwy kod.

Przykłady popularnych koni trojańskich: *NetBus*, *Trojandownloader.Small.ZL* i *Slapper*.

Adware

Adware to oprogramowanie utrzymywane z reklam. Do tej kategorii zaliczane są programy wyświetlające treści reklamowe. Aplikacje adware często powodują automatyczne otwieranie wyskakujących okienek zawierających reklamy lub zmianę strony głównej w przeglądarce internetowej. Oprogramowanie adware jest często dołączane do bezpłatnych programów, umożliwiając ich autorom pokrycie kosztów tworzenia tych (zazwyczaj użytecznych) aplikacji.

Oprogramowanie adware samo w sobie nie jest niebezpieczne — użytkownikom mogą jedynie przeszkadzać wyświetlane reklamy. Niebezpieczeństwo związane z programami adware polega jednak na tym, że mogą one zawierać funkcje śledzące (podobnie jak spyware — oprogramowanie szpiegujące).

Jeśli użytkownik zdecyduje się użyć bezpłatnego oprogramowania, powinien zwrócić szczególną uwagę na jego program instalacyjny. Podczas instalacji jest zazwyczaj wyświetlane powiadomienie o instalowaniu dodatkowych programów adware. Często jest dostępna opcja umożliwiająca anulowanie instalacji programu adware i zainstalowanie programu głównego bez dołączonego oprogramowania reklamowego.

W niektórych przypadkach zainstalowanie programu bez dołączonego oprogramowania adware jest niemożliwe lub powoduje ograniczenie funkcjonalności. Dzięki temu oprogramowanie adware może zostać zainstalowane w systemie w sposób legalny, ponieważ użytkownik wyraża na to zgodę. W takim przypadku należy kierować się względami bezpieczeństwa, aby uniknąć ewentualnych konsekwencji błędnej decyzji. Jeśli na komputerze zostanie wykryty plik rozpoznany jako adware, zaleca się jego usunięcie, ponieważ istnieje duże prawdopodobieństwo, że zawiera on złośliwy kod.

Spyware

Do tej kategorii należą wszystkie aplikacje, które przesyłają prywatne informacje bez zgody i wiedzy użytkownika. Programy typu spyware korzystają z funkcji śledzących do wysyłania różnych danych statystycznych, na przykład listy odwiedzonych witryn internetowych, adresów e-mail z listy kontaktów użytkownika lub listy znaków wprowadzanych za pomocą klawiatury.

Twórcy oprogramowania spyware twierdzą, że te techniki mają na celu uzyskanie pełniejszych informacji o potrzebach i zainteresowaniach użytkowników oraz umożliwiają bardziej trafne kierowanie reklam do odbiorców. Problem polega jednak na tym, że nie ma wyraźnego rozgraniczenia między aplikacjami pożytecznymi i szkodliwymi. Nikt nie może mieć pewności, czy gromadzone informacje nie zostaną wykorzystane w niedozwolony sposób. Dane pozyskiwane przez spyware mogą obejmować kody bezpieczeństwa, kody PIN, numery kont bankowych itd. Aplikacja spyware jest często umieszczana w bezpłatnej wersji programu przez jego autora w celu uzyskania dochodu lub zachęcenia użytkownika do nabycia wersji komercyjnej. Nierzadko podczas instalacji programu użytkownicy są informowani o obecności oprogramowania spyware, co ma ich skłonić do zakupu pozbawionej go wersji płatnej.

Przykładami popularnych bezpłatnych produktów, do których dołączone jest oprogramowanie szpiegujące, są aplikacje klienckie sieci P2P (ang. peer-to-peer). Programy Spyfalcon i Spy Sheriff (oraz wiele innych) należą do szczególnej podkategorii oprogramowania spyware. Wydają się zapewniać przed nim ochronę, ale w rzeczywistości same są takimi programami.

Jeśli na komputerze zostanie wykryty plik rozpoznany jako spyware, zaleca się jego usunięcie, ponieważ najprawdopodobniej zawiera złośliwy kod.

Potencjalnie niebezpieczne aplikacje

Istnieje wiele legalnych programów, które ułatwiają administrowanie komputerami podłączonymi do sieci. Jednak w niewłaściwych rękach mogą one zostać użyte do wyrządzania szkód. Program System Center Endpoint Protection oferuje możliwość wykrywania takich zagrożeń.

„Potencjalnie niebezpieczne aplikacje” to kategoria, do której należą niektóre legalne programy komercyjne. Są to m.in. narzędzia do dostępu zdalnego, programy do łamania haseł i programy rejestrujące znaki wprowadzane na klawiaturze.

W przypadku wykrycia działającej na komputerze potencjalnie niebezpiecznej aplikacji, która nie została zainstalowana świadomie przez użytkownika, należy skonsultować się z administratorem sieci lub usunąć ją.

Potencjalnie niepożądane aplikacje

Potencjalnie niepożądane aplikacje nie muszą być projektowane w złych intencjach, ale mogą negatywnie wpływać na wydajność komputera. Zainstalowanie takiej aplikacji zazwyczaj wymaga zgody użytkownika. Po zainstalowaniu tego rodzaju programu działanie systemu zmienia się w porównaniu z wcześniejszym stanem. Najbardziej widoczne są następujące zmiany:

- otwieranie nowych, nieznanych okien;
- aktywacja i uruchamianie ukrytych procesów;
- zwiększone wykorzystanie zasobów systemowych;
- zmiany w wynikach wyszukiwania;
- łączenie się aplikacji z serwerami zdalnymi.