ESET Endpoint Antivirus for macOS

Podręcznik użytkownika

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Produkt ESET Endpoint Antivirus for macOS został opracowany przez ESET, spol. s r.o.

Aby uzyskać więcej informacji, odwiedź stronę https://www.eset.com.

Pomoc techniczna: https://support.eset.com

WER. 12.04.2024

ESET Endpoint Antivirus for macOS

Program ESET Endpoint Antivirus for macOS 7 jest nowym rozwiązaniem zapewniającym w pełni zintegrowaną ochronę komputera przed zagrożeniami. Bezpieczeństwo komputera zapewnia najnowsza wersja silnika skanowania ThreatSense® o szybkim i precyzyjnym działaniu. W wyniku tego połączenia powstał inteligentny system, który w porę ostrzega przed atakami i szkodliwymi aplikacjami zagrażającymi komputerowi.

Program ESET Endpoint Antivirus for macOS 7 to kompletne rozwiązanie, które zapewnia wysoki poziom bezpieczeństwa. Zaawansowane techniki oparte na sztucznej inteligencji potrafią z wyprzedzeniem eliminować przenikające do systemu wirusy, aplikacje szpiegujące, konie trojańskie, robaki, oprogramowanie reklamowe i programy typu rootkit oraz inne formy ataków z Internetu, unikając przy tym obniżania wydajności komputera czy zakłócania jego pracy.

Produkt jest przeznaczony głównie do użytku na stacjach roboczych w małym środowisku firmowym. Można z niego korzystać w połączeniu z programem ESET PROTECT On-Prem, co pozwala na łatwe zarządzanie dowolną liczbą klienckich stacji roboczych, stosowanie zasad i reguł, monitorowanie procesu wykrywania oraz zdalne wprowadzanie zmian z dowolnego komputera podłączonego do sieci.

Nowe funkcje w wersji 7

ESET Endpoint Antivirus for macOS w wersji 7 to nowa generacja naszego produktu oparta na mikrousługach, a nie pojedynczej usłudze.

- Natywna obsługa układów Apple ARM (od wersji 7.1.1700.0)
- Natywna architektura 64-bitowa
- Zwiększona wydajność i stabilność. Jeśli ESET Endpoint Antivirus for macOS ulegnie awarii, może automatycznie uruchomić się ponownie bez zauważenia przez użytkownika.
- Większe bezpieczeństwo dzięki uniezależnieniu procesów od siebie.
- Nowe główne okno programu zawierające:
  - Obsługę trybu ciemnego
  - Natywne powiadomienia na pulpicie
  - Opcję wyłączenia graficznego interfejsu użytkownika dla użytkownika końcowego
- Ulepszoną ochronę systemu plików w czasie rzeczywistym
  - Najnowszy natywny 64-bitowy silnik skanowania
  - Zoptymalizowany pod kątem wydajności wielordzeniowej
  - Skanowanie w czasie rzeczywistym dla użytkownika lokalnego
- Zupełnie nowy natywny graficzny interfejs użytkownika
- Rozszerzona konfiguracja ESET LiveGrid za pośrednictwem ESET PROTECT On-Prem i ESET PROTECT CLOUD

- Ujednolicenie poleceń wiersza poleceń na platformie Linux.
- Konfiguracja stanów ochrony
- Wsparcie wydajności i obsługa wszystkich wyłączeń wykrycia (według ścieżki, według ścieżki i wykrycia, według skrótu)

Porównanie wersji 6 i wersji 7

Funkcja	Wersja 6	Wersja 7.3 i 7.4
Architektura		
Architektura	Monolityczna	Mikrousługi
Profil zabezpieczeń architektury	Główny proces działa w katalogu głównym (wszystkie ważne operacje są wykonywane przez główny proces)	Każda usługa działa z możliwie najniższymi uprawnieniami Niższy możliwy wektor ataku Luka w zabezpieczeniach jednej usługi nie naraża całej aplikacji. Awaria lub przejęcie jednego procesu produktu nie powoduje wyłączenia wszystkich zabezpieczeń
Profil stabilności architektury	Awaria skanera monolitycznego powoduje czasową pustkę w ochronie Automatyczne ponowne uruchomienie procesu w przypadku awarii	Awaria usługi niekrytycznej nie powoduje wstrzymania ochrony Prostsze usługi zoptymalizowane pod kątem konkretnych zadań Automatyczne ponowne uruchomienie usługi w przypadku awarii
Wsparcie macOS	10.12 (Sierra) 10.13 (High Sierra) 10.14 (Mojave) 10.15 (Catalina) 11 (Big Sur) 12 (Monterey) 13 (Ventura)	10.15 Catalina (tylko wersja 7.3) 11 (Big Sur) 12 (Monterey) 13 (Ventura) 14 (Sonoma)
Natywny 64-bitowy silnik skanowania	x	x
Natywna aplikacja 64-bitowa	x	x
Obsługa wielu języków	pakiet instalacyjny specyficzny dla języka	wszystkie języki w jednym pakiecie (język interfejsu graficznego taki sam jak system)

Funkcja	Wersja 6	Wersja 7.3 i 7.4
Natywna obsługa ARM		od wersji 7.1.1700.0
Pomoc techniczna dla Rosetta ARM	x	x
Ochrona systemu plików		
Wykrywanie potencjalnie niechcianych, niebezpiecznych i podejrzanych aplikacji	x	x
Pliki i foldery wyłączone ze skanowania	x	x
Wyłączenia wykrywania przez funkcję Ścieżka i wykrycie	Po utworzeniu wyłączenia wykrywania (pliki są skanowane, ale problemy są ignorowane) w ESET PROTECT On-Prem, tworzy wyłączenie wydajności (pliki nie są skanowane).	x
Konfiguracja wyłączeń wykrywania wg wykrycia		x
Konfiguracja wyłączeń wykrywania wg funkcji Dokładny plik (skrót)		x
Ochrona systemu plików w czasie rzeczywistym	x	x
Zwiększ zgodność dysków sieciowych	x	nie jest potrzebny
Skanowanie na koncie zalogowanego użytkownika		x
Skanuj dyski lokalne	x	x
Skanowanie nośników wymiennych	x	x
Skanowanie dysków sieciowych	x	x
Skanowanie po otwarciu, po utworzeniu	x	x
Skanowanie po wykonaniu	x	Tak, część otwartego
Wyłączenia procesa		x
Ochrona oparta na chmurze	x	x
Systemu reputacji ESET LiveGrid©	x	x (rozszerzona)
System informacji zwrotnych ESET LiveGrid©	x	x
Szczegółowa konfiguracja tego, co można wysłać		x
Skanowanie w poszukiwaniu szkodliwego oprogramowania (na żądanie)	x	x
Skanowanie dowiązań symbolicznych	x	x
Skanowanie plików e-mail	x	x
Skanowanie skrzynek pocztowych	x	x
Skanowanie archiwów	x	x
Skanowanie archiwów samorozpakowujących	x	x
Skanowanie programów pakujących w czasie wykonywania	x	x
Skanuj alternatywne strumienie danych (ADS)	x	x
Włącz inteligentną optymalizację	x	x

Funkcja	Wersja 6	Wersja 7.3 i 7.4
Wyklucz foldery systemowe ze skanowania	x	Niepotrzebne
Uruchom skanowanie w tle z niskim priorytetem		x
Zachowaj znacznik czasowy ostatniego dostępu	x	x
Skanowanie podczas rozruchu	x	
Ochrona stron internetowych i poczty e-mail		
Wyłączenia aplikacji	x	x
Wyłączenia adresów IP	x	x
Ochrona dostępu do stron internetowych (skanowanie HTTP)	x	x
Ochrona programów poczty e-mail	x	x
Ochrona przed atakami typu „phishing”	x	x
Aktualizator modułów		
Niestandardowy serwer proxy dla podstawowego/pomocniczego serwera aktualizacji	x	x
Cofanie aktualizacji modułów	x	x
Aktualizacje w wersji wstępnej	x	x
Opóźniona aktualizacja	x	x
Inne główne funkcje		
Kontrola dostępu do urządzeń	x	
Zapora		
Kontrola dostępu do stron internetowych		
Obsługa ERMM (interfejs wiersza poleceń do integracji zdalnego monitorowania i zarządzania)	x	
Wsparcie dla programu ESET Enterprise Inspector	x	x
Inne mniejsze funkcje		
Interfejs wiersza poleceń	x	x (ujednolicony z ESET Endpoint for Linux)
Dziennik wykrywania	x	x
Dziennik zdarzeń	x	x
Dziennik skanowania komputera	x	x
Importowanie lub eksportowanie ustawień	x	x
Kwarantanna	x	x
Harmonogram zadań lokalnych	x	x
Konfiguracja serwera proxy	x	x
Tryb prezentacji	x	x (natywny system Nie przeszkadzać)
Interfejs użytkownika		
Pliki dziennika	x	x
Wykryte zagrożenia	x	x
Zdarzenia	x	x
Skanowanie komputera	x	x

Funkcja	Wersja 6	Wersja 7.3 i 7.4
Kontrola dostępu do urządzeń	x	
Zapora	(W Endpoint Security)	
Filtrowanie witryn internetowych	x	x
Kontrola dostępu do stron internetowych	(W Endpoint Security)	
Filtrowanie dziennika	x	x
Statystyki ochrony	x	x
Harmonogram	x	x
Uruchomione procesy	x	
Kwarantanna	x	x
Prześlij plik do analizy	x	x (7.4)
Stan ochrony	x	x
Ręczna aktualizacja modułów	x	x
Ustawienia lokalne/konfiguracja przez użytkownika	x	x
Importowanie lub eksportowanie ustawień z graficznego interfejsu użytkownika	x	
Pomoc	x	x
Zupełnie nowy natywny graficzny interfejs użytkownika		x
Obsługa trybu ciemnego		x
Obsługa wyświetlaczy o wysokiej rozdzielczości	x	x
Możliwość wyłączenia GUI dla użytkownika		x
Powiadomienia natywne		x
Pasek menu	x	x
Możliwość ukrycia ikony na pasku menu	x	x
Integracja z menu kontekstowym	x	
Szczegółowa kontrola stanu ochrony wyświetlanego w graficznym interfejsie użytkownika/zgłaszanie do ESET PROTECT On-Prem lub ESET PROTECT CLOUD	x	x
Powiadomienia o aktualizacjach systemu	x	x
Instalacja		
Instalacja oparta na lokalnym graficznym interfejsie użytkownika	x	x
Instalacja oparta na komponentach	x	
Zdalna instalacja oparta na komponentach (instalacja komponentów wymaga dodatkowych kroków)	x	
Obsługa instalacji cichej (poprzez wstępne zatwierdzenia MDM)	x	x
Aktualizacja produktu poprzez ponowną instalację	x	x
Aktualizacja produktu z ESET PROTECT On-Prem lub ESET PROTECT CLOUD	x	x
Aktywacja produktu		
Aktywacja za pomocą klucza licencyjnego	x	x
Obsługa licencji subskrypcyjnej	x	x

Funkcja	Wersja 6	Wersja 7.3 i 7.4
Aktywacja poprzez ESET PROTECT On-Prem lub ESET PROTECT CLOUD	x	x
Aktywacja za pomocą pliku licencji offline	x	x
Zgodność z konsolami zarządzania ESET		
Zgodność z ESET PROTECT CLOUD	x	x
Zgodność z ESET PROTECT On-Prem	x	x

Migracja ustawień

Proces migracji

Od wersji 7.2 i nowszych ustawienia z wersji ESET Endpoint Antivirus for macOS 6 są automatycznie migrowane do nowej wersji podczas procesu uaktualniania.

Po zakończeniu procesu migracji na ekranie głównym ESET Endpoint Antivirus for macOS zostanie wyświetlone powiadomienie informujące o pomyślnej migracji ustawień: **Twoje ustawienia zostały przeniesione do nowej wersji**.

Polityki z ESET PROTECT On-Prem i ESET PROTECT CLOUD nie zostaną przeniesiona automatycznie, ponieważ nie wszystkie funkcje obecne w 6 wersji ESET Endpoint Antivirus for macOS są obecne w wersji 7. Po uaktualnieniu do wersji 7 należy sprawdzić istniejące polityki i utworzyć nowe w oparciu o funkcje obecne w wersji 7. Więcej informacji na temat tworzenia lub usuwania polityk można znaleźć w temacie Polityki:

- Polityki w ESET PROTECT On-Prem
- Polityki w ESET PROTECT CLOUD

Polityki w ESET PROTECT On-Prem i ESET PROTECT CLOUD dla 6 i 7 wersji ESET Endpoint Antivirus for macOS można aktywować jednocześnie.

Jeśli uaktualniono już wersję ESET Endpoint Antivirus for macOS 6 do wersji 7 lub 7.1, nadal można przeprowadzić migrację ustawień po uaktualnieniu do nowszej wersji. Instrukcje można znaleźć w artykule dotyczącym migracji w bazie wiedzy firmy ESET.

Wszystkie ustawienia dostępne w wersji 7.X zostaną przeniesione z wersji 6, z następującymi wyjątkami:

- Ustawienia uprawnień (nieobsługiwane w wersji 7)
- Niestandardowy serwer proxy dla aktualizacji (niestandardowy serwer proxy nie jest obsługiwany w wersji 7)
- Kwarantanna zawartości
- Poziomy leczenia dla skanowania
- Profile docelowe dla skanowania na żądanie

Ustawienia następujących funkcji są przechowywane w pliku migracji .xml i można je załadować, gdy będą one dostępne w przyszłych wersjach ESET Endpoint Antivirus for macOS:

- Kontrola dostępu do urządzeń
- Logs
- Ochrona dostępu do stron internetowych
- Tryb prezentacji

Inne problemy związane z migracją

- Profile skanowania niestandardowego są przenoszone i można nimi zarządzać za pośrednictwem ESET PROTECT On-Prem, ESET PROTECT CLOUD lub w preferencjach aplikacji

Dziennik zmian

Wymagania systemowe

Aby zapewnić optymalne działanie programu ESET Endpoint Antivirus for macOS, komputer powinien spełniać następujące wymagania dotyczące sprzętu i oprogramowania:

	Wymagania systemowe:
Procesor	Procesor Intel 64-bit, Apple ARM 64-bitowy
System operacyjny	macOS Big Sur (11) do macOS Sonoma (14)
Pamięć	300 MB
Wolne miejsce na dysku	600 MB

ESET Endpoint Antivirus for macOS wymaga dostępu do Internetu podczas instalacji.

ESET Endpoint Antivirus for macOS wersja 7.1.1700.0 i nowsze zapewniają natywną obsługę układu Apple ARM.

Uaktualnij ESET Endpoint Antivirus for macOS z wersji 6 do wersji 7

Po aktualizacji ESET Endpoint Antivirus for macOS z wersji 6 do wersji 7 ESET Endpoint Antivirus for macOS powróci do ustawień domyślnych. Dotyczy to również polityk w konsoli zarządzania ESET.
ESET Endpoint Antivirus for macOS w wersji 7 zawiera wiele różnic w stosunku do wersji 6, a niektórych funkcji brakuje. Zanim zdecydujesz się na uaktualnienie ESET Endpoint Antivirus for macOS, zalecamy przeczytanie tematu Porównanie wersji 6 i wersji 7.

- Uaktualnienie lokalne
- Uaktualnij za pomocą wiersza poleceń
- Aktualizacja za pomocą konsoli zarządzania ESET

- Migracja ustawień

Uaktualnienie lokalne

1. Pobierz najnowszy plik instalacyjny ESET Endpoint Antivirus for macOS (.dmg).

2. Otwórz plik instalacyjny (.dmg).

3. Kliknij dwukrotnie ikonę Instaluj ESET Endpoint Antivirus for macOS  .

4. Kliknij przycisk Kontynuuj, jeśli nie zainstalowano żadnej innej aplikacji zabezpieczającej. Jeśli jest zainstalowana inna aplikacja antywirusowa, instalacja może się nie powieść.

5. Kliknij przycisk Kontynuuj, aby potwierdzić wymagania systemowe.

6. Kliknij Zaakceptuj, aby zaakceptować Umowa Licencyjna Użytkownika Końcowego i politykę prywatności.

7. Jeśli chcesz zmienić folder docelowy lub zmienić to, czy wszyscy użytkownicy mają dostęp do ESET Endpoint Antivirus for macOS, kliknij przycisk Zmień lokalizację instalacji. Aby rozpocząć instalację, kliknij przycisk Zainstaluj.

Zmień miejsce instalacji

Wybierz miejsce docelowe instalacji. Wybierz, czy chcesz zainstalować ESET Endpoint Antivirus for macOS dla wszystkich użytkowników na komputerze, czy tylko dla bieżącego użytkownika. Można również wybrać określony folder do instalacji ESET Endpoint Antivirus for macOS. Wybierz opcję i kliknij przycisk Kontynuuj, aby powrócić do kroku Typ instalacji.

8. Na początku instalacji może zostać wyświetlony monit o wprowadzenie hasła administratora.

9. Kliknij Zamknij, aby zakończyć instalację.

10. Po zakończeniu instalacji wyświetli się kreator wdrażania. Wykonaj czynności opisane tutaj, aby zapewnić ochronę komputera.

Uaktualnij za pomocą wiersza poleceń

Aby uaktualnić ESET Endpoint Antivirus for macOS do wersji 7 za pomocą wiersza poleceń:

1. Pobierz ESET Endpoint Antivirus for macOS w wersji 7.

2. Roześlij pliki .dmg na komputery docelowe.

3. Uruchom instalację zgodnie z opisem w temacie Instalacja z wiersza polecenia.

Uaktualnij ESET Endpoint Antivirus for macOS za pośrednictwem ESET

PROTECT On-Prem lub ESET PROTECT CLOUD

Przed uaktualnieniem należy wprowadzić następujące zmiany w profilach konfiguracji na serwerze MDM:

- W profilu konfiguracji Pełnego dostępu do dysku

Wersja 6		Wersja 7	
Identyfikator	com.eset.eea.6	Identyfikator	com.eset.eea.g2

- Jeśli instalujesz ESET Endpoint Antivirus for macOS w systemie macOS 12 lub nowszym, musisz dodać pełny dostęp do dysku dla Uninstaller.app. Jest to konieczne, aby usunąć wersję 6 z systemu i umożliwić zdalne odinstalowanie wersji 7 w przyszłości. Do profilu konfiguracji pełnego dostępu do dysku dodaj:

ESET Endpoint Antivirus i ESET Endpoint Security na macOS 12 Monterey	
Identyfikator	com.eset.app.Uninstaller
Typ identyfikatora	bundleID
Wymagania dot. kodu	identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikacja lub usługa	SystemPolicyAllFiles
Dostęp	Allow

- W profilu konfiguracji ochrony dostępu do stron internetowych i poczty e-mail

Wersja 6		Wersja 7	
Identyfikator niestandardowego połączenia SSL VPN	com.eset.sysext.manager	Identyfikator niestandardowego połączenia SSL VPN	com.eset.network.manager

Jeśli usuniesz ustawienia dla wersji 6 przed uaktualnieniem do wersji 7, użytkownicy otrzymają powiadomienie, tak jakby te ustawienia nie zostały zastosowane. Zalecamy utworzenie nowego profilu konfiguracji dla ESET Endpoint Antivirus for macOS w wersji 7, wdrożenie profilu konfiguracji na komputerach docelowych, uaktualnienie ESET Endpoint Antivirus for macOS i usunięcie profili konfiguracji dla wersji 6. Zaleca się również, aby upewnić się, czy istnieje tylko jedna polityka instalacji ESET Endpoint Antivirus for macOS na jednym urządzeniu. W przypadku korzystania z zarówno ESET PROTECT On-Prem, jak i Jamf upewnij się, że każdy program ma tylko jedną politykę instalacji.

Nowe profile konfiguracji dla ESET Endpoint Antivirus for macOS w wersji 7 do pobrania można znaleźć w temacie Ustawienia przedinstalacyjne.

Po wdrożeniu nowych profili konfiguracji kontynuuj instalację w temacie Wdrażanie za pomocą konsoli zarządzania ESET.

Instalacja

Metoda instalacji

Metoda instalacji	Typ instalacji	Uwagi
Instalacja graficznego interfejsu użytkownika	Lokalne	Instalację ESET Endpoint Antivirus for macOS można wykonać lokalnie z pliku instalacyjnego .dmg. Przed rozpoczęciem instalacji zamknij wszystkie otwarte programy komputerowe. ESET Endpoint Antivirus for macOS zawiera składniki, które mogą powodować konflikty z innymi programami antywirusowymi zainstalowanymi na komputerze. Dlatego zdecydowanie zalecamy usunięcie wszystkich innych programów antywirusowych, aby zapobiec potencjalnym problemom. Po zakończeniu instalacji wyświetli się kreator wdrażania. Wykonaj czynności opisane tutaj, aby zapewnić ochronę komputera.
Instalacja przy użyciu wiersza polecenia	Lokalna/zdalna	Możesz zainstalować ESET Endpoint Antivirus for macOS bez konieczności interakcji z graficznym interfejsem użytkownika instalatora. Tej metody można również użyć do zdalnej instalacji ESET Endpoint Antivirus for macOS. Jeśli instalujesz ESET Endpoint Antivirus for macOS zdalnie, zalecamy zastosowanie ustawień zgody użytkownika za pośrednictwem MDM przed instalacją.
ESET PROTECT On-Prem	Zdalny	Jeśli komputer jest zarejestrowany w programie ESET PROTECT On-Prem, można utworzyć zadanie instalacji w celu zainstalowania ESET Endpoint Antivirus for macOS na komputerach docelowych.
ESET PROTECT CLOUD	Zdalny	Jeśli komputer jest zarejestrowany w programie ESET PROTECT CLOUD, można utworzyć zadanie instalacji w celu zainstalowania ESET Endpoint Antivirus for macOS na komputerach docelowych.

ESET Endpoint Antivirus for macOS wymaga ustawień zgody użytkownika do działania. Te ustawienia należy zastosować ręcznie po zakończeniu instalacji. Urządzenie musi być zarejestrowane na MDM, aby uniknąć dodawania ustawień zgody użytkownika do każdego komputera. MDM będzie następnie używany do dystrybucji profili konfiguracji do komputerów docelowych. Jeśli nie zastosujesz tych ustawień przed instalacją, to użytkownicy otrzymają wiele wyskakujących okienek dialogowych zachęcających ich do ręcznego zastosowania ustawień zgody użytkownika. Zalecamy dystrybucję profili konfiguracji przed instalacją ESET Endpoint Antivirus for macOS.

Wdrażanie

Po instalacji ESET Endpoint Antivirus for macOS zostanie wyświetlony **Kreator wdrażania** — zestaw ekranów, które poprowadzą Cię przez zalecane i obowiązkowe kroki, które należy wykonać, aby uzyskać w pełni funkcjonalny program ESET Endpoint Antivirus for macOS.

1. Włącz **Zalecane ustawienia ochrony**, wybierz preferowane opcje i kliknij przycisk **Kontynuuj**. Aby uzyskać więcej informacji na temat **ESET LiveGrid©** lub **Potencjalnie niepożądanych aplikacji**, odwiedź nasz Słowniczek.

2. Krok obowiązkowy: Włączanie **rozszerzeń systemu ESET**. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby kontynuować konfigurację.

3. Krok obowiązkowy: Zezwól na **Konfigurację serwera proxy**. W wyświetlonym oknie alertu wybierz **Zezwól**.

4. Krok obowiązkowy: Przyznaj ESET Endpoint Antivirus for macOS**Pełny dostęp do dysku**. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie i zezwól na pełny dostęp do dysku.

5. Następnie kreator wyświetli monit o **aktywowanie ESET Endpoint Antivirus for macOS**. Wiele opcji aktywacji zostało opisanych w rozdziale Aktywacja.

6. **Zezwalaj na powiadomienia**. Zalecamy zezwolenie na otrzymywanie powiadomień o wszelkich wykrytych zagrożeniach w systemie.

Pomijanie kreatora wdrażania ESET Endpoint Antivirus for macOS.
Klikając opcję **Konfiguruj później**, możesz pominąć obowiązkową konfigurację, ale pamiętaj, że ochrona będzie działać tylko częściowo.

Ponowne uruchamianie kreatora wdrażania

Otwórz **Finder** > **Aplikacje** > Ctrl + kliknij (lub kliknij prawym klawiszem myszy) ikonę **ESET Endpoint Antivirus for macOS** > wybierz opcję **Pokaż zawartość pakietu** z menu skrótów > otwórz **Contents** > otwórz **Helpers** > **Wdrażanie**. Możesz również ręcznie skonfigurować obowiązkowe ustawienia zabezpieczeń, wykonując czynności opisane w sekcji Wdrażanie ręczne.

Po zainstalowaniu programu ESET Endpoint Antivirus for macOS należy przeskanować komputer w poszukiwaniu szkodliwego kodu. W głównym menu programu należy kliknąć kolejno opcje **Skanowanie** > **Skanuj teraz**. Więcej informacji o skanowaniu komputera na żądanie można znaleźć w sekcji Skanowanie komputera na żądanie.

Zezwól na rozszerzenia systemu

Podczas pierwszej instalacji programu ESET Endpoint Antivirus for macOS należy zezwolić programowi ESET Endpoint Antivirus for macOS na ochronę **rozszerzeń systemu** oraz na **pełny dostęp do dysku**.

macOS Ventura (13) i nowsze wersje

1. Otwórz **Ustawienia systemu**.
2. Wybierz **Prywatność i bezpieczeństwo** z menu po lewej stronie.
3. Przewiń w dół do sekcji **Bezpieczeństwo** i kliknij opcję **Szczegóły** pod uwagą „Niektóre oprogramowanie systemowe wymaga uwagi, zanim będzie można go użyć”.

Jeśli uwaga **Niektóre oprogramowanie systemowe wymaga uwagi, zanim będzie można go użyć** i przycisk **Szczegóły** są niedostępne, rozszerzenia systemu były wcześniej dozwolone i nie są wymagane żadne dalsze działania.

4. Użyj czytnika **Touch ID** lub kliknij pozycję **Użyj hasła** i wpisz **nazwę użytkownika** i **hasło**, a następnie kliknij przycisk **Odblokuj**.
5. Włącz zarówno **ochronę systemu plików w czasie rzeczywistym**, jak i **ochronę dostępu do stron internetowych i poczty e-mail** firmy ESET, klikając przełączniki.
6. Kliknij przycisk **OK**.
7. Po wyświetleniu alertu **Ochrona dostępu do stron internetowych i poczty e-mail ESET** z monitem o **dodanie konfiguracji serwera proxy** wybierz opcję **Zezwól**. Jeśli po wyświetleniu alertu nie zezwolisz na konfigurację serwera proxy, należy ponownie uruchomić komputer, aby zainicjować alert i mieć możliwość ponownego zezwolenia na konfigurację serwera proxy.

macOS Monterey (12) i starsze wersje

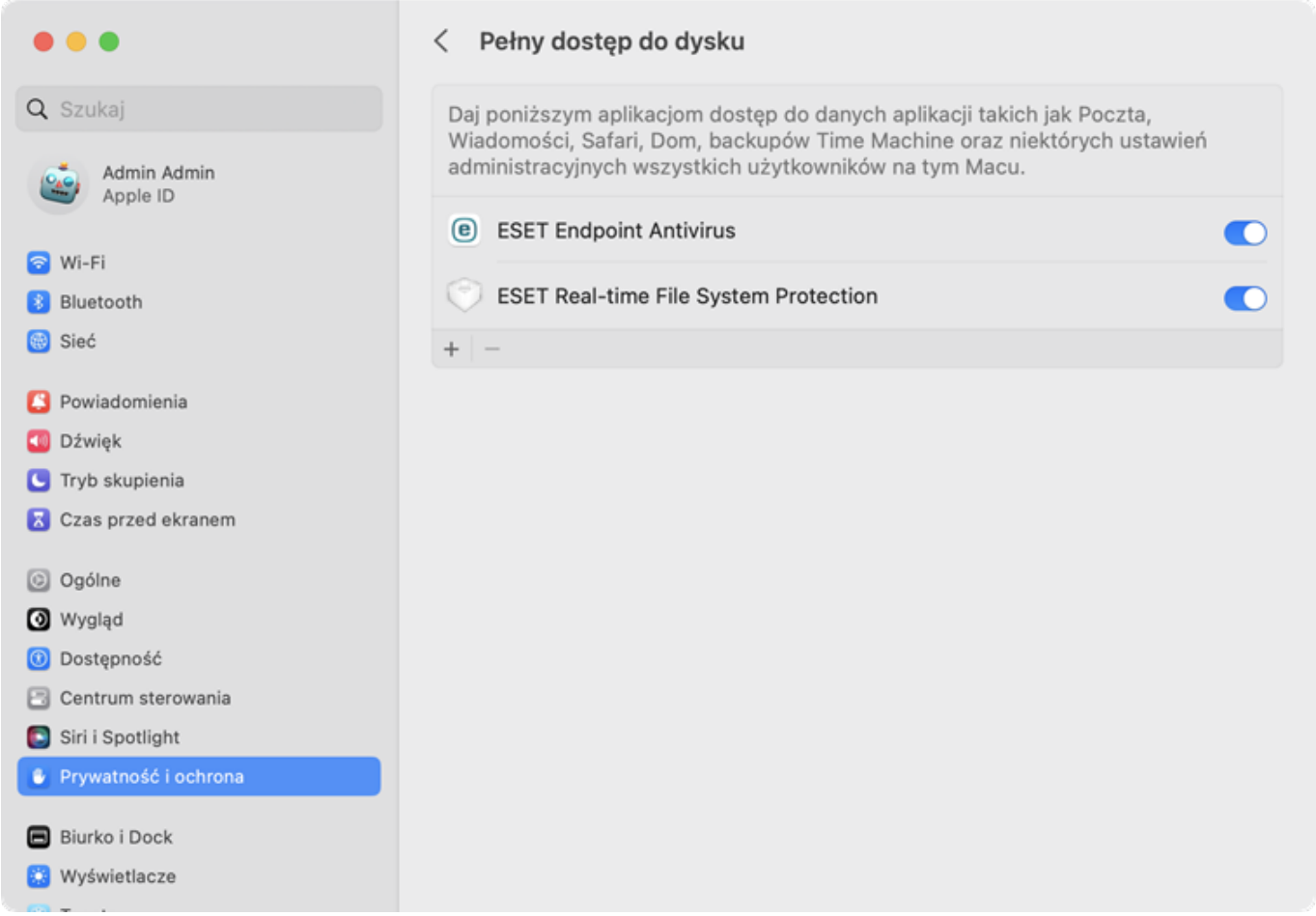
1. Otwórz **Preferencje systemowe**.
2. Wybierz opcję **Ochrona i prywatność**.
3. Kliknij ikonę kłódki w lewym dolnym rogu, aby zezwolić na zmiany w oknie ustawień.
4. Użyj czytnika **Touch ID** lub kliknij pozycję **Użyj hasła** i wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **Odblokuj**.
5. Kliknij pozycję **Szczegóły**.
6. Wybierz wszystkie opcje **ESET Endpoint Antivirus for macOS**.
7. Kliknij przycisk **OK**.

Zezwalaj na pełny dostęp do dysku

Podczas pierwszej instalacji programu ESET Endpoint Antivirus for macOS należy zezwolić programowi ESET Endpoint Antivirus for macOS na ochronę rozszerzeń systemu oraz na **pełny dostęp do dysku**.

macOS Ventura (13) i nowsze wersje

1. Otwórz **Ustawienia systemu**.
2. Wybierz **Prywatność i bezpieczeństwo** z menu po lewej stronie.
3. Kliknij opcję **Pełny dostęp do dysku**, a następnie kliknij przełącznik ESET Endpoint Antivirus for macOS, aby ją włączyć.
4. Użyj czytnika **Touch ID** lub kliknij pozycję **Użyj hasła** i wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **Odblokuj**.
5. Jeśli zostanie wyświetlony monit o ponowne uruchomienie ESET Endpoint Antivirus for macOS, kliknij przycisk **Później**.
6. Kliknij przełącznik **Ochrona systemu plików w czasie rzeczywistym ESET**, aby ją włączyć.



macOS Monterey (12) i starsze wersje

1. Otwórz **Preferencje systemowe**.
2. Przejdź do karty **Prywatność** i wybierz **Pełny dostęp do dysku** z menu po lewej stronie.
3. Kliknij ikonę kłódki w lewym dolnym rogu, aby zezwolić na zmiany w oknie ustawień.
4. Użyj czytnika **Touch ID** lub kliknij pozycję **Użyj hasła** i wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **Odblokuj**.
5. Wybierz **ESET Endpoint Antivirus for macOS** z listy.
6. Zostanie wyświetlone powiadomienie o ponownym uruchomieniu ESET Endpoint Antivirus for macOS. Kliknij przycisk **Później**.
7. Z listy wybierz pozycję **Ochrona systemu plików w czasie rzeczywistym ESET**.

> Jeśli opcja **Ochrona systemu plików w czasie rzeczywistym** jest niedostępna, należy najpierw zezwolić na rozszerzenia systemu, wykonując czynności przedstawione tutaj.

8. Kliknij przycisk **Uruchom ponownie** w oknie dialogowym alertu, aby ponownie uruchomić program ESET Endpoint Antivirus for macOS i wprowadzić zmiany lub ponownie uruchom komputer. Aby uzyskać bardziej szczegółowe informacje, odwiedź nasz artykuł bazy wiedzy.

Instalacja przy użyciu wiersza polecenia

Pomiń instalację graficznego interfejsu użytkownika, instalując ESET Endpoint Antivirus for macOS za pomocą wiersza poleceń. Jeśli komputer nie jest zarejestrowany w MDM, nadal trzeba będzie ręcznie zezwolić użytkownikowi na uprawnienia dostępu ESET Endpoint Antivirus for macOS w Ustawieniach systemu.

> Jeśli do zdalnej instalacji ESET Endpoint Antivirus for macOS używasz instalacji z wiersza polecenia, zaleca się dystrybucję profili konfiguracji z ustawieniami zgody użytkownika za pośrednictwem MDM przed instalacją ESET Endpoint Antivirus for macOS. Ustawienia profilu konfiguracji można znaleźć w temacie Ustawienia przedinstalacyjne.

1. Pobieranie ESET Endpoint Antivirus for macOS.

2. Aby zamontować pobrany plik .dmg, kliknij go dwukrotnie lub użyj następującego procesu w wierszu polecenia:

   a.W Terminalu przejdź do lokalizacji pliku. Wpisz: `cd ~/Downloads`
   Zastąp `Downloads` lokalizacją pobranego pliku.

   b.Wpisz: `hdiutil attach eea_osx_mlp_0.dmg`.
   Zastąp `eea_osx_mlp_0` nazwą swojego pliku.

3. W terminalu wpisz: `sudo installer -pkg /Volumes/ESET\ Endpoint\ Antivirus/.resources/Installer.pkg -target /`
Może być konieczne zastąpienie ścieżki do pliku Installer.pkg lokalizacją swojego pliku Installer.pkg.

4. Po zakończeniu instalacji należy zezwolić na ustawienia zgody użytkownika w ESET Endpoint Antivirus for macOS we Wdrażaniu ręcznym, aby umożliwić pełną ochronę.

Instalacja zdalna

Przed instalacją

ESET Endpoint Antivirus for macOS wymaga ustawień uprawnień, które uniemożliwiają pełną zdalną instalację urządzenia bez zarejestrowania urządzenia w MDM. Jeśli urządzenie jest zarejestrowane w MDM, można użyć

MDM do dystrybucji tych ustawień za pośrednictwem profili konfiguracji. Jeśli urządzenie nie jest zarejestrowane w MDM, te ustawienia uprawnień muszą być dozwolone ręcznie na każdym komputerze.

Jeśli używasz Jamf, możesz skorzystać też z naszego przewodnika po Jamf.

Ustawianie profilów konfiguracji do ESET Endpoint Antivirus for macOS

Przed zainstalowaniem ESET Endpoint Antivirus for macOS należy włączyć następujące ustawienia na komputerach docelowych:

- **Rozszerzenia systemu ESET**
  Jeśli rozszerzenia systemu ESET nie będą włączone przed instalacją, użytkownicy otrzymają powiadomienia o zablokowanych rozszerzeniach systemu do czasu włączenia rozszerzeń systemu ESET.

- **Pełny dostęp do dysku**
  Jeśli pełny dostęp do dysku nie będzie włączony przed instalacją, użytkownicy otrzymają powiadomienia o częściowej ochronie komputera, dopóki nie zostanie włączony pełny dostęp do dysku.

- **Ochrona stron internetowych i poczty e-mail**
  Aby ochrona dostępu do stron internetowych i poczty e-mail działała, należy dodać konfigurację ochrony dostępu do stron internetowych i poczty e-mail do ustawień systemu.
  Jeśli po instalacji ESET Endpoint Antivirus for macOS brakuje konfiguracji ochrony dostępu do stron internetowych i poczty e-mail, użytkownicy otrzymają komunikat „ ESET Endpoint Antivirus for macOS” chce filtrować zawartość sieciową. Po otrzymaniu tego powiadomienia kliknij przycisk Zezwól. Jeśli klikniesz przycisk Nie zezwalaj, ochrona dostępu do stron internetowych i poczty e-mail nie będzie działać.

Aby zdalnie włączyć powyższe ustawienia ESET, komputer musi być zarejestrowany na serwerze MDM (Mobile Device Management), takim jak Jamf.

Włącz na rozszerzenia systemu ESET

Aby zdalnie włączyć rozszerzenia systemu na urządzeniu, przed instalacją wykonaj jedną z następujących czynności:

- Pobierz pakiet danych .plist. Utwórz profil konfiguracji na serwerze MDM przy użyciu pliku danych `.plist`.

- Utwórz profil konfiguracji na serwerze MDM przy użyciu następujących ustawień:

Identyfikator zespołu (TeamID)	`P8DQRXPVLP`
Identyfikator pakietu (BundleID)	`com.eset.endpoint` `com.eset.network`

Zezwól na pełny dostęp do dysku

Aby zdalnie włączyć pełny dostęp do dysku, przed instalacją wykonaj jedną z następujących czynności:

- Pobierz plik pakietu danych .plist dla programu ESET Endpoint Antivirus for macOS. Utwórz profil konfiguracji na serwerze MDM przy użyciu pakietu danych `.plist`.
  Jeśli urządzenie jest zarządzane przez ESET PROTECT On-Prem lub ESET PROTECT CLOUD, należy również włączyć pełen dostęp do dysku dla programu ESET Management Agent. Pobierz plik pakietu danych .plist dla programu ESET Management Agent.

oUtwórz profil konfiguracji przy użyciu następujących ustawień:

ESET Endpoint Antivirus	
Identyfikator	`com.eset.eea.g2`
Typ identyfikatora	`bundleID`
Wymagania dot. kodu	`identifier "com.eset.eea.g2" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Aplikacja lub usługa	`SystemPolicyAllFiles`
Dostęp	`Allow`

Identyfikator	`com.eset.endpoint`
Typ identyfikatora	`bundleID`
Wymagania dot. kodu	`identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Aplikacja lub usługa	`SystemPolicyAllFiles`
Dostęp	`Allow`

Na macOS 12 Monterey lub nowszych wersjach	
Identyfikator	`com.eset.app.Uninstaller`
Typ identyfikatora	`bundleID`
Wymagania dot. kodu	`identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Aplikacja lub usługa	`SystemPolicyAllFiles`
Dostęp	`Allow`

ESET Management Agent	
Identyfikator	`com.eset.remoteadministrator.agent`
Typ identyfikatora	`bundleID`
Wymagania dot. kodu	`identifier "com.eset.remoteadministrator.agent" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Aplikacja lub usługa	`SystemPolicyAllFiles`
Dostęp	`Allow`

Po zdalnym umożliwieniu pełnego dostępu do dysku i rozszerzeń systemu w Ustawieniach systemu > Bezpieczeństwo i prywatność, ustawienia te mogą wyglądać na wyłączone. Jeśli ESET Endpoint Antivirus for macOS nie wyświetla żadnych ostrzeżeń, pełny dostęp do dysku i rozszerzenia systemu są dozwolone, niezależnie od ich stanu w oknie Ustawienia systemu > Bezpieczeństwo i prywatność.

Ochrona stron internetowych i poczty e-mail

Aby zdalnie dodać konfigurację ochrony dostępu do stron internetowych i poczty e-mail do ustawień systemu, przed instalacją wykonaj jedną z następujących czynności:

- Pobierz plik pakietu danych .plist. Utwórz profil konfiguracji na serwerze MDM przy użyciu pakietu danych `.plist`. Komputer musi być zarejestrowany na serwerze MDM, aby wdrożyć profile konfiguracji na tych komputerach.

- Aby utworzyć profil konfiguracji, utwórz profil konfiguracji typu VPN z następującymi ustawieniami:

Typ VPN	VPN
Typ połączenia	Custom SSL
Identyfikator niestandardowego połączenia SSL VPN	com.eset.network.manager
Serwer	localhost
Identyfikator pakietu dostawcy	com.eset.network
Uwierzytelnianie użytkownika	Certyfikat
Typ dostawcy	App-proxy
Wymóg wyznaczony przez dostawcę	identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Włącz VPN na żądanie	✓
XML konfiguracji reguł na żądanie	<array> <dict> <key>Action</key> <string>Connect</string> </dict> </array>
Zegar bezczynności	Nie rozłączaj
Konfiguracja serwera proxy	Brak

Konfiguracja ochrony dostępu do stron internetowych i poczty e-mail jest usuwana po odinstalowaniu programu ESET Endpoint Antivirus for macOS. Jeśli konieczne jest odinstalowanie i zainstalowanie ESET Endpoint Antivirus for macOS, po odinstalowaniu należy wdrożyć ponownie konfigurację ochrony dostępu do stron internetowych i poczty e-mail na komputerze docelowym.

Ustawienia przed instalacją Jamf

W oknie głównym Jamf kliknij **Komputery** > **Profile konfiguracji**.

Ochrona stron internetowych i poczty e-mail

Aby ochrona dostępu do stron internetowych i poczty e-mail działała, należy dodać konfigurację ochrony dostępu do stron internetowych i poczty e-mail do ustawień systemu. Jeśli po instalacji ESET Endpoint Antivirus for macOS brakuje konfiguracji ochrony dostępu do stron internetowych i poczty e-mail, użytkownicy otrzymają komunikat „ESET Endpoint Antivirus for macOS” chce filtrować zawartość sieciową.

Konfiguracja ochrony dostępu do stron internetowych jest usuwana po odinstalowaniu ESET Endpoint Antivirus for macOS. Jeśli konieczne jest odinstalowanie i zainstalowanie programu ESET Endpoint Antivirus for macOS, należy wdrożyć ponownie konfigurację ochrony dostępu do stron internetowych i poczty e-mail na komputerze docelowym.

W sekcji **Ogólne** podaj:

Nazwa	na przykład ESET Web&Email Protection
Poziom	Poziom komputera
Metoda dystrybucji	zwykle: Zainstaluj automatycznie

W sekcji **VPN** podaj:

Typ VPN	VPN
Typ połączenia	Niestandardowy certyfikat SSL
Identyfikator	com.eset.network.manager
serwer	localhost
Identyfikator pakietu dostawcy	com.eset.network
Uwierzytelnianie użytkownika	Certyfikat
Typ dostawcy	App-proxy
Wymóg wyznaczony przez dostawcę	identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Certyfikat tożsamości	Brak
Włącz VPN na żądanie	✓
XML konfiguracji reguł na żądanie	<array> <dict> <key>Action</key> <string>Connect</string> </dict> </array>
Zegar bezczynności	Nie rozłączaj
Konfiguracja serwera proxy	Brak

Włącz na rozszerzenia systemu ESET

W sekcji **Ogólne** podaj:

Nazwa	na przykład ESET SEXT
Poziom	Poziom komputera
Metoda dystrybucji	zwykle, Zainstaluj automatycznie

W sekcji **Rozszerzenia systemu** podaj:

Nazwa wyświetlana	na przykład ESET SEXT
Typy rozszerzeń systemowych	Dozwolone rozszerzenia systemu
Identyfikator zespołu	P8DQRXPVLP
Dozwolone rozszerzenia systemu	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

---

Zezwól na pełny dostęp do dysku

W sekcji **Ogólne** podaj:

Nazwa	na przykład ESET Pełny dostęp do dysku
Poziom	Poziom komputera
Metoda dystrybucji	zwykle, Zainstaluj automatycznie

W sekcji **Kontrola preferencji zasad prywatności** wypełnij:

Identyfikator	com.eset.endpoint
Typ identyfikatora	Identyfikator pakietu
Wymagania dot. kodu	identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikacja lub usługa	SystemPolicyAllFiles
Dostęp	Zezwól

Identyfikator	com.eset.devices
Typ identyfikatora	Identyfikator pakietu
Wymagania dot. kodu	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikacja lub usługa	SystemPolicyAllFiles
Dostęp	Zezwól

Identyfikator	com.eset.eea.g2
Typ identyfikatora	Identyfikator pakietu
Wymagania dot. kodu	identifier "com.eset.eea.g2" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikacja lub usługa	SystemPolicyAllFiles
Dostęp	Zezwól

Identyfikator	com.eset.app.Uninstaller
Typ identyfikatora	Identyfikator pakietu
Wymagania dot. kodu	identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikacja lub usługa	SystemPolicyAllFiles
Dostęp	Zezwól

Po zdalnym umożliwieniu pełnego dostępu do dysku i rozszerzeń systemu w Ustawieniach systemu > Bezpieczeństwo i prywatność, ustawienia te mogą wyglądać na wyłączone. Jeśli ESET Endpoint Antivirus for macOS nie wyświetla żadnych ostrzeżeń, pełny dostęp do dysku i rozszerzenia systemu są dozwolone, niezależnie od ich stanu w oknie Ustawienia systemu > Bezpieczeństwo i prywatność.

Wdrożenie za pomocą konsoli zarządzania ESET

ESET Endpoint Antivirus for macOS wymaga ustawień uprawnień, które uniemożliwiają pełną zdalną instalację urządzenia bez zarejestrowania urządzenia w MDM. Jeśli urządzenie jest zarejestrowane w MDM, można użyć MDM do dystrybucji tych ustawień za pośrednictwem profili konfiguracji. Jeśli urządzenie nie jest zarejestrowane w MDM, te ustawienia uprawnień muszą być dozwolone ręcznie na każdym komputerze.

ESET PROTECT On-Prem

Przed wdrożeniem ESET Endpoint Antivirus for macOS za pomocą ESET PROTECT On-Prem programu należy rozesłać agenta ESET Management Agent na komputer docelowy.

1. Aby zainstalować agenta ESET Management Agent, należy utworzyć Live Installer agenta.

2. Pobierz macOS Agent Live Installer.

3. Wyodrębnij skrypt .sh z pobranego archiwum .tar.gz.

4. Wdróż i uruchom skrypt .sh na komputerze docelowym, aby zainstalować agenta. Jeśli używasz Jamf jako MDM, możesz użyć Jamf do wdrożenia i uruchomienia skryptu.

5. Po zainstalowaniu agenta na komputerze docelowym komputer będzie widoczny w programie ESET PROTECT On-Prem.

Aby zainstalować ESET Endpoint Antivirus for macOS utwórz i uruchom zadanie instalacji oprogramowania w programie ESET PROTECT On-Prem.

ESET PROTECT CLOUD

Można zainstalować ESET Endpoint Antivirus for macOS za pośrednictwem ESET PROTECT CLOUD i agenta ESET Management Agent równocześnie, tworząc instalatora Live installer.

Jeśli posiadasz licencję połączoną z Twoim ESET PROTECT On-Prem lub ESET PROTECT CLOUD, to licencja zostanie automatycznie dodana do pakietu instalacyjnego i ESET Endpoint Antivirus for macOS zostanie aktywowana automatycznie.

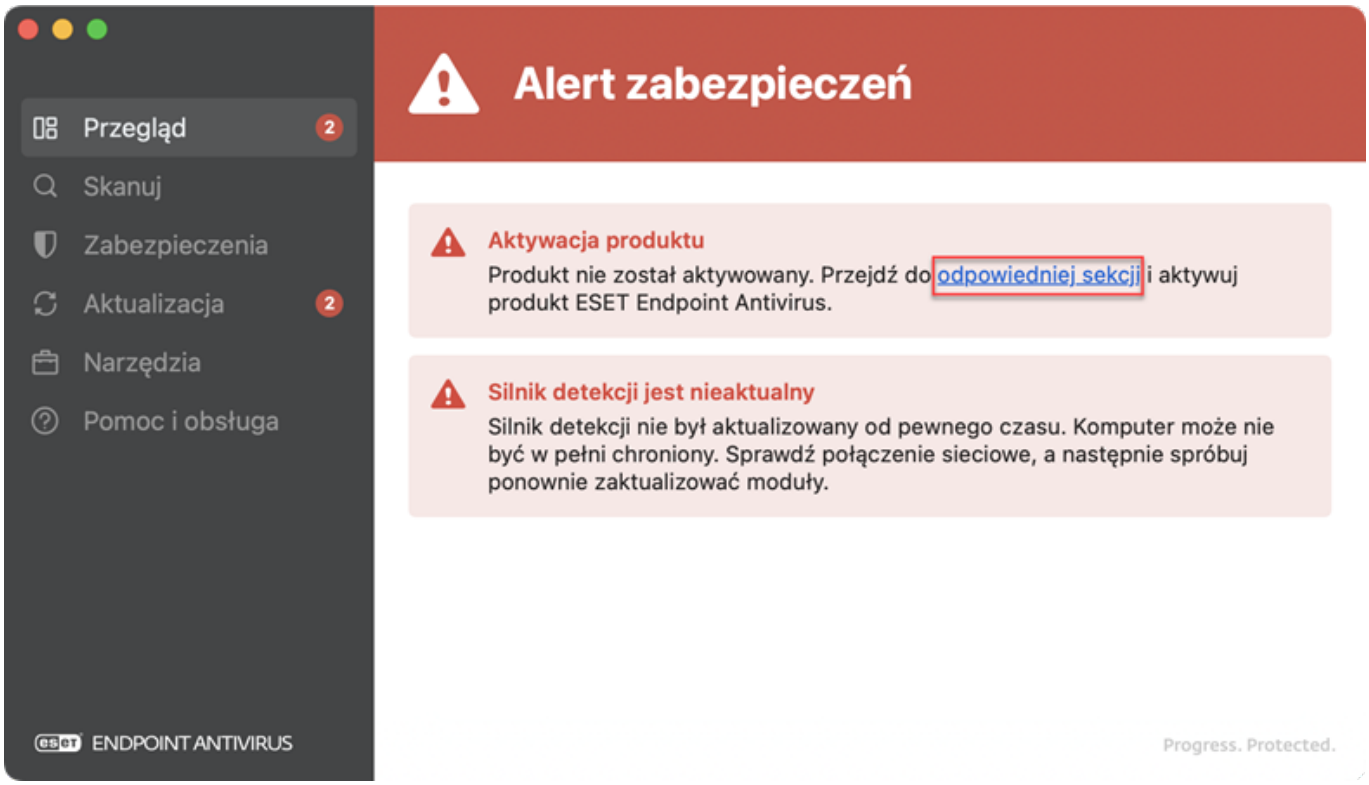
Gdzie znajdę licencja?

Jeśli zakupiono licencję, użytkownik powinien otrzymać dwie wiadomości e-mail od firmy ESET. Pierwsza wiadomość e-mail zawiera informacje o portalu ESET Business Account . Druga wiadomość e-mail zawiera szczegółowe informacje o kluczu licencyjnym (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX), publicznym identyfikatorze licencji (xxx-xxx-xxx), nazwie produktu (lub o liście produktów) i o ilości.

Aktywacja lokalna

1. Otwórz ESET Endpoint Antivirus for macOS.

2. W alercie zabezpieczeń aktywacji produktu kliknij okno dialogowe Aktywacja.



3. Po otwarciu okna dialogowego aktywacji wpisz klucz licencyjny i kliknij przycisk Kontynuuj.

4. Kliknij przycisk Zakończ.

Aktywacja poprzez terminal

Użyj narzędzia `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic` jako uprzywilejowanego użytkownika, aby aktywować ESET Endpoint Antivirus for macOS z poziomu okna Terminala.

Składnia: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic [OPTIONS]`

Przykład

Poniższe polecenia musi wykonywać użytkownik uprzywilejowany.

Aktywacja przy użyciu klucza licencyjnego

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic -k XXXX-XXXX-XXXX-XXXX-XXXX
```

lub

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
```

natomiast `XXXX-XXXX-XXXX-XXXX-XXXX` reprezentuje klucz ESET Endpoint Antivirus for macOS licencyjny.

Zdalna aktywacja

Jeśli instalujesz ESET Endpoint Antivirus for macOS za pośrednictwem ESET PROTECT On-Prem lub ESET PROTECT CLOUD i posiadasz licencję połączoną z Twoim ESET PROTECT On-Prem lub ESET PROTECT CLOUD, to licencja zostanie automatycznie dodana do pakietu instalacyjnego i ESET Endpoint Antivirus for macOS zostanie aktywowana automatycznie.

Aktywuj ESET Endpoint Antivirus for macOS zdalnie za pomocą ESET PROTECT On-Prem

Aby przeprowadzić aktywację ESET Endpoint Antivirus for macOS za pośrednictwem ESET PROTECT On-Prem lub konsoli internetowej ESET PROTECT CLOUD internetowej, zaloguj się do konsoli internetowej ESET PROTECT On-Prem i użyj zadania klienta Aktywacja produktu.

Dokumentacja dotycząca punktów końcowych zarządzanych zdalnie

Wersją 7 programu ESET Endpoint Antivirus for macOS można zarządzać zdalnie za pośrednictwem ESET PROTECT On-Prem lub ESET PROTECT CLOUD. Za pomocą narzędzi do zdalnego zarządzania firmy ESET można wdrażać rozwiązania ESET, zarządzać zadaniami, egzekwować polityki bezpieczeństwa, monitorować stan systemu i szybko reagować na problemy lub zagrożenia na komputerach zdalnych z jednej centralnej lokalizacji.

Narzędzia do zdalnego zarządzania ESET

ESET Endpoint Antivirus for macOS można zarządzać zdalnie za pomocą konsoli zarządzania ESET.

- Wprowadzenie do ESET PROTECT On-Prem
- Wprowadzenie do ESET PROTECT CLOUD

Mobile Device Management (MDM)

Aby zainstalować ESET Endpoint Antivirus for macOS zdalnie, urządzenia muszą być zarejestrowane w MDM. Jeśli urządzenia nie są zarejestrowane w MDM, musisz fizycznie uzyskać dostęp do każdego urządzenia, aby zainstalować ESET Endpoint Antivirus for macOS.

Rozwiązania do zarządzania urządzeniami mobilnymi (MDM) umożliwiają administratorom wdrażanie zasad organizacyjnych i konfiguracyjnych, monitorowanie urządzeń, instalowanie lub odinstalowywanie aplikacji i wiele więcej. Nie wszystkie rozwiązania MDM obsługują urządzenia Apple. Aby pomóc w wyborze rozwiązania MDM, firma Apple utworzyła przewodnik Wybierz rozwiązanie MDM.

Więcej informacji na temat MDM można znaleźć w dokumentacji Apple i dokumentacji specyficznej dla dostawcy MDM.

Konfiguracja ESET Endpoint Antivirus for macOS, która jest wymagana do wykonania za pośrednictwem MDM, zawiera uniwersalne ładunki do pobrania, których można użyć do tworzenia profili konfiguracji na dowolnym MDM. Jeśli używasz Jamf jako MDM, możesz również użyć przewodnika specyficznego dla Jamf.

Konfiguracja produktu w ESET PROTECT On-Prem

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

Silnik detekcji

Silnik detekcji chroni system przed złośliwym oprogramowaniem, kontrolując pliki. Jeśli na przykład zostanie wykryty obiekt sklasyfikowany jako szkodliwe oprogramowanie, rozpocznie się naprawa. Silnik detekcji najpierw blokuje zagrożenie, a następnie je leczy, usuwa lub przenosi do kwarantanny.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W Silniku detekcji można skonfigurować następujące ustawienia:

Podstawowe

Opcje skanera

Włącz wykrywanie potencjalnie niepożądanych aplikacji — zobacz Potencjalnie niepożądane aplikacje w naszym słowniczku.

Włącz wykrywanie potencjalnie niebezpiecznych aplikacji — zobacz Potencjalnie niebezpieczne aplikacje w naszym glosariuszu.

Włącz wykrywanie podejrzanych aplikacji — Podejrzane aplikacje to oprogramowanie skompresowane za pomocą programu pakującego lub zaszyfrowane przy wykorzystaniu zastrzeżonych metod, co ma na celu uniemożliwienie inżynierii wstecznej (odczytu pliku) oraz zaciemniania kodu aplikacji (np. w celu ukrycia szkodliwego oprogramowania).

Kategoria ta obejmuje wszystkie nieznane aplikacje, które zostały skompresowane programem pakującym lub zaszyfrowane z użyciem zastrzeżonych metod, często używanych do ukrywania szkodliwego oprogramowania.

Wyłączenia

Pliki i foldery wyłączone ze skanowania — poprzez wyłączenie ścieżek (folderów) ze skanowania można znacznie skrócić czas potrzebny na skanowanie systemu plików pod kątem obecności szkodliwego oprogramowania.

Aby utworzyć wyłączenie:

1. Kliknij Edytuj obok pozycji Pliki i foldery wyłączone ze skanowania.

2. Kliknij przycisk Dodaj i zdefiniuj ścieżkę, która ma zostać pominięta przez skaner. Opcjonalnie dodaj komentarz do swoich informacji.

3. Kliknij przycisk OK > Zapisz, aby utworzyć wyłączenie i zamknąć okno dialogowe.

Ochrona systemu plików w czasie rzeczywistym

Ochrona systemu plików w czasie rzeczywistym sprawdza wszystkie zdarzenia związane z ochroną antywirusową systemu. Wszystkie pliki w momencie otwarcia, utworzenia lub uruchomienia na komputerze są skanowane w poszukiwaniu szkodliwego kodu. Domyślnie Ochrona systemu plików w czasie rzeczywistym jest włączana przy uruchamianiu systemu i zapewnia nieprzerwane skanowanie.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Silnik detekcji > Ochrona systemu plików w czasie rzeczywistym można skonfigurować następujące ustawienia:

Podstawowe

Ochrona systemu plików 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) można wyłączyć Ochrona systemu plików w czasie rzeczywistym poprzez kliknięcie paska suwaka obok opcji Włącz ochronę systemu plików w czasie rzeczywistym.

Skanowane nośniki

Domyślnie wszystkie typy nośników są skanowane w celu wykrycia potencjalnych zagrożeń:

- Dyski lokalne — sprawdzane są wszystkie dyski twarde w komputerze.
- Nośniki wymienne — sprawdzane są płyty CD i DVD, urządzenia pamięci masowej USB, urządzenia Bluetooth itp.
- Dyski sieciowe — skanowane są wszystkie dyski mapowane.

Firma ESET zaleca korzystanie z ustawień domyślnych i modyfikowanie ich wyłącznie w szczególnych przypadkach, jeśli na przykład skanowanie pewnych nośników znacznie spowalnia przesyłanie danych.

Skanuj podczas

Domyślnie wszystkie pliki są skanowane podczas otwierania, tworzenia i wykonywania. Zalecane jest zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalny poziom ochrony komputera w czasie rzeczywistym:

- Otwierania pliku — włącza lub wyłącza skanowanie plików przy ich otwieraniu.
- Tworzenia pliku — włącza lub wyłącza skanowanie plików przy ich tworzeniu.
- Dostęp do nośników wymiennych — włącza lub wyłącza automatyczne skanowanie nośników wymiennych podczas podłączania do komputera.

Wyłączenia procesów

Procesy, które mają być wykluczone ze skanowania — poprzez wykluczenie procesów ze skanowania czas potrzebny na skanowanie systemu pod kątem obecności szkodliwego oprogramowania może zostać znacznie skrócony.

Aby utworzyć wyłączenie:

1. Kliknij Edytuj obok pozycji Procesy, które mają być wykluczone ze skanowania.
2. Kliknij przycisk Dodaj i podaj ścieżkę do pliku wykonywalnego.
3. Kliknij przycisk Zapisz > Zapisz, aby utworzyć wyłączenie i zamknąć okno dialogowe.

Parametry technologii ThreatSense

Moduł ochrony systemu plików w czasie rzeczywistym sprawdza wszystkie typy nośników. Sprawdzanie jest wywoływane wystąpieniem różnych zdarzeń systemowych, na przykład uzyskaniem dostępu do pliku. Korzystając z metod wykrywania zastosowanych w ramach technologii ThreatSense (opisanych w sekcji Ustawienia parametrów technologii ThreatSense, funkcja ochrony systemu plików w czasie rzeczywistym może działać inaczej w przypadku plików nowo tworzonych, a inaczej w przypadku już istniejących. Na przykład funkcję ochrony systemu plików w czasie rzeczywistym można skonfigurować na dokładniejsze monitorowanie nowo utworzonych plików.

Ochrona oparta na chmurze

ESET LiveGrid® to zaawansowany system wczesnego ostrzegania składający się z kilku technologii opartych na chmurze. Pomaga wykrywać pojawiające się zagrożenia na podstawie reputacji i poprawia wydajność skanowania wykorzystujący białą listę.

Domyślnie w programie ESET Endpoint Antivirus for macOS skonfigurowane jest przesyłanie podejrzanych plików do analizy w laboratorium firmy ESET. Pliki z określonymi rozszerzeniami, takimi jak *.doc* lub *.xls*, są zawsze wyłączane z procesu przesyłania. Można również dodać inne rozszerzenia, jeśli istnieją pliki, które użytkownik lub jego firma życzy sobie wyłączyć z procesu przesyłania.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Silnik detekcji > Ochrona oparta na chmurze można skonfigurować następujące ustawienia:

Ochrona oparta na chmurze

Włączenie systemu reputacji ESET LiveGrid® (zalecane)

System reputacji ESET LiveGrid® poprawia wydajność rozwiązań firmy ESET do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.

Włączenie systemu informacji zwrotnych ESET LiveGrid®

Dane zostaną przesłane do dalszej analizy w laboratorium firmy ESET.

Wysyłaj raporty o awariach i dane diagnostyczne

Wysyłaj dane, takie jak raporty o awariach, modułach czy zrzuty pamięci.

Pomóż w usprawnianiu produktu, przesyłając anonimowe dane statystyczne dotyczące jego używania

Zezwól firmie ESET na zbieranie anonimowych informacji o nowo wykrytych zagrożeniach, takich jak nazwa zagrożenia, data i godzina jego wykrycia, metoda wykrycia i skojarzone metadane, informacje o przeskanowanych plikach (skrót, nazwa pliku, pochodzenie pliku i telemetria), zablokowanych i podejrzanych adresach URL, wersja i konfiguracja produktu. Uwzględnione są także informacje o systemie użytkownika.

Kontaktowy adres e-mail (opcjonalnie)

Wraz z podejrzanymi plikami można wysyłać adres e-mail, który będzie używany do kontaktowania się z użytkownikiem, gdy przeprowadzenie analizy będzie wymagało dodatkowych informacji. Uwaga: użytkownik nie otrzyma odpowiedzi od firmy ESET, jeśli nie będą potrzebne dodatkowe informacje.

Przesyłanie próbek

Automatyczne przesyłanie wykrytych próbek

W zależności od wybranej opcji można przesyłać zainfekowane próbki do laboratorium firmy ESET w celu ich przeanalizowania i udoskonalenia wykrycia w przyszłości.

- Wszystkie zainfekowane próbki
- Wszystkie próbki oprócz dokumentów
- Nie przesyłaj

Automatyczne przesyłanie podejrzanych próbek

Podejrzane próbki przypominające zagrożenia i takie, których zawartość lub działanie jest nietypowe, są przesyłane do laboratorium firmy ESET w celu wykonania analizy.

Pliki wykonywalne — obejmuje pliki wykonywalne, na przykład: *.exe*, *.dll*, *.sys*

Archiwa — obejmuje takie typy archiwów jak: *.zip*, *.rar*, *.7z*, *.arch*, *.arj*, *.bzip2*, *.gzip*, *.ace*, *.arc*, *.cab*

Skrypty — obejmuje takie typy skryptów jak: *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *, .ps1*

Inne — obejmuje następujące typy plików: *.jar*, *.reg*, *.msi*, *.swf*, *.lnk*

Dokumenty — obejmuje dokumenty utworzone w pakiecie Microsoft Office, pakiecie Libre Office lub innym narzędziu pakietu Office albo pliki PDF z zawartością aktywną.

Wyłączenia

Kliknij Edytuj obok pozycji Wyłączenia, aby wykluczyć określone pliki lub foldery z przesyłania. Wykluczone pliki nie zostaną wysłane do laboratorium firmy ESET, nawet jeśli zawierają podejrzany kod.

Maksymalny rozmiar próbek (MB)

Określ maksymalny rozmiar próbek.

Skanowania w poszukiwaniu szkodliwego oprogramowania

Skaner na żądanie jest ważną częścią rozwiązania antywirusowego i służy do skanowania plików i folderów na komputerze. Z punktu widzenia bezpieczeństwa ważne jest, aby skanowanie komputera było wykonywane regularnie w ramach rutynowych środków bezpieczeństwa, a nie tylko w przypadku podejrzenia infekcji.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Silnik detekcji > Skanowanie szkodliwego oprogramowania można skonfigurować opcje profili skanowania na żądanie:

Wybrany profil — wybierz profil do edycji.

Lista profili — aby utworzyć nowy profil lub usunąć istniejący, kliknij przycisk Edytuj. Wpisz nazwę profilu i kliknij przycisk Dodaj. Nowy profil zostanie wyświetlony w menu rozwijanym Wybrany profil, które zawiera menu rozwijane z listą istniejących profili skanowania.

Parametry ThreatSense — opcje konfiguracji profilu skanowania, takie jak rozszerzenia plików, które chcesz kontrolować, obiekty do skanowania, użyte metody wykrywania itp. Zobacz parametry ThreatSense, aby uzyskać szczegółowe informacje.

Parametry technologii ThreatSense

Technologia ThreatSense obejmuje wiele zaawansowanych metod wykrywania zagrożeń. Jest ona proaktywna, 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. Aparat skanowania może kontrolować kilka strumieni danych jednocześnie, co zwiększa do maksimum skuteczność i wskaźnik wykrywalności. Ponadto technologia ThreatSense skutecznie eliminuje programy typu rootkit.

Opcje ustawień technologii ThreatSense pozwalają określić kilka parametrów skanowania:

- typy i rozszerzenia plików, które mają być skanowane;

- kombinacje różnych metod wykrywania;
- poziomy leczenia itp.

Różne scenariusze zabezpieczeń mogą wymagać różnych konfiguracji. Mając to na uwadze, technologię ThreatSense można konfigurować indywidualnie dla następujących modułów ochrony:

- Ochrona systemu plików w czasie rzeczywistym
- Skanowania w poszukiwaniu szkodliwego oprogramowania
- Ochrona dostępu do stron internetowych
- Ochrona programów poczty e-mail

Parametry technologii ThreatSense są w wysokim stopniu zoptymalizowane pod kątem poszczególnych modułów, a ich modyfikacja może znacząco wpływać na działanie systemu. Na przykład ustawienie opcji skanowania spakowanych programów za każdym razem lub włączenie zaawansowanej heurystyki w module ochrony systemu plików w czasie rzeczywistym może spowodować spowolnienie działania systemu (normalnie tymi metodami skanowane są tylko nowo utworzone pliki). Zaleca się pozostawienie niezmienionych parametrów domyślnych technologii dla wszystkich modułów z wyjątkiem modułu Skanowanie komputera.

Skanowane obiekty

W sekcji Obiekty można określić, które pliki i składniki komputera będą skanowane w poszukiwaniu infekcji.

Pliki poczty — program obsługuje następujące rozszerzenia: DBX (Outlook Express) oraz EML.

Archiwa — program obsługuje następujące rozszerzenia: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE i wiele innych.

Archiwa samorozpakowujące— archiwa samorozpakowujące (SFX) to archiwa, które rozpakowują się same.

Programy pakujące w czasie wykonywania — po uruchomieniu — w odróżnieniu od archiwów standardowych — dekompresują swoją zawartość do pamięci. Poza standardowymi statycznymi programami spakowanymi (np. UPX, yoda, ASPack, FSG) skaner umożliwia również rozpoznawanie kilku innych typów programów spakowanych, dzięki emulowaniu ich kodu.

Opcje skanowania

Tu można wybrać metody stosowane podczas skanowania systemu w poszukiwaniu infekcji. Dostępne są następujące opcje:

Heurystyka— heurystyka jest metodą analizy pozwalającą wykrywać działanie szkodliwych programów. Główną zaletą tej technologii jest to, że umożliwia wykrywanie szkodliwego oprogramowania, które w chwili pobierania ostatniej aktualizacji bazy danych sygnatur wirusów jeszcze nie istniało lub nie było w niej ujęte. Wadą może być ryzyko (niewielkie) wystąpienia tzw. fałszywych alarmów.

Zaawansowana heurystyka/sygnatury DNA — zaawansowana heurystyka jest oparta na unikatowym algorytmie heurystycznym opracowanym przez firmę ESET. Został on napisany w językach programowania wysokiego poziomu i zoptymalizowany pod kątem wykrywania robaków i koni trojańskich. Zaawansowana heurystyka znacząco usprawnia wykrywanie zagrożeń w produktach ESET. Sygnatury pozwalają niezawodnie wykrywać i identyfikować wirusy. Dzięki systemowi automatycznej aktualizacji nowe sygnatury są udostępniane w ciągu kilku

godzin od stwierdzenia zagrożenia. Wadą sygnatur jest to, że pozwalają wykrywać tylko znane wirusy (lub ich nieznacznie zmodyfikowane wersje).

Leczenie

Parametry ThreatSense mają następujące poziomy leczenia:

Poziom leczenia	Opis
Brak leczenia	Użytkownik końcowy widzi interaktywne okno podczas leczenia obiektów i musi wybrać akcję (na przykład usunąć lub zignorować). Ten poziom jest przeznaczony dla bardziej zaawansowanych użytkowników, którzy wiedzą, jakie kroki należy podjąć w przypadku wykrycia.
Leczenie normalne	Podjęcie próby naprawienia wykrytego zagrożenia podczas leczenia obiektów bez interwencji użytkownika końcowego. W niektórych przypadkach (np. plików systemowych lub archiwów zawierających zarówno czyste, jak i zainfekowane pliki), kiedy zagrożenia nie można wyleczyć, obiekt pozostanie w pierwotnej lokalizacji.
Leczenie dokładne	Podjęcie próby naprawienia wykrytego zagrożenia podczas leczenia obiektów bez interwencji użytkownika końcowego. W niektórych rzadkich przypadkach (np. plików systemowych), jeśli nie można naprawić wykrycia, zgłoszony obiekt pozostanie w pierwotnej lokalizacji.
Leczenie dokładne	Podjęcie próby wyleczenia wykrytego zagrożenia podczas leczenia obiektów. W niektórych przypadkach, jeśli nie można wykonać żadnej akcji, użytkownikowi zostanie wyświetlony alert interaktywny umożliwiający wybór czynności w ramach leczenia (np. usunięcia lub zignorowania). To ustawienie jest zalecane w większości przypadków.
Usuń	Podjęcie próby usunięcia wszystkich zainfekowanych plików bez interwencji użytkownika końcowego.

Wyłączenia

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

Inne

Podczas konfigurowania ustawień parametrów technologii ThreatSense dotyczących skanowania komputera na żądanie w sekcji Inne dostępne są również następujące opcje:

Skanuj alternatywne strumienie danych (ADS) — alternatywne strumienie danych używane w systemie plików NTFS to skojarzenia plików i folderów, których nie można sprawdzić za pomocą standardowych technik skanowania. Wiele wirusów stara się uniknąć wykrycia, udając alternatywne strumienie danych.

Uruchom skanowanie w tle z niskim priorytetem — każde skanowanie wymaga użycia pewnej ilości zasobów systemowych. W przypadku używania programów, które wymagają dużej ilości zasobów systemowych, można uruchomić skanowanie w tle z niskim priorytetem, oszczędzając zasoby dla innych aplikacji.

Włącz inteligentną optymalizację — po włączeniu funkcji Inteligentna optymalizacja używane są optymalne ustawienia, które zapewniają połączenie maksymalnej skuteczności z największą szybkością skanowania. Poszczególne moduły ochrony działają w sposób inteligentny, stosując różne metody skanowania w przypadku różnych typów plików. Jeśli funkcja inteligentnej optymalizacji jest wyłączona, podczas skanowania są stosowane jedynie określone przez użytkownika dla poszczególnych modułów ustawienia technologii ThreatSense.

Zachowaj znacznik czasowy ostatniego dostępu — wybranie tej opcji pozwala zachować oryginalny znacznik czasowy dostępu do plików zamiast przeprowadzania ich aktualizacji (na przykład na potrzeby systemów wykonywania kopii zapasowych danych).

Limity

W sekcji Limity można określić maksymalny rozmiar obiektów i poziomy zagnieżdżonych archiwów, które mają być skanowane:

Ustawienia obiektów

Wyłącz suwak obok pozycji Domyślne ustawienia obiektu, aby skonfigurować następujące opcje:

Maksymalny rozmiar obiektu — określa maksymalny rozmiar obiektów do skanowania. Dany moduł antywirusowy będzie skanować tylko obiekty o rozmiarze mniejszym niż określony. Ta opcja powinna być modyfikowana tylko przez zaawansowanych użytkowników, którzy mają określone powody do wyłączenia większych obiektów ze skanowania. Wartość domyślna: bez limitu.

Maksymalny czas skanowania dla obiektu (s) — określa maksymalny czas skanowania obiektu. W przypadku wprowadzenia wartości zdefiniowanej przez użytkownika moduł antywirusowy zatrzyma skanowanie obiektu po upływie danego czasu, niezależnie od tego, czy skanowanie zostało ukończone. Wartość domyślna: bez limitu.

Ustawienia skanowania archiwów

Wyłącz suwak obok pozycji Domyślne ustawienia skanowania archiwów, aby skonfigurować następujące opcje:

Poziom zagnieżdżania archiwów — określa maksymalną głębokość skanowania archiwów. Wartość domyślna: 10.

Maksymalny rozmiar pliku w archiwum — ta opcja pozwala określić maksymalny rozmiar plików, które mają być skanowane w rozpakowywanych archiwach. Wartość domyślna: bez limitu.

> Nie zalecamy modyfikowania wartości domyślnych. W zwykłych warunkach nie ma potrzeby ich zmieniać.

Dodatkowe parametry ThreatSense

Te ustawienia są dostępne tylko dla ochrony systemu plików w czasie rzeczywistym.

Prawdopodobieństwo występowania infekcji w nowo utworzonych lub zmodyfikowanych plikach jest stosunkowo większe niż w przypadku istniejących już plików. Z tego powodu program sprawdza te pliki przy użyciu dodatkowych parametrów skanowania. Program ESET Endpoint Antivirus for macOS używa zaawansowanej heurystyki, która może wykryć nowe zagrożenia przed opublikowaniem aktualizacji silnika detekcji wraz z metodami skanowania opartymi na sygnaturach.

Poza nowo utworzonymi plikami skanowanie obejmuje również archiwa samorozpakowujące (.sfx) i programy spakowane (skompresowane wewnętrznie pliki wykonywalne). Domyślnie archiwa są skanowane do dziesiątego poziomu zagnieżdżenia i są sprawdzane niezależnie od ich rozmiaru. Aby zmienić ustawienia skanowania archiwów, należy usunąć zaznaczenie opcji Domyślne ustawienia skanowania archiwów.

Poziomy leczenia

Poziom leczenia	Opis
Brak leczenia	Użytkownik końcowy widzi interaktywne okno podczas leczenia obiektów i musi wybrać akcję (na przykład usunąć lub zignorować). Ten poziom jest przeznaczony dla bardziej zaawansowanych użytkowników, którzy wiedzą, jakie kroki należy podjąć w przypadku wykrycia.
Leczenie normalne	Podjęcie próby naprawienia wykrytego zagrożenia podczas leczenia obiektów bez interwencji użytkownika końcowego. W niektórych przypadkach (np. plików systemowych lub archiwów zawierających zarówno czyste, jak i zainfekowane pliki), kiedy zagrożenia nie można wyleczyć, obiekt pozostanie w pierwotnej lokalizacji.
Leczenie dokładne	Podjęcie próby naprawienia wykrytego zagrożenia podczas leczenia obiektów bez interwencji użytkownika końcowego. W niektórych rzadkich przypadkach (np. plików systemowych), jeśli nie można naprawić wykrycia, zgłoszony obiekt pozostanie w pierwotnej lokalizacji.
Leczenie dokładne	Podjęcie próby wyleczenia wykrytego zagrożenia podczas leczenia obiektów. W niektórych przypadkach, jeśli nie można wykonać żadnej akcji, użytkownikowi zostanie wyświetlony alert interaktywny umożliwiający wybór czynności w ramach leczenia (np. usunięcia lub zignorowania). To ustawienie jest zalecane w większości przypadków.
Usuń	Podjęcie próby usunięcia wszystkich zainfekowanych plików bez interwencji użytkownika końcowego.

Aktualizacja

Ta sekcja umożliwia określenie informacji o źródle aktualizacji, w tym używanych serwerów aktualizacji i dotyczących ich danych uwierzytelniających.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Aktualizacja umożliwia konfigurowanie następujących ustawień:

Podstawowe

Domyślnie Typ aktualizacji to Regularna aktualizacja. Dzięki temu baza sygnatur wykrywania i moduły produktów są automatycznie aktualizowane z serwerów aktualizacji ESET.

Aktualizacje w wersji wstępnej zawierają najnowsze poprawki błędów i metody wykrywania, które w najbliższej przyszłości będą dostępne dla ogółu użytkowników. Jednak mogą nie być stabilne przez cały czas; dlatego nie zaleca się ich używania w środowisku produkcyjnym.

Opóźnione aktualizacje umożliwiają aktualizowanie ze specjalnych serwerów aktualizacji udostępniających nowe wersje baz danych wirusów z opóźnieniem co najmniej X godzin (czyli baz danych przetestowanych w środowisku rzeczywistym i uznanych za stabilne).

Cofanie aktualizacji modułów

W razie podejrzeń, że nowa aktualizacja silnika detekcji lub modułów programu może być niestabilna lub uszkodzona, można skorzystać z zadania ESET PROTECT On-Prem w celu wykonania funkcji Cofanie aktualizacji modułów, aby wycofać zmiany i wrócić do poprzedniej wersji oraz wyłączyć aktualizacje na określony czas. Można także włączyć aktualizacje, które zostały wcześniej wyłączone na czas nieokreślony.

ESET Endpoint Antivirus for macOS zapisuje migawki silnika detekcji i modułów programu przeznaczone do użycia z funkcją cofania zmian. Aby tworzyć migawki modułu bazy danych wirusów, należy pozostawić włączony przełącznik opcji Utwórz migawki modułów. Gdy opcja ta jest włączona, pierwsza migawka tworzona jest przy pierwszej aktualizacji. Następna po 48 godzinach. Pole Liczba kopii przechowywanych lokalnieokreśla liczbę przechowywanych migawek silnika detekcji.

> Po osiągnięciu maksymalnej ilości migawek (na przykład trzy), najstarsza migawka jest zastępowana nową migawką co 48 godzin. ESET Endpoint Antivirus for macOS potrafi przywrócić wersję aparatu wykrywania i aktualizacji modułu programu do najstarszej migawki.

Kopia dystrybucyjna aktualizacji (niestandardowe serwery aktualizacji)

Korzystanie z kopii dystrybucyjnej, czyli kopii plików aktualizacji, w środowisku sieci LAN jest wygodne, ponieważ eliminuje potrzebę pobierania tych plików przez każdą stację roboczą bezpośrednio z serwera aktualizacji dostawcy. Aktualizacje są pobierane na lokalny serwer kopii dystrybucyjnych, a następnie dystrybuowane do wszystkich stacji roboczych, by uniknąć ryzyka generowania nadmiernego ruchu sieciowego. Aktualizowanie klienckich stacji roboczych przy użyciu kopii dystrybucyjnej pozwala na oszczędne korzystanie z przepustowości połączenia internetowego.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Aktualizacja > Główny serwer lub Serwer pomocniczy można skonfigurować ESET Endpoint Antivirus for macOS na używanie kopii dystrybucyjnej aktualizacji (niestandardowe serwery aktualizacji):

1. W sekcji Podstawowe wyłącz suwak obok opcji Wybierz automatycznie.

2. W polu Serwer aktualizacji wpisz adres URL serwera kopii dystrybucyjnej w jednej z następujących postaci:

```
http://<IP>:<port>
```

```
http://<hostname>:<port>
```

Do instalacji aktualizacji należy użyć następującego serwera:
`http://update.eset.com/eset_upd/businessmac/`

3. Wprowadź odpowiednią nazwę użytkownika i hasło.

Jeśli w sieci jest dostępnych więcej serwerów kopii dystrybucyjnych, powtórz powyższe kroki, aby skonfigurować Serwer pomocniczy.

Ochrona przed atakami typu „phishing”

Ochrona przed atakami typu „phishing” to kolejna warstwa zabezpieczeń, zapewniająca wzmocnienie ochrony przed stronami internetowymi służącymi do prób bezprawnego pozyskiwania haseł oraz innych informacji poufnych.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

Ochrona przed atakami typu „phishing” jest domyślnie włączona. Jeśli chcesz wyłączyć ochronę przed atakami typu „phishing”, przejdź do sekcji Strony internetowe i poczta e-mail > Ochrona przed atakami typu „phishing” i kliknij suwak obok pozycji Włącz ochronę przed atakami typu „phishing”.

Ochrona dostępu do stron internetowych

Ochrona dostępu do stron internetowych monitoruje komunikację między przeglądarkami internetowymi i zdalnymi serwerami w celu zapewnienia zgodności z regułami protokołu HTTP (Hypertext Transfer Protocol).

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Strony internetowe i poczta e-mail > Włącz ochronę dostępu do stron internetowych można skonfigurować następujące ustawienia:

Podstawowe

Włącz ochronę dostępu do stron internetowych — monitoruje komunikację HTTP między przeglądarkami internetowymi a zdalnymi serwerami.

Protokoły sieciowe

Włącz sprawdzanie protokołu HTTP — skanuje metody komunikacji HTTP używane przez dowolną aplikację.

Program skanuje ruch tylko na portach zdefiniowanych w funkcji Porty używane przez protokół HTTP. W razie potrzeby można dodać pozostałe porty komunikacyjne. Numery portów muszą być oddzielone przecinkami.

Zarządzanie adresami URL

Zarządzanie adresami URL umożliwia określanie adresów HTTP w celu zablokowania, zezwolenia lub wyłączenia ze sprawdzania. Strony internetowe znajdujące się na liście zablokowanych adresów będą niedostępne. Dostęp do stron internetowych na liście adresów Znalezione szkodliwe oprogramowanie jest ignorowane będzie uzyskiwane bez skanowania pod kątem szkodliwego kodu.

Aby umożliwić dostęp wyłącznie do adresów URL wymienionych na liście Dozwolone adresy URL, należy aktywować suwak obok opcji Ogranicz adresy URL.

Aby aktywować listę, włącz suwak obok pozycji Lista aktywna dla określonej nazwy listy. Aby otrzymywać powiadomienie po wprowadzeniu adresu z określonej listy, włącz suwak obok opcji Powiadom o zastosowaniu.

Podczas tworzenia list adresów można używać symboli specjalnych: * (gwiazdka) oraz ? (znak zapytania).

Gwiazdka zastępuje dowolny ciąg znaków, a znak zapytania — dowolny symbol.

Szczególną ostrożność należy zachować podczas określania adresów wyłączonych, ponieważ lista powinna zawierać wyłącznie zaufane i bezpieczne adresy. Należy również zapewnić prawidłowe stosowanie na liście symboli * i ?.

Parametry technologii ThreatSense

Parametry ThreatSense umożliwiają określenie opcji konfiguracji ochrony dostępu do stron internetowych, takich jak obiekty do skanowania, użyte metody wykrywania itp. Zobacz parametry ThreatSense, aby uzyskać szczegółowe informacje.

Ochrona programów poczty e-mail

Ochrona programów poczty e-mail — zapewnia sprawdzanie komunikacji e-mail przychodzącej za pośrednictwem protokołów POP3 oraz IMAP.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Strony internetowe i poczta e-mail > Ochrona programów poczty e-mail można skonfigurować następujące ustawienia:

Podstawowe

Integracja ESET Endpoint Antivirus for macOS z klientem poczty e-mail zwiększa poziom aktywnej ochrony przed złośliwym kodem w wiadomościach e-mail. Firma ESET zaleca pozostawienie aktywnej opcji Włącz ochronę poczty e-mail przez wtyczki klienckie.

Protokoły poczty e-mail

Protokoły IMAP i POP3 to najbardziej rozpowszechnione protokoły używane do obsługi komunikacji przychodzącej w programach poczty e-mail. IMAP (Internet Message Access Protocol) to kolejny protokół internetowy do odbierania poczty e-mail. Protokół IMAP ma pod pewnymi względami przewagę nad protokołem POP3. Na przykład wiele klientów może być podłączonych równocześnie do tej samej skrzynki pocztowej przy zachowaniu informacji o stanie wiadomości (czy została ona przeczytana, usunięta albo czy udzielono już na nią odpowiedzi).

Moduł ochrony udostępniający tę opcję jest automatycznie inicjowany po uruchomieniu komputera i jest aktywny w pamięci.

ESET Endpoint Antivirus for macOS zapewnia ochronę tych protokołów niezależnie od używanego klienta poczty e-mail i bez konieczności ponownej konfiguracji klienta poczty e-mail. Program skanuje ruch tylko na portach zdefiniowanych w portach używanych przez protokół IMAP/POP3. W razie potrzeby można dodać pozostałe porty komunikacyjne. Numery portów muszą być oddzielone przecinkami.

Parametry technologii ThreatSense

Parametry ThreatSense umożliwiają określenie opcji konfiguracji ochrony programu poczty e-mail, takich jak obiekty do skanowania, użyte metody wykrywania itp. Zobacz parametry ThreatSense, aby uzyskać szczegółowe informacje.

Alerty i powiadomienia

Po sprawdzeniu wiadomości e-mail może do niej zostać dołączone powiadomienie o wynikach skanowania. Do wyboru są następujące opcje: Oznacz otrzymaną i przeczytaną wiadomość e-mail oraz Oznacz wysyłaną wiadomość e-mail. Należy pamiętać, że w rzadkich przypadkach takie powiadomienia mogą być pomijane w przypadku kłopotliwych wiadomości w formacie HTML lub wiadomości fałszowanych przez szkodliwe oprogramowanie. Powiadomienia mogą być dodawane do odebranych i przeczytanych wiadomości. Dostępne są następujące opcje:

- Nigdy — do wiadomości nie będą dołączane powiadomienia.
- W przypadku wykrycia — tylko wiadomości zawierające szkodliwe oprogramowanie zostaną oznaczone jako sprawdzone (ustawienie domyślne).
- Do wszystkich wiadomości e-mail po zeskanowaniu — program będzie dołączać powiadomienia do wszystkich przeskanowanych wiadomości e-mail.

Aktualizuj temat otrzymanych i przeczytanych wiadomości e-mail — tę opcję należy wyłączyć, jeśli funkcja ochrony poczty e-mail ma nie umieszczać w temacie zainfekowanej wiadomości ostrzeżenia o wirusie. Ta opcja umożliwia później proste odfiltrowanie zainfekowanych wiadomości na podstawie analizy ich tematów (o ile program pocztowy udostępnia taką funkcję). Zwiększa ona też wiarygodność wiadomości dla odbiorcy, a w przypadku wykrycia zagrożenia udostępnia cenne informacje na temat poziomu zagrożenia, jakie stanowi dana wiadomość lub jej nadawca.

Komunikat dołączany do tematu wykrytej wiadomości e-mail — edytowanie tego szablonu pozwala zmodyfikować format przedrostka tematu zainfekowanej wiadomości e-mail. Korzystając z tej funkcji, można zastąpić temat wiadomości „Witaj” następującym formatem: „[wykryto %VIRUSNAME%] Witaj”. Zmienna %VIRUSNAME% zawiera nazwę wykrytego obiektu.

Narzędzia

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Narzędzia można skonfigurować następujące ustawienia:

Harmonogram

Harmonogram służy do zarządzania zaplanowanymi zadaniami skanowania na żądanie i uruchamiania ich ze wstępnie zdefiniowanymi konfiguracjami.

Kliknij przycisk Edytuj obok pozycji Zadania, aby wyświetlić listę wszystkich zaplanowanych zadań i właściwości konfiguracji.

Aby zmodyfikować konfigurację istniejącego zaplanowanego zadania, kliknij zadanie do modyfikacji i wybierz pozycję Edytuj. Aby usunąć zadanie, zaznacz zadanie i kliknij przycisk Usuń.

Aby dodać nowe zadanie:

1. Kliknij przycisk Dodaj u dołu listy.

2. Wprowadź Nazwę zadania i ustaw Czas wykonania zadania.

3. Wybierz dni, w których zadanie będzie uruchamiane wielokrotnie. Kliknij przycisk Dalej.

4. Wybierz opcję Profil skanowania, który ma być używany w ramach planowanego skanowania. Aby wyświetlić i edytować profile skanowania, zobacz Skanowanie w poszukiwaniu szkodliwego oprogramowania.

5. Zdefiniuj Skanowane obiekty, wybierz, czy wykryte elementy zostaną wyleczone i czy planowane skanowanie ma skanować również wyłączenia ustawione w konfiguracji profilu skanowania.

6. Kliknij przycisk Zakończ > Zapisz.

Serwer proxy

W dużych sieciach lokalnych komputery mogą komunikować się z Internetem za pośrednictwem serwera proxy. Korzystając z tych opcji konfiguracji można zdefiniować następujące ustawienia. W przeciwnym razie program nie będzie mógł być automatycznie aktualizowany.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Narzędzia > Serwer proxy można określić ustawienia serwera proxy. Zdefiniowane tutaj parametry będą używane przez wszystkie moduły, które wymagają połączenia z Internetem.

Aby skonfigurować serwer proxy:

1. Włącz opcję Użyj serwera proxy i wprowadź adres serwera proxy w polu Serwer proxy oraz numer Portu serwera proxy.

2. Jeśli komunikacja z serwerem proxy wymaga uwierzytelnienia, włącz opcję Serwer proxy wymaga uwierzytelniania i wprowadź prawidłową nazwę użytkownika i hasło w odpowiednich polach.

3. Włącz opcję Użyj bezpośredniego połączenia, jeśli serwer proxy nie jest dostępny, aby pominąć serwer proxy i komunikować się bezpośrednio z serwerami ESET, jeśli serwer proxy jest nieosiągalny.

Pliki dziennika

Zmodyfikuj konfigurację ESET Endpoint Antivirus for macOS rejestrowania. Pliki dziennika można przeglądać za pomocą programu ESET PROTECT On-Prem.

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W menu Narzędzia > Pliki dziennika można skonfigurować następujące ustawienia:

Minimalna szczegółowość zapisów w dzienniku

Szczegółowość rejestrowania określa poziom szczegółów zawartych w plikach dziennika.

• Ostrzeżenia krytyczne — zawiera tylko błędy krytyczne (na przykład nie można uruchomić ochrony antywirusowej).

• Błędy — rejestrowanie błędów typu „Błąd podczas pobierania pliku” zostanie zarezerwowane w dodatku do ostrzeżeń krytycznych.

• Ostrzeżenia — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych razem z błędami.

• Rekordy informacyjne — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.

• Rekordy diagnostyczne — zawierają informacje potrzebne do ulepszania konfiguracji programu, a także wszystkich rekordów wyższych kategorii.

Automatycznie usuwaj rekordy starsze niż (dni) — Wpisy dziennika starsze niż liczba dni podana w polu będą usuwane automatycznie.

Automatycznie optymalizuj pliki dzienników — włączenie tej opcji powoduje automatyczną defragmentację plików dziennika po przekroczeniu stopnia fragmentacji określonego w polu Jeśli liczba nieużywanych rekordów przekracza (%). Wszystkie puste wpisy dzienników są usuwane w celu zwiększenia wydajności i szybkości przetwarzania dzienników. Poprawę można zaobserwować zwłaszcza w przypadku dzienników zawierających dużą liczbę wpisów.

Funkcja pliku syslog

Funkcja pliku syslog to parametr rejestrowania pliku syslog używana do grupowania podobnych komunikatów dziennika. Na przykład dzienniki demona (które zbierają dzienniki za pośrednictwem demona funkcji pliku syslog) mogą być zapisywane w pliku *~/log/daemon.log*, jeśli skonfigurowano tę funkcję. Wraz z niedawnym przejściem na systemd i jego dziennik, funkcja pliku syslog jest mniej ważna, ale nadal może być używana do filtrowania dzienników.

Interfejs użytkownika

Aby skonfigurować ESET Endpoint Antivirus for macOS zdalnie:

1. W programie ESET PROTECT On-Prem kliknij pozycję Polityki > Nowa zasada i wpisz nazwę polityki.

> Aby dostosować ustawienia w ramach istniejącej polityki dla ESET Endpoint for macOS (V7+), kliknij politykę, którą chcesz zmienić, na liście, a następnie kliknij przycisk Edytuj > Ustawienia.

2. Kliknij Ustawienia i wybierz ESET Endpoint for macOS (V7+) z menu rozwijanego.

3. Dostosuj żądane ustawienia.

4. Kliknij przycisk Kontynuuj > Przypisz i wybierz odpowiednią grupę komputerów.

5. Kliknij przycisk OK > Zakończ.

> Aby skonfigurować ESET Endpoint Antivirus for macOS lokalnie, zapoznaj się z preferencjami aplikacji.

W Interfejsie użytkownika można skonfigurować następujące ustawienia:

Elementy interfejsu użytkownika

Zezwól użytkownikowi na otwieranie graficznego interfejsu użytkownika — Wyłącz to ustawienie, aby uniemożliwić użytkownikom dostęp do graficznego interfejsu użytkownika. Ten tryb może być przydatny w środowiskach zarządzanych lub w sytuacjach, gdy trzeba oszczędzać zasoby systemowe.

Pokazuj ikonę w elementach dodatkowych paska menu — Wyłączenie tego ustawienia powoduje usunięcie ikony ESET Endpoint Antivirus for macOS z elementów dodatkowych paska menu w ramach menu systemu macOS (u góry ekranu).

Powiadomienia

Wyświetlaj powiadomienia na pulpicie — powiadomienia na pulpicie (takie jak komunikaty o pomyślnej aktualizacji, ukończenie zadań skanowania antywirusowego lub znalezienie nowych zagrożeń) są reprezentowane przez małe wyskakujące okienko obok paska menu systemu macOS. Jeśli ta opcja jest włączona, ESET Endpoint Antivirus for macOS może informować o wystąpieniu nowego zdarzenia.

Stany

Stany aplikacji — kliknij przycisk Edytuj, aby skonfigurować, które stany aplikacji będą wyświetlać powiadomienie w oknie Stan ochrony i które stany aplikacji będą raportowane do ESET PROTECT On-Prem konsoli internetowej.

Wprowadzenie do ESET PROTECT CLOUD

ESET PROTECT CLOUD umożliwia zarządzanie produktami firmy ESET na stacjach roboczych i serwerach w środowisku sieciowym z jednej lokalizacji centralnej bez konieczności korzystania z serwera fizycznego lub wirtualnego na potrzeby konsoli ESET PROTECT On-Prem lub ESET Security Management Center. Przy użyciu konsoli webowej ESET PROTECT CLOUD można wdrażać rozwiązania ESET, zarządzać zadaniami, egzekwować polityki bezpieczeństwa, monitorować stan systemu, a także szybko reagować na problemy i zagrożenia pojawiające się na komputerach zdalnych.

- Więcej informacji na ten temat można znaleźć w podręczniku użytkownika online programu ESET PROTECT CLOUD.

Wprowadzenie do ESET PROTECT On-Prem

ESET PROTECT On-Prem umożliwia zarządzanie produktami ESET na stacjach roboczych, serwerach oraz urządzeniach mobilnych w środowisku sieciowym z jednej lokalizacji centralnej.

Za pomocą konsoli internetowej ESET PROTECT On-Prem można wdrażać rozwiązania ESET, zarządzać zadaniami, wymuszać polityki zabezpieczeń, monitorować status systemu oraz błyskawicznie reagować na problemy lub wykrycia na komputerach zdalnych. Zobacz też Omówienie architektury i infrastruktury rozwiązania ESET PROTECT On-Prem, Informacje wstępne dotyczące konsoli internetowej ESET PROTECT On-Prem oraz Obsługiwane środowiska przydzielania komputerów.

ESET PROTECT On-Prem obejmuje następujące składniki:

- Serwer ESET PROTECT On-Prem — serwer ESET PROTECT On-Prem można instalować na serwerach z systemem Windows oraz Linux. Jest on również dostępny jako urządzenie wirtualne. Obsługuje komunikację z agentami i gromadzi dane aplikacji oraz przechowuje je w bazie danych.

- Konsola internetowa ESET PROTECT On-Prem — konsola internetowa ESET PROTECT On-Prem jest podstawowym interfejsem umożliwiającym zarządzanie komputerami klienckimi w danym środowisku. Umożliwia wyświetlanie podsumowania stanu klientów w danej sieci i zdalne wdrażanie rozwiązań ESET na niezarządzanych komputerach. Po zainstalowaniu serwera ESET PROTECT On-Prem dostęp do konsoli internetowej można uzyskać przy użyciu przeglądarki internetowej. Jeśli serwer sieciowy będzie dostępny przez Internet, można używać programu ESET PROTECT On-Prem z dowolnego miejsca, za pomocą dowolnego urządzenia z połączeniem internetowym.

- Agent ESET Management — agent ESET Management usprawnia komunikację między serwerem ESET PROTECT On-Prem i komputerami klienckimi. Agent musi być zainstalowany na komputerze klienckim, aby nawiązać komunikację pomiędzy tym komputerem a serwerem ESET PROTECT On-Prem. Ponieważ agent ESET Management znajduje się na komputerze klienckim i umożliwia przechowywanie wielu scenariuszy zabezpieczeń, korzystanie z agenta znacznie zwiększa szybkość reagowania na nowe wykrycia. Przy użyciu konsoli internetowej ESET PROTECT On-Prem można wdrożyć agenta ESET Management na komputerach niezarządzanych identyfikowanych przez usługę Active Directory lub przy użyciu narzędzia ESET RD Sensor. W razie konieczności można ręcznie zainstalować agenta ESET Management na komputerach klienckich.

- Narzędzie Rogue Detection Sensor — narzędzie ESET PROTECT On-Prem Rogue Detection (RD) Sensor służy do wykrywania niezarządzanych komputerów w danej sieci i umożliwia wysyłanie ich danych do serwera ESET PROTECT On-Prem. Dzięki temu można z łatwością dodawać nowe komputery klienckie do sieci objętej zabezpieczeniami. Wykryte komputery są zapamiętywane w narzędziu RD Sensor i te same informacje nie są wysyłane ponownie.

- ESET Bridge — usługa, z której można korzystać w połączeniu z programem ESET PROTECT On-Prem w celu:

  - Dystrybuowania aktualizacji wśród komputerów klienckich oraz przesyłania pakietów instalacyjnych do agenta ESET Management.

  - Przesyłania dalej komunikacji z agentów ESET Management do serwera ESET PROTECT On-Prem.

- Mobile Device Connector — komponent umożliwiający zarządzanie urządzeniami mobilnymi (z systemem Android i iOS) przy użyciu programu ESET PROTECT On-Prem oraz administrowanie programem ESET Endpoint Security dla systemu Android.

- Urządzenie wirtualne ESET PROTECT On-Prem — urządzenie wirtualne ESET PROTECT On-Prem jest przeznaczone dla użytkowników, którzy chcą uruchamiać ESET PROTECT On-Prem w środowisku zwirtualizowanym.

- Mirror Tool — narzędzie Mirror Tool jest potrzebne w przypadku aktualizacji bazy danych wirusów offline. Jeśli komputery klienckie nie mają połączenia z Internetem, przy użyciu narzędzia Mirror Tool można pobrać pliki aktualizacji z serwerów aktualizacji firmy ESET, aby przechowywać je lokalnie.

- ESET Remote Deployment Tool — to narzędzie umożliwia wdrażanie pakietów kompleksowych utworzonych w konsoli internetowej ESET PROTECT On-Prem. Stanowi ono wygodny sposób dystrybucji agenta ESET Management z produktem firmy ESET na komputerach w sieci.

- ESET Business Account — nowy portal licencyjny produktów biznesowych ESET pozwala na zarządzanie licencjami. Więcej informacji na temat korzystania z ESET Business Account można znaleźć w Podręczniku użytkownika ESET Business Account.

- ESET Enterprise Inspector — wszechstronny system detekcji i reakcji dla punktów końcowych, którego funkcje obejmują: wykrywanie incydentów, zarządzanie i odpowiedź na incydenty, zbieranie danych, wskaźniki wykrycia naruszeń, wykrywanie anomalii, wykrywanie zachowań i naruszenia polityk.

Za pomocą konsoli internetowej ESET PROTECT On-Prem można wdrażać rozwiązania ESET, zarządzać zadaniami, wymuszać polityki zabezpieczeń, monitorować status systemu oraz błyskawicznie reagować na problemy lub zagrożenia na komputerach zdalnych.

Więcej informacji zawiera podręcznik użytkownika online programu ESET PROTECT On-Prem.

Wyłącz powiadomienia przez MDM

Powiadomienia ESET Endpoint Antivirus for macOS są wyświetlane w konsoli zarządzania ESET. Nie musisz otrzymywać powiadomień ESET Endpoint Antivirus for macOS, jeśli zarządzasz produktami ESET w konsoli zarządzania ESET.

Możesz wyłączyć powiadomienie za pomocą MDM.

Aby utworzyć profil konfiguracji, pobierz plik pakietu danych .plist.

Większość modułów MDM umożliwia dołączenie pliku pakietu danych .plist lub kopiowanie/wklejanie zawartości pliku w profilu konfiguracji.

Użytkownicy Jamf

1. W oknie głównym Jamf kliknij **Komputery** > **Profile konfiguracji**.

2. W sekcji **Ogólne** podaj:

Ustawienie	Wartość
Nazwa	Na przykład powiadomienie ESET
Poziom	Poziom komputera
Metoda dystrybucji	Zwykle, Zainstaluj automatycznie

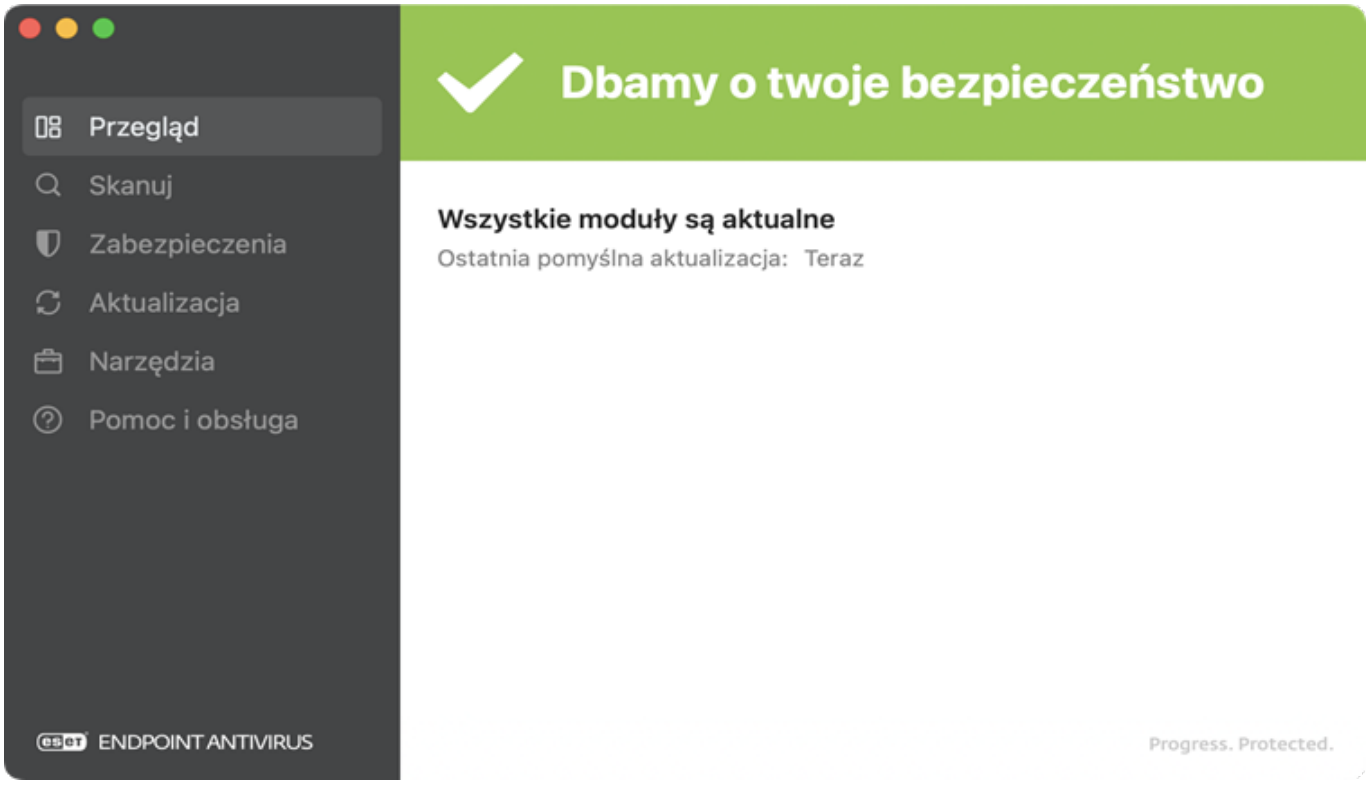
3. W sekcji **Powiadomienie** kliknij **Dodaj+** i wypełnij:

Ustawienie	Wartość
Nazwa aplikacji	ESET Endpoint Antivirus for macOS
Identyfikator pakietu	com.eset.eea.agent
Alerty krytyczne	Wyłącz
Powiadomienia	Wyłącz

Praca z programem ESET Endpoint Antivirus for macOS

Aby otworzyć główne okno programu, kliknij ikonę programu ESET Endpoint Antivirus for macOS wyświetlaną na pasku menu macOS (na górze ekranu), a następnie kliknij PokażESET Endpoint Antivirus for macOS.

Główne okno programu ESET Endpoint Antivirus for macOS jest podzielone na dwie części. W okienku z prawej strony są wyświetlane informacje dotyczące opcji wybranej w menu głównym z lewej strony.



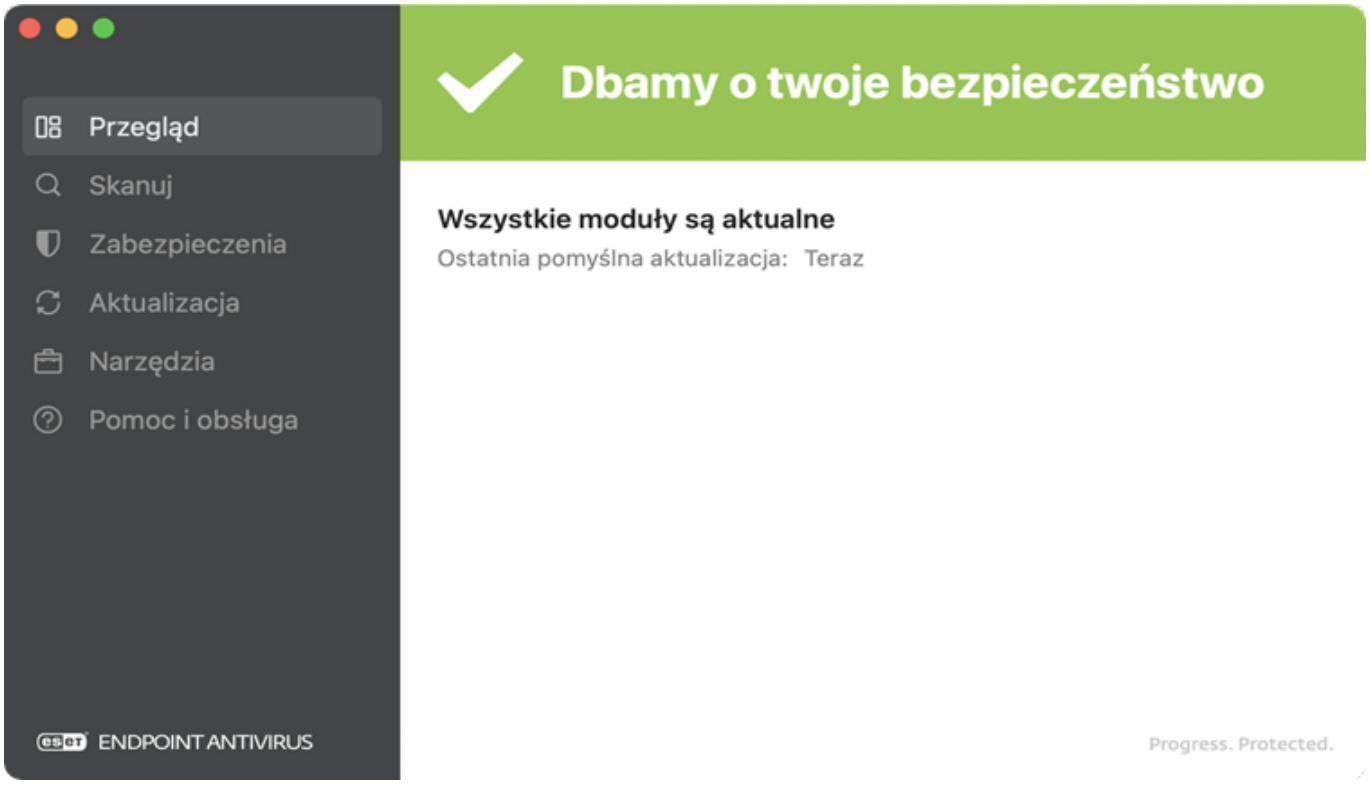
W menu głównym dostępne są następujące opcje:

- Przegląd
- Skanuj
- Zabezpieczenia
- Aktualizacja
- Narzędzia
- Pomoc i obsługa

Aby zmodyfikować ustawienia zaawansowane programu ESET Endpoint Antivirus for macOS, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia). Jeśli program ESET Endpoint Antivirus for macOS jest zarządzany, możesz skonfigurować ustawienia ESET Endpoint Antivirus for macOS za pomocą ESET PROTECT On-Prem lub ESET PROTECT CLOUD.

Przegląd

Kliknij przycisk Przegląd w głównym oknie programu, aby wyświetlić informacje o bieżącym poziomie ochrony komputera.



W oknie przeglądu jest wyświetlany też bieżący stan aktualizacji, w tym data i godzina ostatniej pomyślnej aktualizacji.

ESET Endpoint Antivirus for macOS może wyświetlać jeden z następujących stanów ochrony:

- Stan Dbamy o twoje bezpieczeństwo z zielonym nagłówkiem — zapewniona maksymalna ochrona.
- Stan Wymagana uwaga z pomarańczowym nagłówkiem — ESET Endpoint Antivirus for macOS wymaga uwagi z powodu problemu niekrytycznego.
- Stan Alert zabezpieczeń z czerwonym nagłówkiem — występuje krytyczny problem i nie jest zapewniona maksymalna ochrona.

Jeśli stan ochrony to Wymagana uwaga lub Alert zabezpieczeń, w oknie stanu ochrony są wyświetlane powiadomienia z dodatkowymi informacjami i sugerowanymi rozwiązaniami.

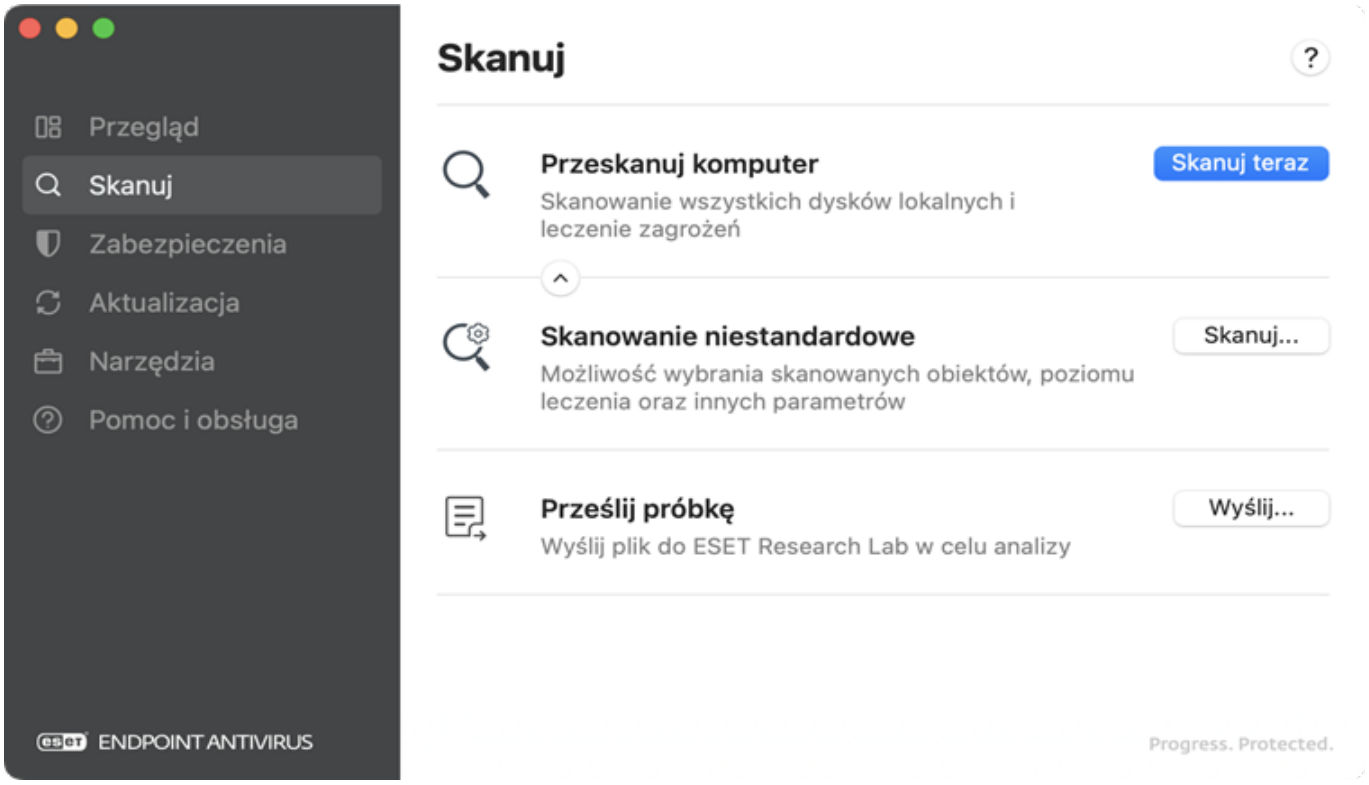
Jeśli nie możesz rozwiązać problemu przy użyciu proponowanych rozwiązań, to możesz przeszukać bazę wiedzy ESET. Jeśli nadal będzie potrzebna pomoc, możesz przesłać zgłoszenie do działu pomocy technicznej ESET.

Skanuj

Kliknij **Skanuj** w głównym oknie programu, aby wykonać skanowanie plików i folderów na komputerze.

Skaner na żądanie jest ważną częścią rozwiązania antywirusowego i służy do skanowania plików i folderów na komputerze. Z punktu widzenia bezpieczeństwa ważne jest, aby skanowanie komputera było wykonywane regularnie w ramach rutynowych środków bezpieczeństwa, a nie tylko w przypadku podejrzenia infekcji.

Zalecamy regularne i dokładne skanowanie systemu w celu wykrycia wirusów, które nie są przechwytywane przez ochronę systemu plików w czasie rzeczywistym. Może się tak zdarzyć, jeśli zagrożenie zostanie wprowadzone, gdy ochrona systemu plików w czasie rzeczywistym jest wyłączona, silnik detekcji jest nieaktualny lub jeśli zagrożenie nie zostało wykryte podczas zapisywania go na dysku.



Skanowanie komputera

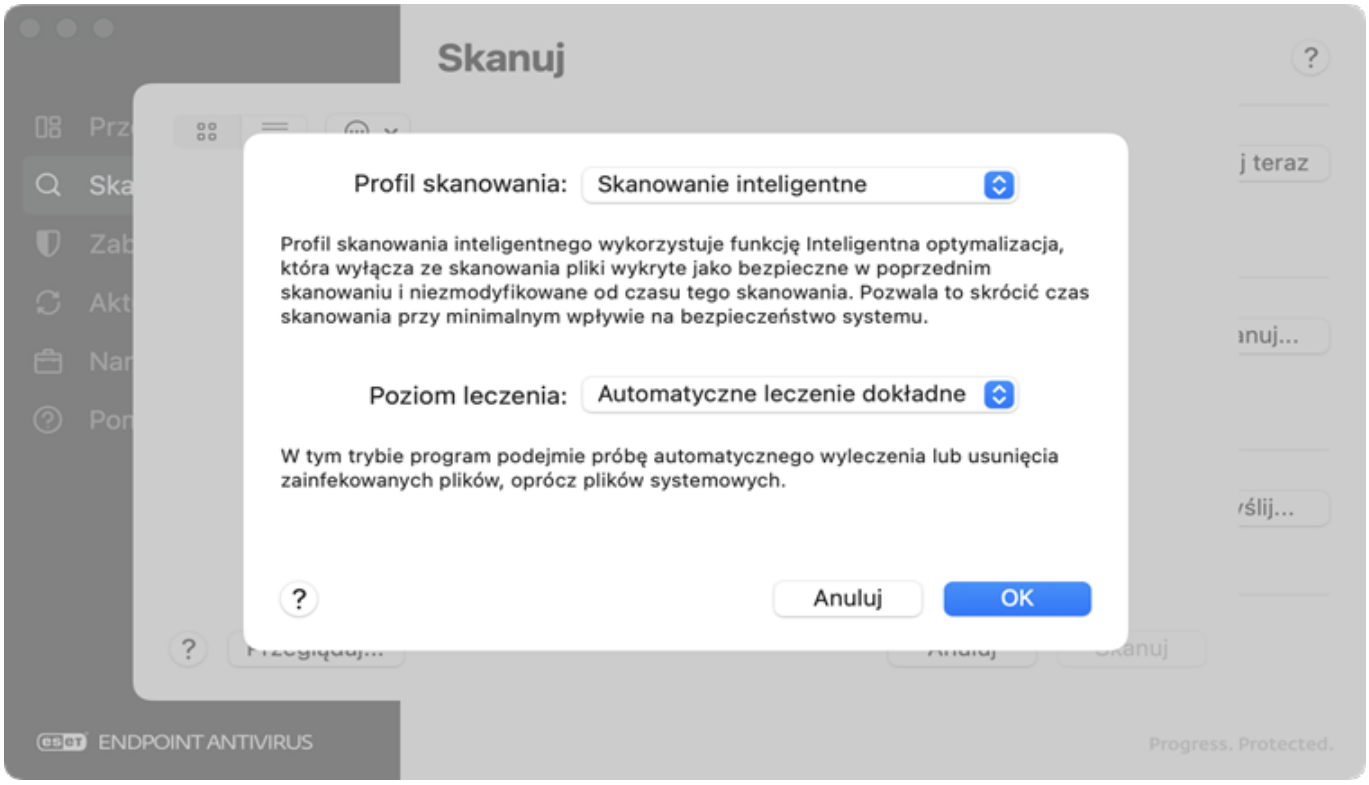
Kliknij Skanuj teraz w celu szybkiego uruchomienia skanowania komputera i wyleczenie zainfekowanych plików bez konieczności podejmowania dodatkowych działań przez użytkownika. Skanowanie komputera jest łatwe w obsłudze i eliminuje konieczność szczegółowej konfiguracji skanowania. W ramach skanowania sprawdzane są wszystkie pliki na dyskach lokalnych, a wykryte infekcje są automatycznie leczone lub usuwane.

Kliknij ikonę strzałki , aby wyświetlić opcje **Skanowanie niestandardowe** i **Prześlij próbkę**.

Skanowanie niestandardowe

Kliknij przycisk Skanuj, aby otworzyć okno skanowania niestandardowego.

Skanowanie niestandardowe umożliwia określenie parametrów skanowania, takich jak skanowane obiekty docelowe, profil skanowania, poziom czyszczenia i wykluczenia.



Aby dodać niestandardowe obiekty docelowe skanowania:

- Przeciągnij i upuść plik lub folder ręcznie, klikając plik lub folder, przesuwając wskaźnik myszy do zaznaczanego obszaru, przytrzymując wciśnięty przycisk myszy, a następnie zwalniając go.
- Kliknij przycisk Przeglądaj i wybierz pliki lub foldery, które chcesz przeskanować.

Kliknij ikonę menu ⋯, aby wyświetlić zaawansowane opcje skanowania:

Wybierz profil skanowania — wybierz Profil skanowania i Poziom leczenia dla skanowania niestandardowego.

> Możesz edytować profile skanowania za pomocą ESET PROTECT On-Prem, ESET PROTECT CLOUD lub w preferencjach aplikacji.

Wykluczenia instalacyjne — dodaj pliki lub foldery, które zostaną wykluczone ze skanowania.

Aby uruchomić skanowanie na żądanie przez Terminal przy użyciu narzędzia **odscan**, zapoznaj się z tematem Skanowanie na żądanie przez Terminal.

Prześlij próbkę

Ta opcja umożliwia wybranie podejrzanego pliku odnalezionego na komputerze lub w witrynie online i przesłanie go do laboratorium badawczego ESET do analizy.

Kliknij przycisk **Wyślij**, aby określić pliki, które chcesz przesłać do analizy. Najpierw należy wybrać powód przesłania, a następnie wybrać plik. Ręcznie przeciągnij lub upuść plik lub folder, klikając plik lub folder, przesuwając wskaźnik myszy do zaznaczanego obszaru, przytrzymując wciśnięty przycisk myszy, a następnie zwalniając go. Istnieje możliwość dołączenia adresu e-mail, aby umożliwić nam kontakt, gdy potrzebne będą dodatkowe informacje. Nie musisz dołączać swojego adresu e-mail, jeśli włączysz opcję **Prześlij anonimowo**.

Przesłana próbka musi spełniać co najmniej jedno z następujących kryteriów:

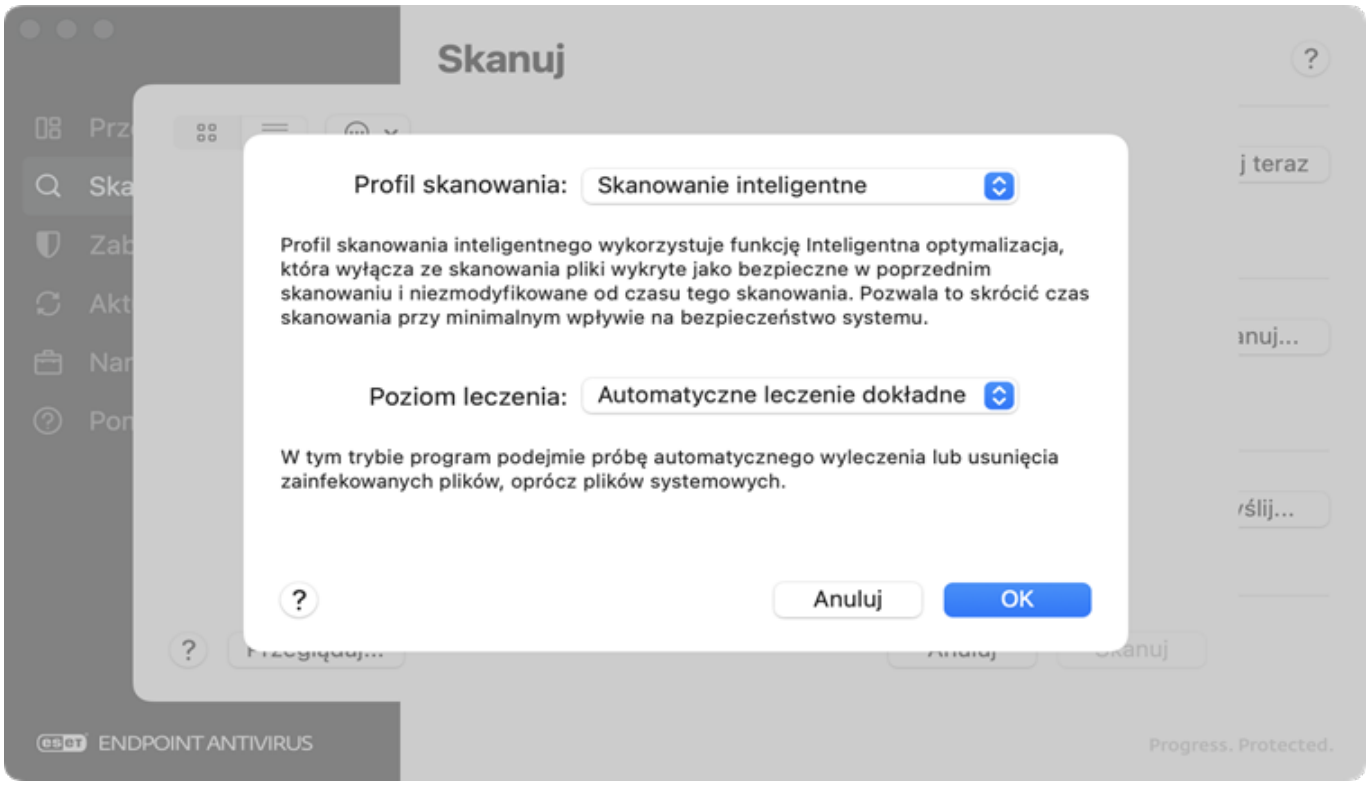
- Próbka nie została wykryta przez produkt ESET.
- Plik jest błędnie wykrywany jako zagrożenie.

Kliknięcie przycisku **Dalej** powoduje przejście do ostatniego kroku, w którym należy podać dodatkowe informacje o próbce, takie jak obserwowane oznaki lub objawy infekcji złośliwym oprogramowaniem i pochodzenie pliku. Podanie dodatkowych informacji pomoże naszym laboratoriom w identyfikacji i przetworzeniu próbek.

ESET nie akceptuje plików osobistych (które chcesz przeskanować pod kątem szkodliwego oprogramowania) jako próbek. Laboratorium badawcze ESET nie przeprowadza skanowania na żądanie dla użytkowników.

Skanowanie niestandardowe

Skanowanie niestandardowe umożliwia określenie parametrów skanowania, takich jak skanowane obiekty docelowe, profil skanowania, poziom czyszczenia i wykluczenia.



Aby dodać niestandardowe obiekty docelowe skanowania:

- Przeciągnij i upuść plik lub folder ręcznie, klikając plik lub folder, przesuwając wskaźnik myszy do zaznaczanego obszaru, przytrzymując wciśnięty przycisk myszy, a następnie zwalniając go.
- Kliknij przycisk Przeglądaj i wybierz pliki lub foldery, które chcesz przeskanować.

Kliknij ikonę menu ⋯, aby wyświetlić zaawansowane opcje skanowania:

Wybierz profil skanowania — wybierz Profil skanowania i Poziom leczenia dla skanowania niestandardowego.

Możesz edytować profile skanowania za pomocą ESET PROTECT On-Prem, ESET PROTECT CLOUD lub w preferencjach aplikacji.

Wykluczenia instalacyjne — dodaj pliki lub foldery, które zostaną wykluczone ze skanowania.

Prześlij próbkę

W głównym oknie aplikacji wybierz **Skanowanie** w lewym menu i kliknij ikonę strzałki , aby wyświetlić opcję **Prześlij próbkę**.

Ta opcja umożliwia wybranie podejrzanego pliku odnalezionego na komputerze lub w witrynie online i przesłanie go do laboratorium badawczego ESET do analizy.

Kliknij przycisk **Wyślij**, aby określić pliki, które chcesz przesłać do analizy. Najpierw wybierz powód przesłania, a następnie plik. Ręcznie przeciągnij i upuść plik lub folder, klikając plik lub folder, przesuwając wskaźnik myszy do zaznaczanego obszaru, przytrzymując wciśnięty przycisk myszy, a następnie zwalniając go. Istnieje możliwość dołączenia adresu e-mail, aby umożliwić nam kontakt, gdy potrzebne będą dodatkowe informacje. Nie musisz dołączać swojego adresu e-mail, jeśli włączysz opcję **Prześlij anonimowo**.

Przesłana próbka musi spełniać co najmniej jedno z następujących kryteriów:

- Próbka nie została wykryta przez produkt ESET.
- Plik jest błędnie wykrywany jako zagrożenie.

Kliknięcie przycisku **Dalej** powoduje przejście do ostatniego kroku, w którym należy podać dodatkowe informacje o próbce, takie jak obserwowane oznaki lub objawy infekcji złośliwym oprogramowaniem i pochodzenie pliku. Podanie dodatkowych informacji pomoże naszym laboratoriom w identyfikacji i przetworzeniu próbek.

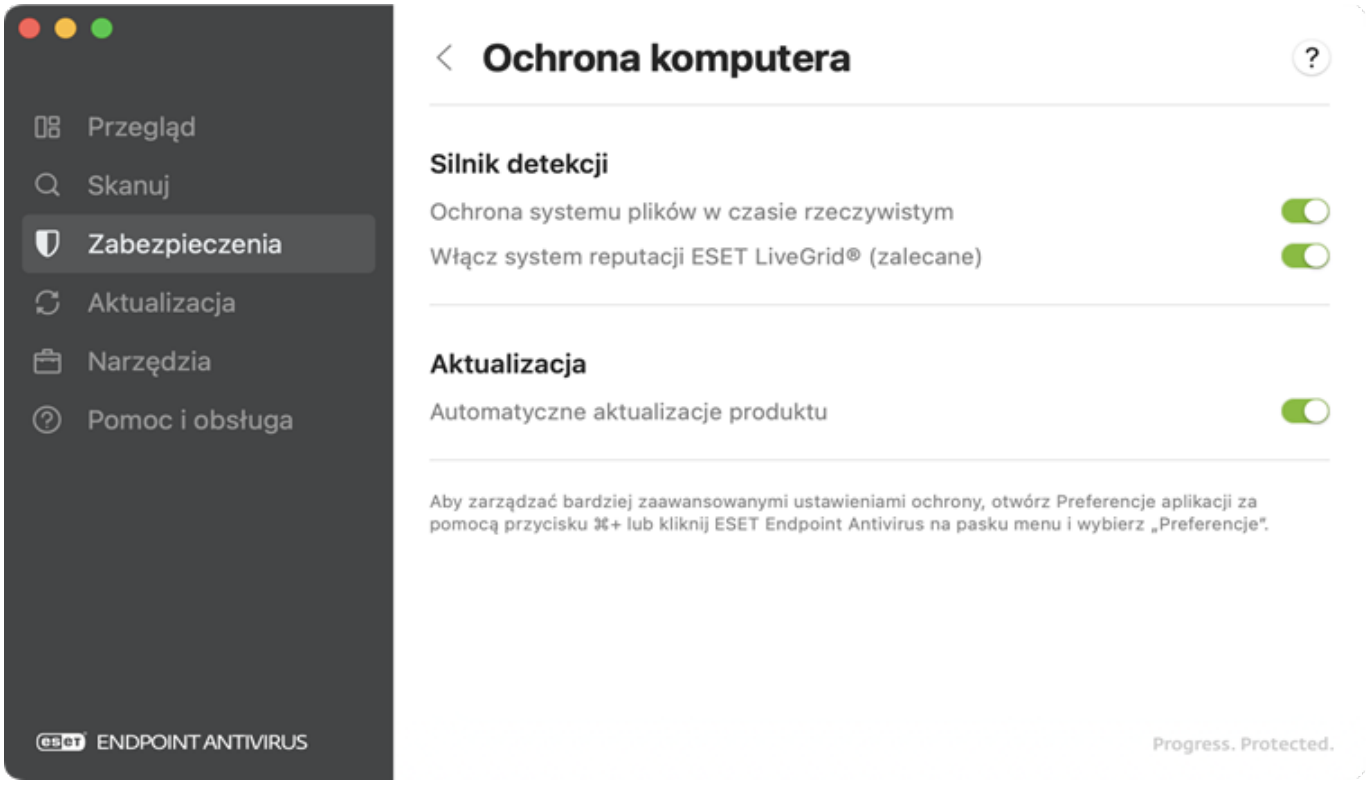
ESET nie akceptuje plików osobistych (które chcesz przeskanować pod kątem szkodliwego oprogramowania) jako próbek. Laboratorium badawcze ESET nie przeprowadza skanowania na żądanie dla użytkowników.

Zabezpieczenia

Możesz dostosować poziom ochrony komputera, stron internetowych i poczty e-mail, używając opcji **Zabezpieczenia** w głównym oknie aplikacji. Zarówno sekcja Ochrona komputera, jak i Ochrona dostępu do stron internetowych i poczty e-mail zawierają moduły ochrony, które można włączyć lub wyłączyć. Zdecydowanie zalecamy włączenie wszystkich modułów, aby w pełni wykorzystać ESET Endpoint Antivirus for macOS i zapewnić bezpieczeństwo komputera.

Komputer

Konfigurację ochrony komputera można znaleźć w sekcji **Zabezpieczenia** > **Komputer**. To okno pokazuje stan modułów **ochrony systemu plików w czasie rzeczywistym** i systemu reputacji **ESET LiveGrid©**. Zalecamy pozostawienie obu modułów włączonych, wyłączenie jednego z nich może zmniejszyć ochronę komputera.



Możesz kliknąć przełącznik, aby włączyć lub wyłączyć funkcję **automatycznej aktualizacji** w sekcji **Aktualizacja**. Gdy funkcja Automatyczna aktualizacja jest włączona, ESET Endpoint Antivirus for macOS wyszukuje najnowsze aktualizacje produktów i pobiera je automatycznie.

Strony internetowe i poczta e-mail

Aby z menu głównego przejść do ochrony stron internetowych i poczty e-mail, kliknij kolejno opcje **Zabezpieczenia** > **Strony internetowe i poczta e-mail**. Aby zarządzać bardziej zaawansowanymi ustawieniami poszczególnych modułów, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając opcję ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia). W ramach ochrony dostępu do stron internetowych i poczty e-mail dostępne są następujące moduły ochrony:

- **Web** — monitoruje komunikację HTTP między przeglądarkami internetowymi a zdalnymi serwerami.
- **Anti-Phishing** — blokuje potencjalne ataki typu „phishing" pochodzące z witryn internetowych lub domen.
- **E-mail** — zapewnia sprawdzanie komunikacji e-mail przychodzącej za pośrednictwem protokołów POP3 oraz IMAP.

Aktualizacja

Kliknij przycisk Aktualizacja w głównym oknie programu, aby wyświetlić bieżący stan aktualizacji, w tym datę i godzinę ostatniej pomyślnej aktualizacji, oraz ustalić, czy w danej chwili należy przeprowadzić aktualizację.

Regularne aktualizowanie programu ESET Endpoint Antivirus for macOS to najlepszy sposób na zapewnienie maksymalnego poziomu bezpieczeństwa komputera. Automatyczne aktualizacje zapewniają, że moduły programu i komponenty systemu są zawsze aktualne. Kliknij Sprawdź dostępność aktualizacji, aby uruchomić ręczną

aktualizację. Jeśli jest dostępna aktualizacja produktu, wyświetlane są informacje o bieżącej i dostępnej wersji wraz z rozmiarem aktualizacji i datą wydania. Aby kontynuować aktualizację produktu, należy zaakceptować **Umowę licencyjną użytkownika końcowego** i **Politykę prywatności**. Można wybrać opcję **Akceptuj i aktualizuj teraz** lub **Akceptuj i zaktualizuj przy ponownym uruchomieniu**. Aby zobaczyć więcej szczegółów na temat poszczególnych wersji produktu, kliknij odnośnik **Zobacz dziennik zmian**.

Ostatnia pomyślna aktualizacja — wyświetla datę ostatniej udanej aktualizacji. Jeśli nie jest wyświetlona niedawna data, moduły produktu mogą być nieaktualne.

Ostatnie sprawdzenie dostępności aktualizacji: — wyświetla datę ostatniego udanego sprawdzenia dostępności aktualizacji.

Aby zmodyfikować ustawienia zaawansowane programu ESET Endpoint Antivirus for macOS w zakresie **Aktualizacji**, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia). Jeśli program ESET Endpoint Antivirus for macOS jest zarządzany, możesz skonfigurować zaawansowane ustawienia aktualizacji zdalnie za pomocą ESET PROTECT On-Prem lub ESET PROTECT CLOUD.

Aby zaktualizować moduły wykrywania za pośrednictwem Terminala i używając narzędzia **upd**, zapoznaj się z tematem Aktualizuj moduły wykrywania za pośrednictwem Terminala.

Narzędzia

Menu **Narzędzia** zawiera moduły, które upraszczają administrowanie programem i udostępniają dodatkowe opcje dla użytkowników zaawansowanych. To menu zawiera następujące narzędzia:

- **Pliki dziennika**
- **Kwarantanna**

Pliki dziennika

Pliki dziennika zawierają informacje o wszystkich ważnych zdarzeniach, jakie miały miejsce, oraz przegląd wykrytych zagrożeń. Rejestrowanie jest niezbędne do analizy systemu, wykrywania zagrożeń i rozwiązywania problemów. Dziennik jest aktywnie tworzony w tle i nie wymaga żadnych działań ze strony użytkownika. Informacje są zapisywane zgodnie z bieżącymi ustawieniami szczegółowości dziennika. Za pomocą środowiska programu ESET Endpoint Antivirus for macOS można bezpośrednio wyświetlać wiadomości tekstowe oraz wyświetlać i archiwizować dzienniki.

Pliki dziennika są dostępne z poziomu okna głównego programu ESET Endpoint Antivirus for macOS po kliknięciu kolejno opcji **Narzędzia** > **Pliki dziennika**. Wybierz odpowiedni typ dziennika, korzystając z menu rozwijanego po prawej stronie u góry okna. Dostępne są następujące dzienniki:

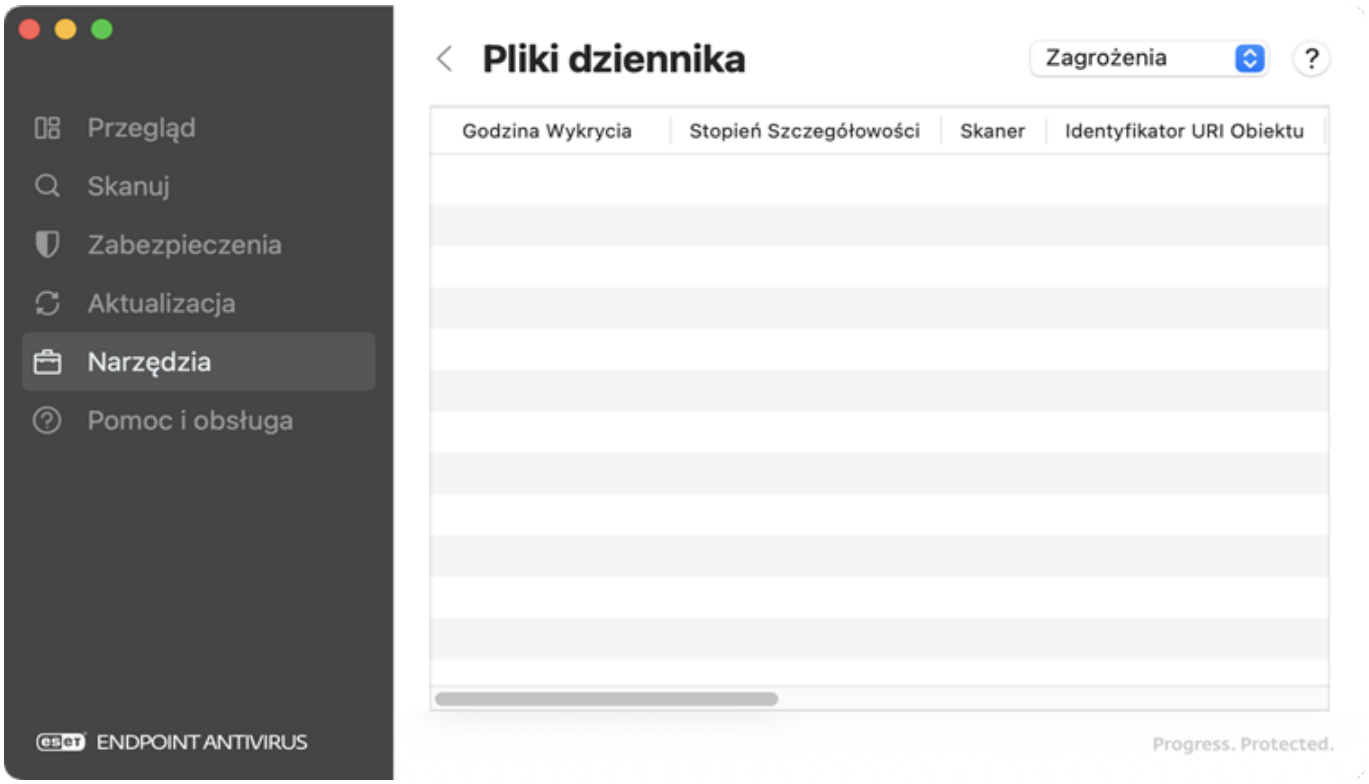
- **Wykrycia** — wyświetla wszystkie informacje o zdarzeniach związanych z wykrywaniem infekcji.
- **Skanowanie komputera** — wyświetla wyniki wszystkich ukończonych operacji skanowania. Dwukrotne kliknięcie dowolnego wpisu powoduje wyświetlenie szczegółowych informacji na temat danej operacji skanowania komputera na żądanie.
- **Zdarzenia** — pomaga administratorom systemu i użytkownikom w rozwiązywaniu problemów. Wszystkie

ważne czynności podejmowane przez program ESET Endpoint Antivirus for macOS są zapisywane w dziennikach zdarzeń.

- **Zablokowane pliki** — zawiera rekordy plików zablokowanych podczas skanowania na podstawie listy zablokowanych plików (zablokowanych skrótów) skonfigurowanej przez program ESET Inspect.

- **Filtrowane witryny internetowe** — wyświetla listę witryn zablokowanych przez funkcję ochrony dostępu do stron internetowych. W dziennikach odnotowane są: czas, adres URL, adres IP, nazwa użytkownika oraz aplikacja, która nawiązała połączenie z daną stroną internetową.

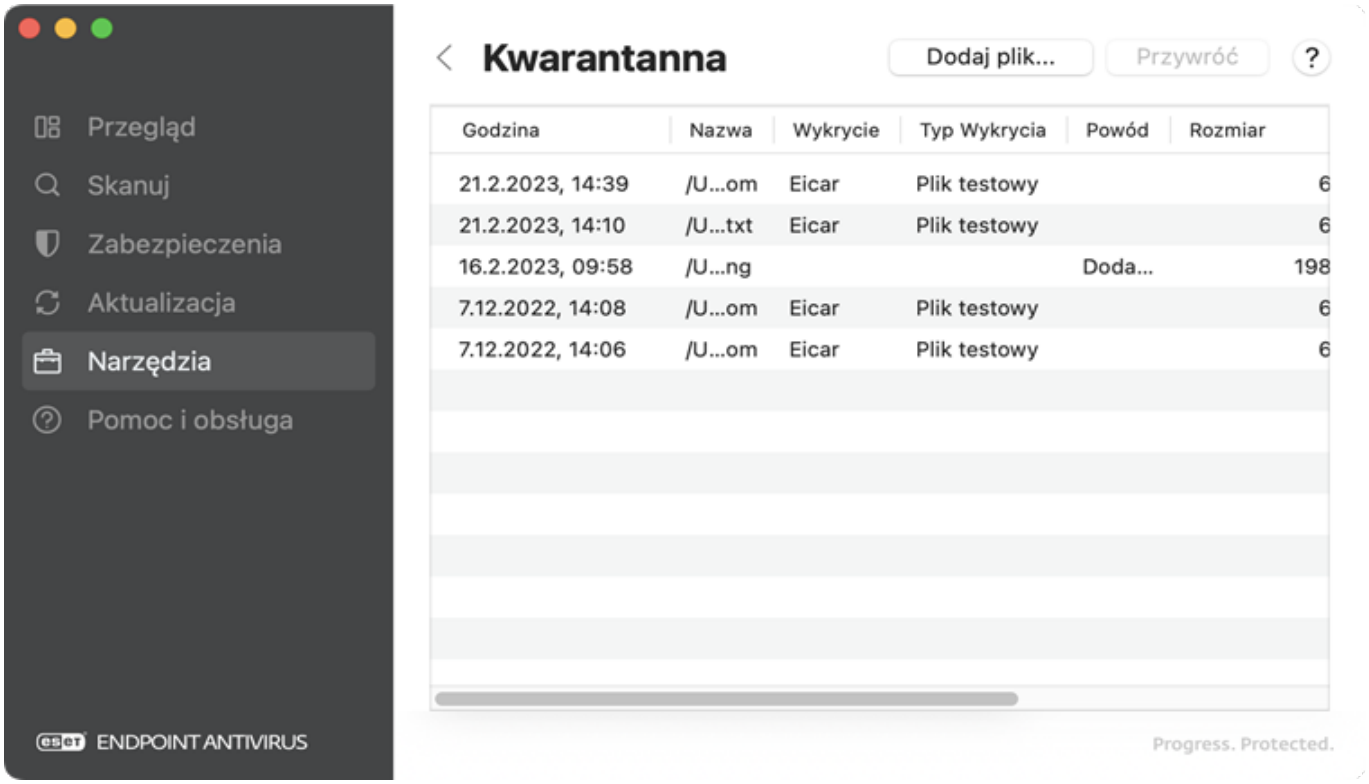
- **Wysłane pliki** — zawiera zapisy próbek wysłanych do analizy.



Kwarantanna

Kwarantanna umożliwia bezpieczne przechowywanie zainfekowanych plików. Pliki należy poddawać kwarantannie w przypadku, gdy nie można ich wyleczyć, gdy ich usunięcie nie jest bezpieczne lub zalecane, lub gdy są one nieprawidłowo wykrywane przez program ESET Endpoint Antivirus for macOS.

Możesz przeglądać pliki przechowywane w folderze kwarantanny w tabeli zawierającej datę i godzinę poddania kwarantannie, ścieżkę do pierwotnej lokalizacji zainfekowanego pliku, rozmiar pliku w bajtach, powód (np. obiekt dodany przez użytkownika) oraz liczbę zagrożeń (np. jeśli plik jest archiwum zawierającym wiele infekcji). Folder kwarantanny z plikami poddanymi kwarantannie (*/Library/Application Support/Eset/security/cache/quarantine*) pozostaje w systemie nawet po usunięciu aplikacji ESET Endpoint Antivirus for macOS. Pliki poddane kwarantannie są przechowywane w bezpiecznej, zaszyfrowanej postaci. Można je przywrócić po ponownym zainstalowaniu programu ESET Endpoint Antivirus for macOS.



Poddaj pliki kwarantannie

Program ESET Endpoint Antivirus for macOS automatycznie poddaje kwarantannie usunięte pliki (jeśli ta opcja nie została anulowana w oknie alertu). Kliknij **Dodaj plik**, aby ręcznie poddać kwarantannie podejrzany plik. Możesz też przeciągnąć i upuścić plik lub folder, klikając plik lub folder, przesuwając wskaźnik myszy do zaznaczanego obszaru, przytrzymując wciśnięty przycisk myszy, a następnie zwalniając go.

Przywróć z kwarantanny

Wybierz plik poddany kwarantannie i kliknij przycisk **Przywróć**, aby przywrócić go do oryginalnej lokalizacji. Ta funkcja jest również dostępna po kliknięciu z wciśniętym klawiszem Ctrl (lub kliknięciu prawym przyciskiem myszy) danego pliku w oknie **Kwarantanna** i kliknięciu przycisku **Przywróć**. Menu kontekstowe oferuje również opcję **Przywróć do**, która umożliwia przywrócenie pliku do innej lokalizacji niż ta, z której został usunięty.

Przesyłanie pliku z kwarantanny

Jeśli poddano kwarantannie podejrzany plik, który nie został wykryty przez program, lub jeśli plik został błędnie oceniony jako zainfekowany (na przykład w drodze analizy heurystycznej kodu) i następnie poddany kwarantannie, należy przesłać plik do laboratorium firmy ESET. Aby przesłać plik z kwarantanny, należy kliknąć go z przytrzymanym klawiszem Ctrl (lub prawym przyciskiem myszy) i z menu kontekstowego wybrać polecenie **Prześlij do analizy**. Aby uzyskać więcej informacji o przesyłaniu próbki, patrz Prześlij próbkę.

Pomoc i obsługa

Program ESET Endpoint Antivirus for macOS udostępnia narzędzia i informacje ułatwiające rozwiązywanie problemów, które można napotkać. Sekcję Pomoc i wsparcie techniczne można znaleźć w oknie głównym aplikacji. Aby wyświetlić listę zainstalowanych składników, kliknij przycisk **Zobacz szczegóły** obok pozycji **Zainstalowane składniki**. Aby skopiować listę do schowka, kliknij prawym przyciskiem myszy dowolne miejsce w

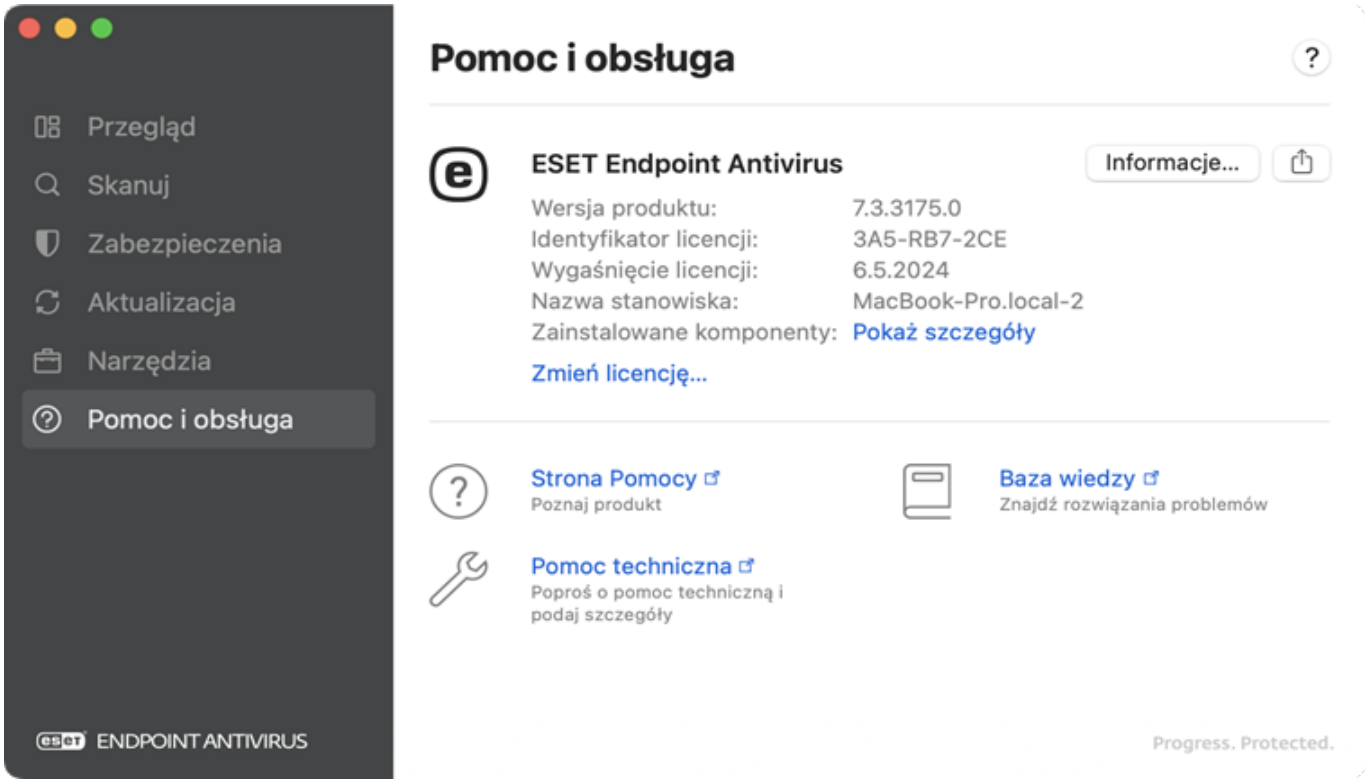
oknie Zainstalowane składniki, a następnie kliknij polecenie **Kopiuj wszystko**. Może to być przydatne podczas rozwiązywania problemów lub podczas kontaktowania się z pomocą techniczną.

Wyświetlana jest wersja **ESET Endpoint Antivirus for macOS** oraz identyfikator licencji produktu. Istnieje możliwość Zmiany licencji — kliknij tę opcję, aby otworzyć okno aktywacji i aktywować produkt. Klikając przyciskInformacje, możesz wyświetlić więcej informacji o ESET Endpoint Antivirus for macOS.

Strona Pomocy — kliknięcie tego łącza powoduje otwarcie stron pomocy programu ESET Endpoint Antivirus for macOS.

Pomoc techniczna — jeśli nie możesz rozwiązać problemu za pomocą naszych stron pomocy, skontaktuj się z pomocą techniczną firmy ESET.

Baza wiedzy — odwiedź Bazę wiedzy firmy ESET, aby znaleźć odpowiedzi na często zadawane pytania i zalecane rozwiązania różnych problemów. Dzięki regularnym aktualizacjom przez specjalistów z firmy ESET baza wiedzy jest bardzo skutecznym narzędziem do rozwiązywania różnych problemów.



Narzędzia terminalowe i demony

Narzędzia wiersza poleceń

- ./lslog — narzędzie do tworzenia list dzienników i wyświetlania dzienników zebranych przez ESET Endpoint Antivirus for macOS.

- ./odscan — skaner na żądanie, który może służyć do uruchomienia skanowania na żądanie za pośrednictwem okna Terminala.

- ./cfg — narzędzie konfiguracyjne, które może służyć do importowania i eksportowania ustawień ESET Endpoint Antivirus for macOS.

• ./mdm-info — informacyjne narzędzie mdm, które wyświetla informacje potrzebne do utworzenia profili konfiguracji potrzebnych do ukończenia konfiguracji przed instalacją za pośrednictwem MDM.

• ./lic — nadrzędzie licencjonujące, które służy do aktywacji ESET Endpoint Antivirus for macOS przy użyciu zakupionego klucza licencyjnego lub do sprawdzenia statusu aktywacji i ważności licencji.

• ./upd — narzędzie do aktualizacji modułów, które służy do aktualizowania modułów lub modyfikowania ustawień aktualizacji.

• ./quar — narzędzie do zarządzania kwarantanną, które służy do zarządzania elementami poddanymi kwarantannie.

Kwarantanna

Kwarantanna umożliwia bezpieczne przechowywanie zainfekowanych plików. Pliki należy poddawać kwarantannie w przypadku, gdy nie można ich wyleczyć, gdy ich usunięcie nie jest bezpieczne lub zalecane, lub gdy są one nieprawidłowo wykrywane przez program ESET Endpoint Antivirus for macOS. Do kwarantanny można przenieść każdy plik, co jest zalecane, jeśli plik zachowuje się w podejrzany sposób, ale nie jest wykrywany przez skaner antywirusowy. Pliki poddane kwarantannie można przesłać do analizy przez ESET Virus Lab.

Zarządzanie elementami poddanymi kwarantannie za pośrednictwem Terminala

Składnia: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar [OPTIONS]`

Opcje — skrócona forma	Opcje — długa forma	Opis
-i	--import	Importuj plik do kwarantanny
-l	--list	Wyświetl listę plików poddanych kwarantannie
-r	--restore=id	Przywróć element poddany kwarantannie i oznaczony identyfikatorem do ścieżki zdefiniowanej przez --restore-path
-e	--restore-exclude=id	Przywróć element poddany kwarantannie oznaczony identyfikatorem i symbolem „x” w kolumnie elementów do wykluczenia
-d	--delete=id	Usuń element poddany kwarantannie oznaczony identyfikatorem
	--restore-path=path	Nowa ścieżka do przywrócenia elementu poddanego kwarantannie
-h	--help	Pokaż pomoc
-v	--version	Pokaż informacje o wersji i zakończ.

> **Przywróć**
> Przywracanie jest niedostępne, jeśli polecenie nie jest wykonywane przez uprzywilejowanego użytkownika.

Przykład

Usuń element poddany kwarantannie o identyfikatorze „0123456789”:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -d 0123456789
```

lub

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --delete=0123456789
```

Przywróć element poddany kwarantannie o identyfikatorze „9876543210” do folderu *Download* zalogowanego użytkownika i zmień jego nazwę na *restoredFile.test* :

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -r 9876543210 --
restore-path=/Users/$USER/Desktop/restoredFile.test
```

lub

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --
restore=9876543210 --restore-path=/Users/$USER/Desktop/restoredFile.test
```

Przywróć element poddany kwarantannie o identyfikatorze „9876543210”, oznaczony symbolem „**x**” w kolumnie elementów **do wykluczenia**, do folderu *Download*:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -e 9876543210 --
restore-path=/Users/$USER/Downloads/restoredFile.test
```

lub

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --restore-
exclude=9876543210 --restore-path=/Users/$USER/Downloads/restoredFile.test
```

Przywróć plik z kwarantanny za pośrednictwem Terminala

1. Stwórz listę elementów poddanych kwarantannie.
   `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -l`

2. Wyszukaj identyfikator i nazwę obiektu poddanego kwarantannie, który chcesz przywrócić, a następnie uruchom następujące polecenie:
   `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-`

Konfiguracja

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/cfg --export-
xml=/tmp/export.xml
```

Konfiguracja importowania

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/cfg --import-xml=/tmp/export.xml
```

Dostępne opcje

Skrócona forma	Długa forma	Opis
	--import-xml	importowanie ustawień
	--export-xml	eksportowanie ustawień
-h	--help	pokaż pomoc
-v	--version	pokaż informacje o wersji

Zdarzenia

Ważne działania podejmowane w interfejsie internetowym ESET Endpoint Antivirus for macOS, nieudane próby logowania do interfejsu internetowego, polecenia związane z ESET Endpoint Antivirus for macOS, wykonywane za pośrednictwem Terminala, a także dodatkowe informacje są rejestrowane na ekranie **Zdarzenia**.

Każde zarejestrowane działanie uwzględnia następujące informacje: godzina wystąpienia zdarzenia, komponent (jeśli dostępny), zdarzenie i użytkownik.

Wyświetlanie zdarzeń za pośrednictwem Terminala

Aby wyświetlić zawartość ekranu **Zdarzenia** w oknie Terminala, użyj narzędzia wiersza polecenia o nazwie `lslog`.

Składnia: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog [OPTIONS]`

Opcje — skrócona forma	Opcje — długa forma	Opis
-f	--follow	Poczekaj na nowe dzienniki i dodaj je do wyników
-o	--optimize	Optymalizuj zapiszy w dzienniku.
-c	--csv	Wyświetlanie dzienników w formacie CSV.
-e	--events	Wyświetlanie listy dzienników zdarzeń.
-u	--urls	Wyświetl rekordy dziennika adresów URL.
-n	--sent-files	Wyświetlanie listy plików przesłanych do analizy.
-s	--scans	Pokaż dzienniki skanowania na żądanie.
	--with-log-name	Dodatkowe wyświetlanie kolumny „Nazwa dziennika”.
	--ods-details=log-name	Wyświetlanie szczegółów skanowania na żądanie identyfikowanego nazwą dziennika.
	--ods-events=log-name	Drukowanie znalezionych wykryć i plików, które nie zostały przeskanowane podczas określonego skanowania na żądanie identyfikowanego nazwą dziennika.

Opcje — skrócona forma	Opcje — długa forma	Opis
	--ods-detections=log-name	Wyświetlanie wykryć w ramach skanowania na żądanie identyfikowanego nazwą dziennika.
	--ods-notscanned=log-name	Wyświetlanie elementów nieprzeskanowanych w ramach skanowania na żądanie identyfikowanego nazwą dziennika.
-d	--detections	Lista dziennika wykrytych zagrożeń.
-b	--blocked files	Wyświetl dziennik zablokowanych plików.

Przykłady

Wyświetl wszystkie dzienniki zdarzeń:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog -e
```

Zapisz wszystkie dzienniki zdarzeń w formacie CSV w katalogu *Dokumenty* bieżącego użytkownika:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog -
ec > /Users/$USER/Desktop/eventlogs.csv
```

Aktualizuj moduły wykrywania za pośrednictwem Terminala

Aktualizuj moduły za pośrednictwem Terminala

Aby zaktualizować wszystkie moduły produktów w oknie Terminala, wykonaj następujące polecenie:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd -u
```

Aktualizacja i cofanie zmian za pośrednictwem Terminala

Opcje — skrócona forma	Opcje — długa forma	Opis
-u	--update	Zaktualizuj moduły
-c	--cancel	Anuluj pobieranie modułów
-e	--resume	Odblokowanie aktualizacji
-r	--rollback=VALUE	Cofnięcie do najstarszej migawki modułu skanera i zablokowanie wszystkich aktualizacji na liczbę godzin określoną parametrem WARTOŚĆ.
-l	--list-modules	Wyświetl listę modułów produktu
	--check-app-update	Sprawdź dostępność nowych wersji produktu w repozytorium

Opcje — skrócona forma	Opcje — długa forma	Opis
	--download-app-update	Pobierz nową wersję produktu, jeśli jest dostępna
	--perform-app-update	Pobierz i zainstaluj nową wersję produktu, jeśli jest dostępna
	--accept-license	Zaakceptuj zmiany licencji

Ograniczenie narzędzia upd
Za pomocą narzędzia upd nie można wprowadzać zmian w konfiguracji produktu.

Aby zatrzymać aktualizacje na 48 godzin i przywrócić najstarszą migawkę modułu skanera, wykonaj następujące polecenie jako uprzywilejowany użytkownik:
```
sudo /opt/eset/efs/bin/upd --rollback=48
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```
Aby wznowić automatyczne aktualizacje modułu skanera, wykonaj następujące polecenie jako uprzywilejowany użytkownik:
```
sudo /opt/eset/efs/bin/upd --resume
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```
Aby przeprowadzić aktualizację z serwera lustrzanego dostępnego pod adresem IP „192.168.1.2” i pod numerem portu „2221”, wykonaj następujące polecenie jako uprzywilejowany użytkownik:
```
sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```

Skanowanie na żądanie za pośrednictwem Terminala

Składnia: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan [OPTIONS..]`

Opcje — skrócona forma	Opcje — długa forma	Opis
-l	--list	Pokaż aktualnie uruchomione skanowania
	--list-profiles	Pokaż wszystkie dostępne profile skanowania
	--all	Pokaż również skanowania wykonane przez innego użytkownika (wymaga uprawnień użytkownika głównego)
-r	--resume=session_id	Wznów wcześniej wstrzymane skanowanie identyfikowane przez session_id
-p	--pause=session_id	Wstrzymaj skanowanie identyfikowane przez session_id
-t	--stop=session_id	Zatrzymaj skanowanie identyfikowane przez session_id
-s	--scan	Start scan
	--show-scan-info	Wyświetl podstawowe informacje (w tym log_name) na temat rozpoczętego skanowania
	--profile=PROFILE	Skanuj z wybranym PROFILEM
	--profile-priority=PRIORYTET	Zadanie zostanie uruchomione z określonym priorytetem. Dostępne priorytety: normalny, niższy, najniższy, bezczynność
	--readonly	Skanuj bez leczenia
	--local	Skanuj dyski lokalne
	--network	Skanowanie dysków sieciowych

Opcje — skrócona forma	Opcje — długa forma	Opis
	--removable	Skanowanie nośników wymiennych
	--exclude=FILE	Pomiń wybrany plik lub katalog
	--ignore-exclusions	Skanuj także wyłączone ścieżki i rozszerzenia

Narzędzie `odscan` obejmuje kod zakończenia po ukończeniu skanowania. Wykonaj polecenie `echo $?` w oknie Terminala po zakończeniu skanowania, aby wyświetlić kod zakończenia.

Kody zakończenia

Kod zakończenia	Znaczenie
0	Nie znaleziono zagrożenia.
1	Zagrożenie zostało wykryte i usunięte.
10	Niektórych plików nie można przeskanować (mogą stanowić zagrożenia).
50	Znaleziono zagrożenie.
100	Błąd

Przykład

Uruchom rekurencyjnie skanowanie na żądanie katalogu */root/* z profilem skanowania „@Smart scan” jako procesem w tle:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@Smart scan" / &
```

Uruchom skanowanie na żądanie z profilem skanowania „@Smart scan” rekurencyjnie dla wielu miejsc docelowych:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@Smart scan" /Application/ /tmp/ /home/
```

Wyświetl wszystkie uruchomione skanowania

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -l
```

Wstrzymaj skanowanie z session-id „15”. Każde skanowanie ma swój unikatowy identyfikator sesji generowany podczas jego uruchamiania.

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -p 15
```

Zatrzymaj skanowanie z session-id „15”. Każde skanowanie ma swój unikatowy identyfikator sesji generowany podczas jego uruchamiania.

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -t 15
```

Uruchom skanowanie na żądanie z wyłączonym katalogiem */exc_dir* i z wyłączonym plikiem */eicar.com*:

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@In-depth scan" --exclude=/exc_dir/ --exclude=/eicar.com /
```

Skanuj sektor startowy urządzeń wymiennych. Wykonaj poniższe polecenie jako użytkownik uprzywilejowany.

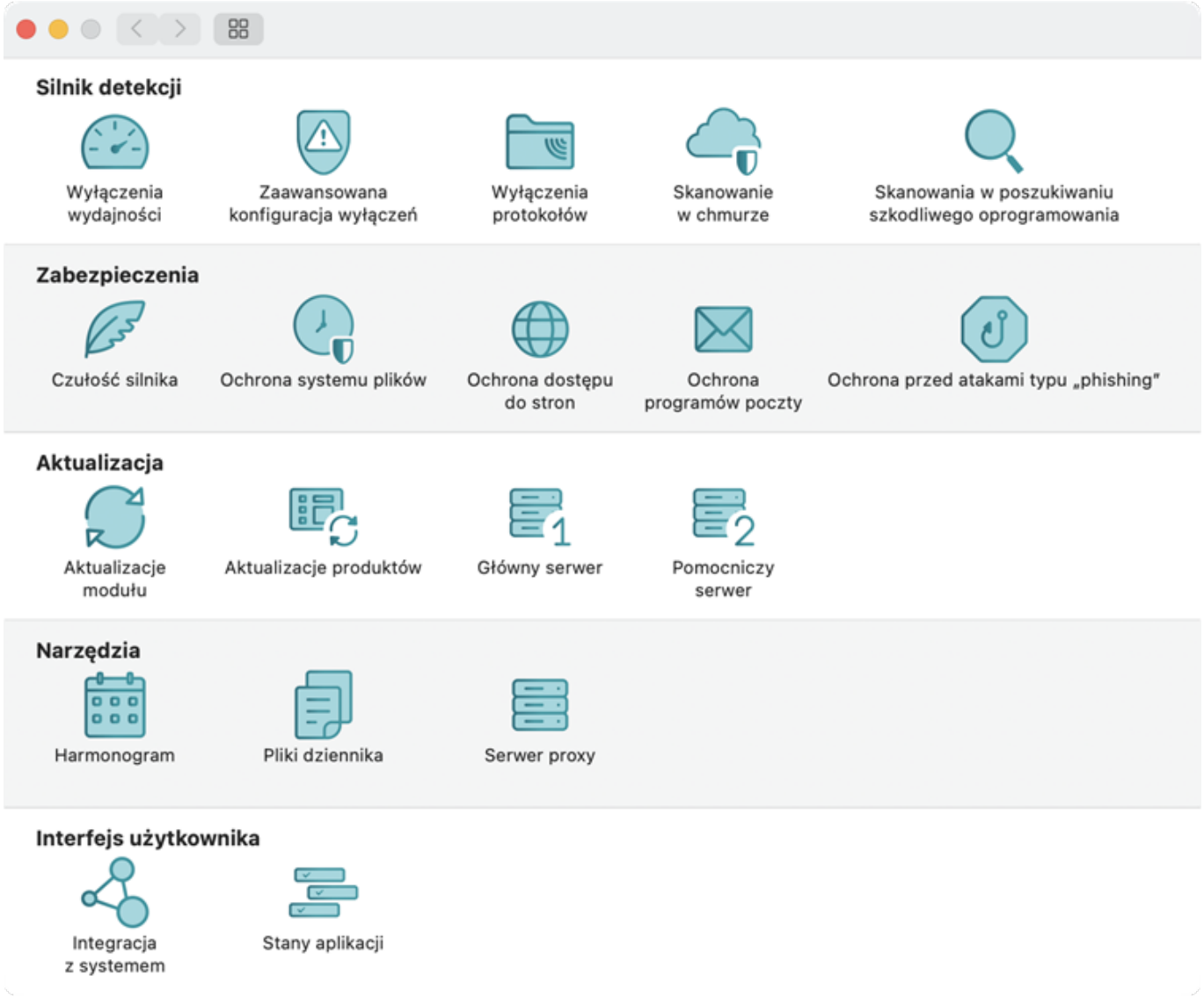
```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --
profile="@In-depth scan" --boot-removable
```

Preferencje aplikacji

Aby zmodyfikować zaawansowane ustawienia programu ESET Endpoint Antivirus for macOS, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia).

Ustawienia modułu można skonfigurować dla następujących kategorii:

- Silnik detekcji
- Zabezpieczenia
- Aktualizacja
- Narzędzia
- Interfejs użytkownika



Silnik detekcji

Silnik detekcji chroni system przed złośliwym oprogramowaniem, kontrolując pliki. Jeśli na przykład zostanie wykryty obiekt sklasyfikowany jako szkodliwe oprogramowanie, rozpocznie się naprawa. Silnik detekcji najpierw eliminuje zagrożenie, blokując je, a następnie je leczy, usuwa lub przenosi do kwarantanny.

Aby zmodyfikować zaawansowane ustawienia **Silnika detekcji** programu ESET Endpoint Antivirus for macOS, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia).

Wyłączenia wydajności

W sekcji **Pliki i foldery wyłączone ze skanowania** można wykluczyć pewne pliki i foldery, aplikacje lub adresy IP/IPv6 ze skanowania. Poprzez wyłączenie ścieżek (folderów) ze skanowania można znacznie skrócić czas potrzebny na skanowanie systemu plików pod kątem szkodliwego oprogramowania.

- + — tworzy nowe wyłączenie; wprowadź ścieżkę do obiektu.
- − – usuwa zaznaczone elementy.

Pliki ze skanowania należy wykluczać tylko w przypadku poważnych problemów z ochroną w czasie rzeczywistym, ponieważ obniża to ogólny poziom ochrony.

Zaawansowana konfiguracja wyłączeń

Zaawansowana konfiguracja wyłączeń umożliwia wyłączenie obiektów z leczenia dzięki filtrowaniu nazwy wyłączenia, ścieżki do obiektu lub jego skrótu.

Podczas konfiguracji wyłączeń wykrycia należy podać określone kryteria wyłączeń. Należy podać prawidłową nazwę wykrycia lub skrót SHA-1. Aby znaleźć prawidłową nazwę lub skrót SHA-1, należy przejść do Pliki dziennika, a następnie wybrać z menu rozwijanego pozycję Wykrycia. Jest to przydatne w przypadku fałszywego alarmu dotyczącego próbki w programie ESET Endpoint Antivirus for macOS. Wyłączenia dotyczące prawdziwych infekcji są bardzo niebezpieczne. Należy rozważyć wyłączenie odpowiednich plików lub katalogów tylko na określony czas. Wyłączenia dotyczą także potencjalnie niepożądanych, niebezpiecznych i podejrzanych aplikacji.

Kryteria wykluczenia są następujące:

- **Dokładny plik** – Wyłącza plik na podstawie określonego skrótu SHA-1 bez względu na typ, lokalizację, nazwę i rozszerzenie pliku.
- **Wykrycie** — wyłącza poszczególne pliki według nazwy wykrycia.
- **Ścieżka + wykrycie** — wyłącza poszczególne pliki według nazwy wykrycia i ścieżki z uwzględnieniem nazwy pliku (np. `file:///Users/documentation/Downloads/eicar_com.zip`).

Z wyłączeń wykrycia należy korzystać tylko w przypadku poważnych problemów z wykrywaniem, np. szkodliwego oprogramowania, ponieważ wykluczenie szkodliwego oprogramowania ze skanowania obniża ogólny poziom ochrony.

Wyłączenia protokołów

Pozycje na liście wyłączeń zostaną wyłączone z filtrowania zawartości protokołów. Zalecamy użycie tej opcji tylko w przypadku adresów, o których wiadomo, że są godne zaufania.

Skanowanie w chmurze

Włączenie systemu reputacji ESET LiveGrid© (zalecane)

System reputacji ESET LiveGrid© poprawia wydajność rozwiązań firmy ESET do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.

Włączenie systemu informacji zwrotnych ESET LiveGrid©

Dane zostaną przesłane do dalszej analizy w laboratorium firmy ESET.

Przesyłanie próbek

Automatyczne przesyłanie wykrytych próbek: W zależności od wybranej opcji można przesyłać zainfekowane próbki do laboratorium firmy ESET w celu ich przeanalizowania i udoskonalenia wykrycia w przyszłości.

- Wszystkie wykryte próbki
- Wszystkie próbki oprócz dokumentów
- Nie przesyłaj

Automatyczne przesyłanie podejrzanych próbek: Podejrzane próbki przypominające zagrożenia i takie, których zawartość lub działanie jest nietypowe, są przesyłane do laboratorium firmy ESET w celu wykonania analizy.

- Pliki wykonywalne — typy plików: .exe, .dll, .sys
- Archiwum — typy plików: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- Skrypty — typy plików: .bat, .cmd, .hta, .js, .vbs, .ps1
- Dokumenty — dokumenty utworzone w pakiecie Microsoft Office, pakiecie Libre Office lub innym narzędziu pakietu Office albo pliki PDF z zawartością aktywną.
- Inne — typy plików: .jar, .reg, .msi, .swf, .lnk

Automatyczne wyłączenia przesyłania: Wykluczone pliki nie zostaną wysłane do laboratorium firmy ESET, nawet jeśli zawierają podejrzany kod.

Wysyłaj raporty o awariach i dane diagnostyczne

Wysyłaj dane, takie jak raporty o awariach, modułach czy zrzuty pamięci.

Pomóż w usprawnianiu produktu, przesyłając anonimowe dane statystyczne dotyczące jego używania

Zezwól firmie ESET na zbieranie anonimowych informacji o nowo wykrytych zagrożeniach, takich jak nazwa zagrożenia, data i godzina jego wykrycia, metoda wykrycia i skojarzone metadane, informacje o przeskanowanych plikach (skrót, nazwa pliku, pochodzenie pliku i telemetria), zablokowane i podejrzane adresy URL, wersja i konfiguracja produktu. Uwzględnione są także informacje o systemie użytkownika.

Kontaktowy adres e-mail (opcjonalnie)

Wraz z podejrzanymi plikami można wysyłać adres e-mail, który będzie używany do kontaktowania się z użytkownikiem, gdy przeprowadzenie analizy będzie wymagało dodatkowych informacji. Należy pamiętać, że specjaliści z firmy ESET kontaktują się z użytkownikiem tylko w szczególnych przypadkach, gdy wymagane są dodatkowe informacje.

Skanowania w poszukiwaniu szkodliwego oprogramowania

Skaner na żądanie jest ważną częścią rozwiązania antywirusowego, ponieważ skanuje pliki i foldery na komputerze. Z punktu widzenia bezpieczeństwa skanowanie komputera należy przeprowadzać regularnie w ramach rutynowych środków bezpieczeństwa, a nie tylko w przypadku podejrzenia infekcji. W sekcji **Skanowanie w poszukiwaniu szkodliwego oprogramowania** można skonfigurować opcje profili skanowania na żądanie:

Lista profili — aby utworzyć nową listę profili lub usunąć istniejącą, wybierz  lub  . Podczas dodawania nowej listy profili wpisz nazwę profilu i kliknij przycisk **OK**. Nowy profil zostanie wyświetlony w menu rozwijanym Wybrany profil, które zawiera menu rozwijane z listą istniejących profili skanowania.

Parametry ThreatSense — opcje konfiguracji profilu skanowania, takie jak rozszerzenia plików, które chcesz kontrolować, obiekty do skanowania, użyte metody wykrywania itp.

Zabezpieczenia

Aby zmodyfikować ustawienia zaawansowane programu ESET Endpoint Antivirus for macOS w zakresie **Ochrony**, otwórz **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia).

Czułość silnika

Czułość silnika umożliwia skonfigurowanie poziomów raportowania i ochrony następujących kategorii dla wszystkich modułów ochrony.

- **Szkodliwe oprogramowanie** — to elementy szkodliwego kodu, które stanowią część istniejących plików na komputerze.

- **Potencjalnie niepożądane aplikacje** — grayware lub potencjalnie niepożądane aplikacje (PUA) to szeroka kategoria oprogramowania, które nie jest tak jednoznacznie niebezpieczne jak inne rodzaje szkodliwego oprogramowania, np. wirusy lub konie trojańskie. Może ono jednak instalować niechciane oprogramowanie, zmieniać sposób działania urządzenia cyfrowego lub wykonywać działania, których użytkownik nie zatwierdził lub których się nie spodziewał. Więcej informacji na temat tych aplikacji można znaleźć w słowniczku.

- **Podejrzane aplikacje** — należą do nich programy skompresowane przy użyciu programów pakujących lub zabezpieczających. Programy zabezpieczające są często używane przez twórców szkodliwego oprogramowania w celu uniknięcia wykrycia. Programy spakowane to wykonywalne pliki archiwów samorozpakowujących, które w ramach jednego archiwum mogą zawierać różnego rodzaju szkodliwe oprogramowanie. Do najczęściej używanych formatów programów spakowanych należą UPX, PE_Compact, PKLite oraz ASPack. Użycie innego programu do kompresji może zmienić sposób wykrywania szkodliwego oprogramowania. Sygnatury programów spakowanych mogą również z czasem mutować, utrudniając wykrywanie i usuwanie szkodliwego oprogramowania.

- **Potencjalnie niebezpieczne aplikacje** — do aplikacji tych zaliczane są niektóre legalne programy komercyjne, które mogą zostać wykorzystane przez intruzów do prowadzenia niebezpiecznych działań w

przypadku ich zainstalowania bez zgody użytkownika. Ta klasyfikacja obejmuje programy, takie jak narzędzia dostępu zdalnego. Domyślnie opcja ta jest wyłączona.

Ochrona systemu plików

Jeśli jest używana technologia ESET LiveGrid© (opis w sekcji Ustawienia parametrów technologii ThreatSense), ochrona systemu plików w czasie rzeczywistym dla nowych plików może się różnić od ochrony już istniejących plików. Nowo utworzone pliki mogą być kontrolowane bardziej rygorystycznie.

Ze skanera Real-time można wykluczyć następujące nośniki:

- **Dyski lokalne** — dyski twarde w systemie
- **Nośniki wymienne** — nośniki USB, urządzenia Bluetooth itp.
- **Nośniki sieciowe** — wszystkie zmapowane dyski

Domyślnie wszystkie pliki są skanowane podczas **otwierania** i **tworzenia** plików. Zalecane jest zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalną ochronę komputera w czasie rzeczywistym.

Można również wykluczyć określone procesy ze skanowania.

Zalecane jest zachowanie ustawień domyślnych i modyfikowanie wyłączeń ze skanowania tylko w szczególnych przypadkach, jeśli na przykład sprawdzanie pewnych nośników znacznie spowalnia przesyłanie danych.

Ochrona dostępu do stron internetowych

Ochrona dostępu do stron internetowych monitoruje komunikację między przeglądarkami internetowymi i zdalnymi serwerami w celu zapewnienia zgodności z regułami protokołu HTTP (Hypertext Transfer Protocol).

Filtrowanie sieci internetowej można uzyskać, definiując numery portów dla komunikacji HTTP i adresów URL.

Protokoły sieciowe

W sekcji Protokoły sieciowe można włączyć lub wyłączyć sprawdzanie protokołu HTTP oraz zdefiniować numery portów używane do komunikacji HTTP. Domyślnie wstępnie zdefiniowane są numery portów 80, 8080 i 3128.

Zarządzanie adresami URL

Ta sekcja umożliwia określanie adresów HTTP w celu zablokowania, zezwolenia lub wyłączenia ze sprawdzania. Strony internetowe znajdujące się na liście zablokowanych adresów będą niedostępne. Dostęp do stron internetowych na liście wyłączonych adresów będzie uzyskiwany bez skanowania pod kątem szkodliwego kodu.

Aby aktywować listę dozwolonych, zablokowanych lub wykluczonych adresów, wybierz jeden z nich i włącz opcję **Lista aktywnych**. Aby otrzymywać powiadomienia podczas wprowadzania adresu z bieżącej listy, należy włączyć opcję **Powiadom o zastosowaniu**.

Można użyć symboli specjalnych *** (gwiazdka) i *?* (znak zapytania) na dowolnej liście. Gwiazdka zastępuje dowolny ciąg znaków, a znak zapytania — dowolny symbol. Szczególną ostrożność należy zachować podczas określania adresów wyłączonych, ponieważ lista powinna zawierać wyłącznie zaufane i bezpieczne adresy. Należy również

zapewnić prawidłowe stosowanie na symboli * i ?.

Ochrona programów poczty e-mail

Ochrona programów poczty e-mail — zapewnia sprawdzanie komunikacji e-mail przychodzącej za pośrednictwem protokołów POP3 oraz IMAP. Podczas analizowania wiadomości przychodzących program ESET Endpoint Antivirus for macOS stosuje zaawansowane metody skanowania dostępne w ramach technologii ThreatSense. Skanowanie komunikacji za pośrednictwem protokołów POP3 oraz IMAP odbywa się niezależnie od użytkowanego klienta poczty e-mail. Dostępne są następujące ustawienia:

Protokoły poczty e-mail

Można tu włączyć lub wyłączyć sprawdzanie komunikacji przychodzącej za pośrednictwem protokołów POP3 oraz IMAP.

Sprawdzanie protokołu POP3

Protokół POP3 jest najpopularniejszym protokołem używanym do odbioru poczty e-mail w programach poczty e-mail. Program ESET Endpoint Antivirus for macOS udostępnia ochronę tego protokołu bez względu na używany program poczty e-mail.

Moduł ochrony udostępniający tę opcję jest automatycznie inicjowany po uruchomieniu komputera i jest aktywny w pamięci. Aby moduł działał prawidłowo, należy włączyć sprawdzanie protokołu POP3. Kontrola protokołu POP3 jest wykonywana automatycznie, bez potrzeby ponownego konfigurowania programu poczty. Domyślnie skanowana jest cała komunikacja przechodząca przez port 110, ale w razie potrzeby można dodać pozostałe porty komunikacyjne. Numery portów należy oddzielić przecinkami.

Po włączeniu opcji sprawdzania protokołu POP3 cały ruch **POP3** będzie monitorowany pod kątem szkodliwego oprogramowania.

Sprawdzanie protokołu IMAP

IMAP (Internet Message Access Protocol) to kolejny protokół internetowy do odbierania poczty e-mail, który pod pewnymi względami jest lepszy niż protokół POP3. Program ESET Endpoint Antivirus for macOS zapewnia ochronę tego protokołu niezależnie od używanego programu poczty e-mail.

Moduł ochrony udostępniający tę opcję jest automatycznie inicjowany po uruchomieniu komputera i jest aktywny w pamięci. Aby moduł działał prawidłowo, należy włączyć sprawdzanie protokołu IMAP. Kontrola protokołu IMAP jest wykonywana automatycznie, bez potrzeby ponownego konfigurowania programu poczty. Domyślnie skanowana jest cała komunikacja przechodząca przez port 143, ale w razie potrzeby można dodać pozostałe porty komunikacyjne. Przecinek musi oddzielać numery portów.

W przypadku włączenia opcji **Sprawdzanie protokołu IMAP** cały ruch protokołu IMAP jest monitorowany pod kątem szkodliwego oprogramowania.

Tagi e-mail

Korzystanie ze znaczników wiadomości e-mail umożliwia dołączenie znacznika wiadomości do jej stopki. Po przeskanowaniu wiadomości e-mail może zostać do niej dołączone powiadomienie z wynikiem skanowania. Powiadomienia dołączane do wiadomości są przydatnym narzędziem, ale nie można ich traktować jako ostatecznego potwierdzenia bezpieczeństwa wiadomości, ponieważ mogą one być pomijane w problematycznych

wiadomościach HTML lub fałszowane przez pewne zagrożenia. Dostępne są następujące opcje:

- **Do otrzymanych i przeczytanych wiadomości e-mail po wykryciu** — tylko wiadomości e-mail zawierające złośliwe oprogramowanie są oznaczane jako sprawdzone.
- **Do wszystkich zeskanowanych wiadomości e-mail** — do wszystkich zeskanowanych wiadomości e-mail dołączane są znaczniki.
- **Nigdy** — znaczniki nie będą dodawane do żadnych wiadomości.

Aktualizuj temat odebranych wiadomości e-mail— zaznacz to pole wyboru, aby ochrona poczty e-mail obejmowała ostrzeżenia o zagrożeniu w zainfekowanej wiadomości. Ta opcja umożliwia proste filtrowanie zainfekowanych wiadomości e-mail. Zwiększa ona również wiarygodność odbiorcy oraz, w przypadku wykrycia infekcji, udostępnia ważne informacje o poziomie zagrożenia danej wiadomości e-mail lub jej nadawcy.

Dodaj do tematu wykrytej wiadomości e-mail — edytowanie tego szablonu pozwala zmodyfikować format przedrostka tematu zainfekowanej wiadomości e-mail.

Parametry technologii ThreatSense

Zaawansowana konfiguracja skanera umożliwia skonfigurowanie poziomów leczenia, opcji skanowania i rozszerzeń plików wykluczonych ze skanowania.

Ochrona przed atakami typu „phishing”

Ochrona przed atakami typu „phishing” to kolejna warstwa zabezpieczeń, zapewniająca wzmocnienie ochrony przed stronami internetowymi służącymi do prób bezprawnego pozyskiwania haseł oraz innych informacji poufnych. Ochrona przed atakami typu „phishing” jest domyślnie włączona i zalecamy, aby tak pozostało.

Aktualizacja

Ta sekcja umożliwia określenie informacji o źródle aktualizacji, w tym o używanych serwerach aktualizacji i dotyczących ich danych uwierzytelniających. Aby zmodyfikować ustawienia zaawansowane programu ESET Endpoint Antivirus for macOS w zakresie **Aktualizacji**, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia).

Aktualizacje modułów i produktów

Aktualizacje modułów

Typy aktualizacji

- **Regularne aktualizacje**. Jest to domyślny rodzaj aktualizacji. Dzięki temu baza sygnatur wykrywania i moduły produktów są automatycznie aktualizowane z serwerów aktualizacji ESET.
- **Aktualizacje w wersji wstępnej** zawierają najnowsze poprawki błędów i metody wykrywania, które w najbliższej przyszłości będą dostępne dla ogółu użytkowników. Jednak nie zawsze mogą być stabilne, dlatego nie zaleca się używania ich w środowisku produkcyjnym.

- **Opóźnione aktualizacje** umożliwiają aktualizowanie ze specjalnych serwerów aktualizacji udostępniających nowe wersje baz danych wirusów z opóźnieniem co najmniej X godzin (czyli baz danych przetestowanych w środowisku rzeczywistym i uznanych za stabilne).

Cofanie aktualizacji modułów

W razie podejrzeń, że nowa aktualizacja silnika detekcji i/lub modułu programu może być niestabilna lub uszkodzona, można wycofać zmiany i wrócić do poprzedniej wersji oraz wyłączyć aktualizacje na określony czas.

Utwórz migawki modułów

ESET Endpoint Antivirus for macOS rejestruje migawki silnika detekcji i modułu programu dla funkcji cofania zmian. Aby tworzyć migawki modułu bazy danych wirusów, należy pozostawić włączony przełącznik opcji **Utwórz migawki modułów**. Gdy opcja ta jest włączona, pierwsza migawka tworzona jest przy pierwszej aktualizacji. Następna po 48 godzinach. Pole **Liczba kopii przechowywanych lokalnie**określa liczbę przechowywanych migawek silnika detekcji.

> Po osiągnięciu maksymalnej ilości migawek (na przykład trzy), najstarsza jest zastępowana nową migawką co 48 godzin. ESET Endpoint Antivirus for macOS dla macOS potrafi przywrócić wersję silnika detekcji i aktualizacji modułu programu do najstarszej migawki.

Aktualizacje produktów

Aktualizacje produktu zapewniają, że zawsze używasz najnowszej wersji produktu. Włącz przełącznik **Aktualizacja automatyczna**, aby aktualizacje produktu były instalowane automatycznie przy następnym ponownym uruchomieniu i aby utrzymać stały dostęp do najnowszych funkcji i najlepszej ochrony.

Serwer podstawowy i dodatkowy

Opcja automatycznego wyboru podstawowego i dodatkowego serwera aktualizacji jest domyślnie włączona. Oba serwery można określić, gdy przełącznik wyboru automatycznego zostanie wyłączony.

Narzędzia

Aby zmodyfikować zaawansowane ustawienia **Narzędzi** programu ESET Endpoint Antivirus for macOS, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia).

Harmonogram

Harmonogram umożliwia konfigurację zadań skanowania na żądanie wykonywanych automatycznie o określonej godzinie. Aby utworzyć nowe zaplanowane zadanie lub usunąć istniejące, wybierz + lub −. Możesz również zdefiniować dzień lub dni, w których zadanie ma być powtarzane.

Pliki dziennika

Szczegółowość dziennika

Szczegółowość zapisywania w dzienniku definiuje poziom szczegółów zawartych w plikach dziennika.

- **Ostrzeżenia krytyczne** — obejmuje tylko błędy krytyczne (na przykład: **Nie udało się uruchomić ochrony antywirusowej**)
- **Błędy** — rejestrowanie błędów takich jak **Błąd pobierania pliku** poza ostrzeżeniami krytycznymi.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Rekordy informacyjne** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Rekordy diagnostyczne** — zawierają informacje potrzebne do ulepszania konfiguracji programu, a także wszystkich rekordów wyższych kategorii.

Czyszczenie plików dziennika

Automatycznie usuwaj rekordy starsze niż (dni) — wpisy dziennika starsze niż podana liczba dni będą usuwane automatycznie.

Optymalizacja plików dziennika

Automatycznie optymalizuj pliki dzienników — włączenie tej opcji powoduje automatyczną defragmentację plików dziennika po przekroczeniu stopnia fragmentacji określonego w polu **Jeśli liczba nieużywanych rekordów przekracza (%)**. Wszystkie puste wpisy dzienników są usuwane w celu zwiększenia wydajności i szybkości przetwarzania dzienników. Poprawę można zauważyć, gdy dzienniki zawierają dużo wpisów.

Ustawienia serwera proxy

Tutaj możesz określić ustawienia serwera proxy. Zdefiniowane parametry będą używane przez wszystkie moduły wymagające połączenia z Internetem.

Aby skonfigurować serwer proxy:

1. Włącz opcję **Użyj serwera proxy** i wpisz adres serwera proxy w polu **Serwer proxy** oraz numer **Portu** serwera proxy.
2. Włącz opcję **Użyj bezpośredniego połączenia**, jeśli serwer proxy jest niedostępny do pominięcia i komunikuje się bezpośrednio z serwerami ESET.
3. Jeśli komunikacja z serwerem proxy wymaga uwierzytelnienia, włącz opcję **Serwer proxy wymaga uwierzytelniania** i wprowadź prawidłową **Nazwę użytkownika** i **Hasło** w odpowiednich polach.

Interfejs użytkownika

Aby zmodyfikować zaawansowane ustawienia **Interfejsu użytkownika** programu ESET Endpoint Antivirus for macOS, otwórz okno **Preferencje aplikacji**, używając cmd+, lub klikając ESET Endpoint Antivirus for macOS na pasku menu macOS i wybierając opcję **Preferencje** (Ustawienia).

Integracja z systemem

Elementy interfejsu użytkownika

Zezwól użytkownikowi na otwieranie graficznego interfejsu użytkownika — Wyłącz to ustawienie, aby uniemożliwić użytkownikom dostęp do graficznego interfejsu użytkownika. Ten tryb może być przydatny w środowiskach zarządzanych lub gdy trzeba oszczędzać zasoby systemowe.

Pokazuj ikonę w elementach dodatkowych paska menu — Wyłączenie tego ustawienia powoduje usunięcie ikony ESET Endpoint Antivirus for macOS z elementów dodatkowych paska menu w ramach menu systemu macOS (u góry ekranu).

Powiadomienia

Wyświetlaj powiadomienia na pulpicie — powiadomienia na pulpicie (takie jak komunikaty o pomyślnej aktualizacji, ukończenie zadań skanowania antywirusowego lub znalezienie nowych zagrożeń) są reprezentowane przez okno alertu obok paska menu systemu macOS. Jeśli ta opcja jest włączona, ESET Endpoint Antivirus for macOS może informować o wystąpieniu nowego zdarzenia.

Stany aplikacji

W tym miejscu można wybrać statusy aplikacji widoczne w programie ESET Endpoint Antivirus for macOS i konsoli internetowej. Po zgłoszeniu problemu, dla którego przełącznik **Pokaż stan** jest wyłączony, aplikacja ESET Endpoint Antivirus for macOS zachowuje zielony stan **Jesteś chroniony**.

Odinstalowanie

Dezinstalacja lokalna

Nie można całkowicie odinstalować ESET Endpoint Antivirus for macOS poprzez przeciągnięcie ikony ESET Endpoint Antivirus for macOS do Kosza z folderu Aplikacje. Rozszerzenie systemu pozostanie zainstalowane na komputerze, a Uninstaller.app nie będzie mógł ich później usunąć.
Aby uniemożliwić użytkownikom odinstalowywanie ESET Endpoint Antivirus for macOS, zalecamy dodanie oznaczenia „no modify” do programu ESET Endpoint Antivirus for macOS. Aby dodać oznaczenie „no modify”, uruchom następujące polecenie na komputerze docelowym:

```
sudo chflags -Rf schg /Applications/ESET\ Endpoint\ Antivirus\.app
```

Przed odinstalowaniem ESET Endpoint Antivirus for macOS należy usunąć oznaczenie „no modify”. Aby usunąć oznaczenie „no modify”, uruchom następujące polecenie na komputerze docelowym:

```
sudo chflags -Rf noschg /Applications/ESET\ Endpoint\ Antivirus\.app
```

Aby odinstalować ESET Endpoint Antivirus for macOS:

Jeśli zarządzasz ESET Endpoint Antivirus for macOS za pomocą ESET PROTECT On-Prem lub ESET PROTECT CLOUD, możesz utworzyć i uruchomić zadanie klienta, aby zdalnie odinstalować ESET Endpoint Antivirus for macOS:
- Utwórz i uruchom zadanie Odinstalowywanie oprogramowania w programie ESET PROTECT On-Prem.
- Utwórz i uruchom zadanie Odinstalowywanie oprogramowania w programie ESET PROTECT CLOUD.

1. Uruchom Dezinstalator programu ESET Endpoint Antivirus for macOS. Dezinstalator programu ESET Endpoint Antivirus for macOS można uruchomić na wiele sposobów:

- Otwórz plik instalacyjny programu ESET Endpoint Antivirus for macOS (*.dmg*) i kliknij dwukrotnie opcję Odinstaluj.

- Uruchom Finder, otwórz folder Aplikacje na dysku twardym, kliknij z naciśniętym klawiszem Ctrl (lub prawym przyciskiem myszy) ikonę **ESET Endpoint Antivirus for macOS** > wybierz opcję **Pokaż zawartość pakietu** z menu skrótów. Otwórz folder **Contents** > **Helpers** i kliknij dwukrotnie ikonę Uninstaller.

2. Kliknij przycisk **Odinstaluj**, aby rozpocząć proces odinstalowywanie. Zostanie wyświetlony monit o wpisanie hasła administratora.

Jeśli wystąpi problem z usunięciem rozszerzeń systemu, podczas procesu odinstalowywania może zostać wyświetlony monit o wpisanie hasła administratora.

3. Jeśli odinstalowujesz ESET Endpoint Antivirus for macOS w systemie macOS 12 Monterey, zostaniesz poproszony o zezwolenie Uninstaller.app na zarządzanie użytkownikami utworzonymi przez ESET Endpoint Antivirus for macOS. Zostanie wyświetlone następujące okno dialogowe:
„Uninstaller.app” chce uzyskać dostęp do administrowania komputerem. Administrowanie może dotyczyć modyfikowania haseł, ustawień usług sieciowych oraz systemowych.
Kliknij przycisk OK. Jeśli klikniesz przycisk Nie zezwalaj, ESET Endpoint Antivirus for macOS nie zostanie całkowicie odinstalowany.

4. Kliknij przycisk Zamknij, aby zamknąć Dezinstalator.

5. Uruchom ponownie komputer.

Odinstalowanie za pomocą wiersza poleceń

Możesz odinstalować ESET Endpoint Antivirus for macOS poprzez uruchomienie skryptu dezinstalacyjnego z **Terminala**. Jeśli zainstalowano ESET Endpoint Antivirus for macOS w lokalizacji domyślnej, uruchom następujące polecenie:

```
sudo /Applications/ESET\ Endpoint\
Antivirus.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```

Pomoc techniczna

Kontakt z działem pomocy technicznej

Jeśli nie możesz znaleźć odpowiedzi na problem, możesz użyć tego formularza dostępnego w witrynie firmy ESET, aby szybko skontaktować się z działem pomocy technicznej firmy ESET.

Dostarcz informacje działowi pomocy technicznej

Aby zapewnić szybkie i pomyślne rozwiązanie problemu, zalecamy wykonanie następujących czynności podczas tworzenia zgłoszenia:

- Dołącz informacje takie jak szczegóły na temat licencji, nazwa produktu, wersja produktu i system operacyjny.
- Opisz szczegółowo swój problem.
- Dołącz zrzuty ekranu lub film przedstawiający problem.
- Dołącz dzienniki z ESET LogCollector.

ESET LogCollector

ESET LogColletor tworzy dzienniki zawierające ważne informacje, które mogą przydać się pomocy technicznej i programistom w identyfikacji problemów napotkanych podczas korzystania z ESET Endpoint Antivirus for macOS.

Szczegółowe informacje na temat ESET LogCollector można znaleźć w artykule bazy wiedzy ESET. Artykuł może nie być dostępny we wszystkich językach.

Aby utworzyć dzienniki za pomocą ESET LogCollector:

1. Pobieranie ESET LogCollector.
2. Otwórz plik **eset_logcollector.dmg** i uruchom aplikację LogCollector.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby utworzyć dzienniki.

> **Wskazówki dotyczące korzystania z ESET LogCollector**
> - Aby utworzyć bardziej szczegółowe dzienniki dla pomocy technicznej firmy ESET, w sekcji **Replikacja** kliknij ikonę koła zębatego i otwórz opcje zaawansowane.
> - Nie należy uruchamiać replikacji, zanim nie będzie można odtworzyć problemu i kroków, które do niego doprowadziły.

Po utworzeniu plików dziennika można je znaleźć na pulpicie w archiwum **customer_info.zip**. Dołącz ten plik do zgłoszenia do pomocy technicznej.

Umowa Licencyjna Użytkownika Końcowego

Obowiązuje od 19 października 2021 r..

WAŻNE: Przed pobraniem, zainstalowaniem, skopiowaniem lub użyciem Oprogramowania należy się dokładnie zapoznać z poniższymi warunkami korzystania z produktu. **POBRANIE, ZAINSTALOWANIE, SKOPIOWANIE LUB UŻYCIE OPROGRAMOWANIA OZNACZA WYRAŻENIE ZGODY NA NINIEJSZE WARUNKI I AKCEPTACJĘ POLITYKI**

PRYWATNOŚCI.

Umowę Licencyjną Użytkownika Końcowego

Niniejsza Umowa licencyjna użytkownika końcowego („Umową"), zawierana między spółką ESET, spol. s r. o., z siedzibą w Słowacji pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, zarejestrowaną w Rejestrze Handlowym Sądu Rejonowego dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 („firmą ESET" lub „Dostawcą"), a licencjobiorcą, który jest osobą fizyczną lub prawną („Licencjobiorcą" lub „Użytkownikiem końcowym"), uprawnia Licencjobiorcę do korzystania z Oprogramowania określonego w punkcie 1 niniejszej Umowy. Oprogramowanie określone w punkcie 1 niniejszej Umowy może znajdować się na nośniku danych albo zostać przesłane pocztą elektroniczną, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł na warunkach wyszczególnionych poniżej.

NINIEJSZA UMOWA DOTYCZY WYŁĄCZNIE OKREŚLENIA PRAW UŻYTKOWNIKA KOŃCOWEGO I NIE STANOWI UMOWY SPRZEDAŻY. Dostawca pozostaje właścicielem kopii Oprogramowania i nośnika fizycznego zawartego w opakowaniu z produktem, a także wszystkich innych kopii Oprogramowania, które Użytkownik końcowy może wykonać zgodnie z niniejszą Umową.

Kliknięcie opcji „Akceptuję" lub „Akceptuję..." w trakcie instalowania, pobierania, kopiowania lub używania Oprogramowania oznacza, że Licencjobiorca wyraża zgodę na warunki określone w niniejszej Umowie oraz akceptuje Politykę prywatności. Jeśli Licencjobiorca nie wyraża zgody na którykolwiek warunek określony w niniejszej Umowie i/lub Polityce prywatności, powinien niezwłocznie kliknąć opcję anulowania i przerwać instalację lub pobieranie albo zniszczyć Oprogramowanie, nośnik instalacyjny, dokumentację towarzyszącą Oprogramowaniu i dowód sprzedaży Oprogramowania bądź zwrócić je Dostawcy lub w miejscu zakupu Oprogramowania.

LICENCJOBIORCA PRZYJMUJE DO WIADOMOŚCI, ŻE KORZYSTANIE Z OPROGRAMOWANIA OZNACZA ZAPOZNANIE SIĘ Z NINIEJSZĄ UMOWĄ, ZROZUMIENIE WARUNKÓW W NIEJ OKREŚLONYCH ORAZ ZOBOWIĄZANIE DO ICH PRZESTRZEGANIA.

1. **Oprogramowanie.** W niniejszej Umowie termin „Oprogramowanie" oznacza: (i) program komputerowy, do którego dołączono niniejszą Umowę, i wszystkie jego składniki; (ii) całą zawartość dysków, płyt CD-ROM i płyt DVD, wiadomości e-mail wraz z ich załącznikami oraz innych nośników, do których jest dołączona niniejsza Umowa, w tym Oprogramowanie w formie kodu obiektowego dostarczone na nośniku danych albo za pośrednictwem poczty elektronicznej lub Internetu; (iii) wszelkie powiązane drukowane materiały instruktażowe oraz wszelką inną dokumentację powiązaną z Oprogramowaniem, w tym przede wszystkim wszelkie opisy Oprogramowania, jego dane techniczne, wszelkie opisy jego właściwości lub działania, wszelkie opisy środowiska operacyjnego, w którym Oprogramowanie jest używane, instrukcje obsługi lub instalacji Oprogramowania oraz wszelkie opisy sposobu korzystania z Oprogramowania („Dokumentacją"); (iv) wszelkie ewentualne kopie Oprogramowania, poprawki możliwych błędów Oprogramowania, dodatki do Oprogramowania, rozszerzenia Oprogramowania, zmodyfikowane wersje Oprogramowania oraz aktualizacje składników Oprogramowania, na które Dostawca udziela Licencjobiorcy licencji zgodnie z zapisami w punkcie 3 niniejszej Umowy. Oprogramowanie będzie dostarczane wyłącznie w postaci wykonywalnego kodu obiektowego.

2. **Instalacja, komputer i klucz licencyjny**. Oprogramowanie dostarczone na nośniku danych, otrzymane za pośrednictwem poczty elektronicznej, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł musi zostać zainstalowane. Oprogramowanie należy zainstalować na prawidłowo skonfigurowanym komputerze, który spełnia minimalne wymagania określone w Dokumentacji. Procedurę instalacji również opisano w Dokumentacji. Na komputerze, na którym zostanie zainstalowane Oprogramowanie, nie można instalować sprzętu komputerowego ani programów komputerowych, które mogłyby niekorzystnie wpłynąć na Oprogramowanie. Komputer oznacza sprzęt, w tym między innymi komputery osobiste, laptopy, stacje robocze, palmtopy, smartfony, przenośne urządzenia elektroniczne lub inne urządzenia elektroniczne, dla których przeznaczone jest Oprogramowanie, na których zostanie zainstalowane i/lub będzie używane. Klucz licencyjny

oznacza niepowtarzalny ciąg symboli, liter, cyfr i znaków specjalnych, dostarczony Użytkownikowi końcowemu w celu umożliwienia mu legalnego korzystania z Oprogramowania, jego określonych wersji lub rozszerzenia warunków Licencji zgodnie z niniejszą Umową.

3. **Licencja**. Dostawca udziela Licencjobiorcy praw określonych poniżej (w dalszej części nazywanych zbiorczo „Licencją"), jeśli Licencjobiorca zobowiązał się przestrzegać i przestrzega wszelkich warunków określonych w niniejszej Umowie:

a) **Instalacja i użycie.** Licencjobiorcy przysługują niewyłączne, nieprzenoszalne prawa do zainstalowania Oprogramowania na dysku twardym komputera lub na innym nośniku do trwałego przechowywania danych, do zainstalowania i przechowywania Oprogramowania w pamięci systemu komputerowego oraz do zaimplementowania, przechowywania i wyświetlania Oprogramowania.

b) **Postanowienia w sprawie liczby Licencji.** Prawo do korzystania z Oprogramowania w ramach jednej Licencji jest ograniczone do jednego Użytkownika końcowego. Jeden Użytkownik końcowy oznacza: (i) instalację Oprogramowania na jednym komputerze lub, jeśli liczba Licencji zależy od liczby skrzynek pocztowych, (ii) użytkownika komputera, który odbiera pocztę elektroniczną za pośrednictwem klienta poczty elektronicznej. Jeśli do klienta poczty elektronicznej dociera poczta elektroniczna, która jest następnie automatycznie dystrybuowana do innych użytkowników, liczbę Użytkowników końcowych stanowi liczba wszystkich użytkowników, do których jest dostarczana poczta. Jeśli serwer poczty pełni funkcję bramy pocztowej, liczba Użytkowników końcowych jest równa liczbie użytkowników serwera poczty, którzy są obsługiwani przez tę bramę. Jeśli jeden użytkownik odbiera pocztę przesyłaną na różne adresy e-mail (np. za pośrednictwem usługi aliasów), a liczba tych adresów jest nieokreślona i wiadomości nie są automatycznie dystrybuowane przez klienta poczty elektronicznej do większej liczby użytkowników, wymagana jest Licencja na jednego użytkownika komputera. Z jednej Licencji można korzystać każdorazowo tylko na jednym komputerze. Użytkownik końcowy może wprowadzić klucz licencyjny do Oprogramowania tylko w zakresie, w jakim przysługuje mu prawo do korzystania z Oprogramowania zgodnie z ograniczeniami wynikającymi z liczby Licencji przyznanych przez Dostawcę. Klucz licencyjny ma charakter poufny, Licencjobiorca nie może udostępniać Licencji stronom trzecim ani pozwalać im na używanie klucza licencyjnego, o ile nie dopuszcza tego niniejsza Umowa lub Dostawca. W przypadku naruszenia klucza licencyjnego należy bezzwłocznie powiadomić Dostawcę.

c) **Wersja Home/Business Edition.** Wersja Home Oprogramowania jest przeznaczona wyłącznie do używania w środowiskach prywatnych i/lub niekomercyjnych tylko na użytek domowy i rodzinny. W przypadku zamiaru zainstalowania i użycia Oprogramowania w środowisku komercyjnym, na serwerze poczty, w systemie przekazywania wiadomości e-mail lub w połączeniu z bramą pocztową bądź internetową wymagane jest nabycie wersji Business Edition Oprogramowania.

d) **Okres obowiązywania Licencji.** Prawo do korzystania z Oprogramowania jest ograniczone w czasie.

e) **Oprogramowanie dostarczone przez producenta urządzenia (OEM).** Prawo do korzystania z Oprogramowania, które zostało dostarczone przez producenta zakupionego urządzenia (OEM, Original Equipment Manufacturer), jest ograniczone do tego urządzenia. Prawa tego nie można przenosić na inne urządzenia.

f) **Oprogramowanie w wersji próbnej lub nieprzeznaczonej do obrotu handlowego.** Nie można pobierać opłat za korzystanie z Oprogramowania, które jest oznaczone napisem „Not for resale" lub „NFR" (Nie do sprzedaży) albo „TRIAL" (Wersja próbna). Oprogramowanie takie jest przeznaczone wyłącznie do prezentacji lub testowania jego funkcji.

g) **Wygaśnięcie Licencji.** Licencja wygasa automatycznie po upływie okresu jej obowiązywania. Jeśli Licencjobiorca naruszył którekolwiek z postanowień niniejszej Umowy, Dostawca jest uprawniony do rozwiązania niniejszej Umowy oraz do wykonania wszelkich innych praw i zastosowania wszelkich innych środków prawnych przysługujących mu w takiej sytuacji. W razie anulowania Licencji Licencjobiorca musi natychmiast usunąć lub

zniszczyć Oprogramowanie i wszystkie jego kopie zapasowe lub zwrócić je na własny koszt do firmy ESET bądź w miejscu zakupu Oprogramowania. Po wygaśnięciu Licencji Dostawca jest też uprawniony do anulowania prawa Użytkownika końcowego do używania funkcji Oprogramowania, które wymagają połączenia z serwerami Dostawcy lub serwerami innych firm.

4. **Wymagania dotyczące funkcji gromadzących dane i połączenia z Internetem.** Aby Oprogramowanie działało poprawnie, wymagane jest stałe połączenie z Internetem oraz regularne połączenia z serwerami Dostawcy lub z serwerami innych firm, a gromadzenie potrzebnych danych powinno odbywać się zgodnie z obowiązującą Polityką prywatności. Połączenie z Internetem oraz gromadzenie potrzebnych danych są wymagane w przypadku następujących funkcji Oprogramowania:

a) **Aktualizacje Oprogramowania.** Dostawca jest uprawniony do wprowadzania aktualizacji w Oprogramowaniu (w dalszej części nazywanych „Aktualizacjami"), przy czym nie jest zobowiązany do ich wprowadzania. Funkcja Aktualizacji jest domyślnie włączona w ustawieniach standardowych Oprogramowania, dlatego Aktualizacje są instalowane automatycznie, o ile Użytkownik końcowy nie zmienił ustawienia automatycznego instalowania Aktualizacji. W celu przeprowadzania aktualizacji wymagana jest weryfikacja autentyczności Licencji, w tym informacji dotyczących komputera i/lub platformy, na której zostało zainstalowane Oprogramowanie, zgodnie z Polityką Prywatności.

Dostarczanie wszelkich Aktualizacji może podlegać Polityce końca okresu użytkowania ("Polityka EOL"), która jest dostępna na stronie stronie https://go.eset.com/eol_business. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, nie będą dostarczane żadne aktualizacje.

b) **Przekazywanie szkodliwego oprogramowania i informacji o komputerze do Dostawcy**. Oprogramowanie obejmuje funkcje, które gromadzą próbki wirusów komputerowych, innych szkodliwych programów komputerowych oraz podejrzanych, problematycznych, potencjalnie niepożądanych lub niebezpiecznych obiektów, takich jak pliki, adresy URL, pakiety IP oraz ramki Ethernet („Szkodliwe oprogramowanie"), po czym wysyłają je do Dostawcy. Wysyłane dane obejmują m.in. informacje o procesie instalacji, komputerze i/lub platformie, na której zainstalowano Oprogramowanie, a także informacje o działaniu i funkcjonalności Oprogramowania („Informacje"). Informacje oraz Szkodliwe oprogramowanie mogą obejmować dane Użytkownika końcowego (w tym jego dane osobowe pobrane losowo lub przypadkowo) lub dane innych użytkowników komputera, na którym zainstalowano Oprogramowanie, a także pliki uszkodzone przez Szkodliwe oprogramowanie wraz z powiązanymi z nimi metadanymi.

Informacje oraz Szkodliwe oprogramowanie mogą być gromadzone przy użyciu następujących funkcji Oprogramowania:

i. Funkcja systemu reputacji LiveGrid służy do gromadzenia i wysyłania do Dostawcy jednokierunkowych skrótów związanych ze Szkodliwym oprogramowaniem. Funkcję tę można włączyć w ustawieniach standardowych Oprogramowania.

ii. System informacji zwrotnych LiveGrid służy do gromadzenia i wysyłania do Dostawcy Szkodliwego oprogramowania wraz z powiązanymi metadanymi, a także Informacji. Funkcję tę może włączyć Użytkownik końcowy podczas procesu instalacji Oprogramowania.

Dostawca może wykorzystać otrzymane Informacje oraz Szkodliwe oprogramowanie tylko w celu analizy Szkodliwego oprogramowania, usprawnienia Oprogramowania i zweryfikowania autentyczności Licencji i jest zobowiązany do podjęcia stosownych środków gwarantujących zachowanie poufności Szkodliwego oprogramowania i Informacji. Włączenie tej funkcji Oprogramowania oznacza, że Dostawca może gromadzić i przetwarzać Szkodliwe oprogramowanie i Informacje zgodnie z Polityką prywatności i obowiązującymi przepisami prawa. Użytkownik może wyłączyć te funkcje w każdej chwili.

Na potrzeby niniejszej Umowy konieczne jest gromadzenie, przetwarzanie i przechowywanie danych umożliwiających Dostawcy identyfikację Licencjobiorcy zgodnie z Polityką prywatności. Licencjobiorca niniejszym zgadza się, aby Dostawca, korzystając z własnych środków, mógł sprawdzić, czy Licencjobiorca używa Oprogramowania zgodnie z postanowieniami niniejszej Umowy. Licencjobiorca zgadza się, że na potrzeby niniejszej Umowy konieczne jest przekazywanie jego danych podczas komunikacji pomiędzy Oprogramowaniem a systemami komputerowymi Dostawcy lub jego partnerów handlowych w ramach sieci dystrybucyjnej i wsparcia Dostawcy w celu zapewnienia funkcjonalności Oprogramowania i upoważnienia do używania Oprogramowania oraz ochrony praw Dostawcy.

Po zawarciu niniejszej Umowy Dostawca i każdy z jego partnerów handlowych, w ramach sieci dystrybucyjnej i wsparcia Dostawcy, będzie uprawniony do przekazywania, przetwarzania i przechowywania istotnych danych identyfikujących Licencjobiorcę w celach związanych z rozliczaniem opłat, wykonywaniem niniejszej Umowy i przekazywaniem powiadomień na komputerze Licencjobiorcy.

Szczegółowe informacje na temat ochrony prywatności, danych osobowych i praw Licencjobiorcy jako podmiotu danych dostępne są w Polityce prywatności w witrynie Dostawcy, bezpośrednio podczas procesu instalacji. Można do niej przejść także z poziomu sekcji pomocy w Oprogramowaniu.

5. **Wykonywanie praw Użytkownika końcowego**. Licencjobiorca może wykonywać swoje prawa wyłącznie osobiście lub za pośrednictwem swoich pracowników. Licencjobiorca może korzystać z Oprogramowania wyłącznie w celu zapewnienia ciągłości swojej działalności gospodarczej i w celu zabezpieczenia komputerów lub systemów komputerowych, na które uzyskał Licencję.

6. **Ograniczenie praw.** Licencjobiorca nie może kopiować, rozpowszechniać ani wyodrębniać składników Oprogramowania, jak również nie może tworzyć produktów na podstawie Oprogramowania (nie może wykonywać dzieł pochodnych). Korzystając z Oprogramowania, Licencjobiorca musi przestrzegać następujących ograniczeń:

a) Licencjobiorca może wykonać jedną kopię Oprogramowania na nośniku przeznaczonym do trwałego przechowywania danych i przechowywać tę kopię w charakterze archiwalnej kopii zapasowej, tj. nie może zainstalować ani użyć takiej kopii na żadnym komputerze. Wszelkie inne kopie Oprogramowania wykonane przez Licencjobiorcę stanowią naruszenie warunków określonych w niniejszej Umowie.

b) Licencjobiorca nie może używać, modyfikować, tłumaczyć ani odtwarzać Oprogramowania ani jego kopii w sposób inny niż wyszczególniony w niniejszej Umowie.

c) Licencjobiorca nie może sprzedawać Oprogramowania, udzielać na nie podlicencji, oddawać go w użytkowanie, wypożyczać go innym osobom ani pożyczać go od innych osób, a także nie może używać Oprogramowania w celu świadczenia usług o charakterze dochodowym.

d) Licencjobiorca nie może podejmować prób odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji ani w żaden inny sposób, chyba że pozwalają mu na to przepisy, które w stosownym zakresie wyraźnie znoszą niniejsze postanowienie.

e) Licencjobiorca zobowiązuje się używać Oprogramowania w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Oprogramowania ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

f) Licencjobiorca zgadza się korzystać z Oprogramowania i jego funkcji w sposób, który nie ograniczy dostępu do tych usług innym Użytkownikom końcowym. Dostawca zastrzega sobie prawo do ograniczenia zakresu usług udostępnianych konkretnym Użytkownikom końcowym w celu zapewnienia możliwości korzystania z nich jak największej liczbie Użytkowników końcowych. Ograniczenie zakresu usług może również oznaczać całkowitą blokadę funkcji Oprogramowania oraz usunięcie Danych i informacji przechowywanych na serwerach Dostawcy

lub zewnętrznego podmiotu związanych z wybranymi funkcjami Oprogramowania.

g) Licencjobiorca zobowiązuje się nie podejmować działań obejmujących korzystanie z klucza licencyjnego, niezgodnych z postanowieniami niniejszej Umowy lub prowadzących do przekazania klucza licencyjnego osobie nieuprawnionej do korzystania z Oprogramowania, takich jak przekazanie wykorzystanego lub niewykorzystanego klucza licencyjnego w dowolnej formie, a także nieautoryzowana reprodukcja lub dystrybucja zduplikowanych lub wygenerowanych kluczy licencyjnych albo korzystanie z Oprogramowania w wyniku wykorzystania klucza licencyjnego uzyskanego z innego źródła niż Dostawca.

7. **Prawo autorskie**. Oprogramowanie i wszystkie prawa z nim związane, w tym między innymi prawa własności i prawa własności intelektualnej do Oprogramowania, należą do firmy ESET i/lub jej licencjodawców. Prawa te gwarantują zapisy traktatów międzynarodowych oraz wszelkie właściwe przepisy ustawowe obowiązujące w kraju, w którym jest używane Oprogramowanie. Struktura Oprogramowania, sposób jego zorganizowania i kod w nim zawarty są cennymi tajemnicami handlowymi oraz informacjami poufnymi firmy ESET i/lub jej licencjodawców. Licencjobiorca nie może kopiować Oprogramowania poza okolicznościami opisanymi w punkcie 6(a). Wszelkie kopie utworzone przez Licencjobiorcę zgodnie z niniejszą Umową muszą zawierać te same informacje o prawie autorskim i innych prawach własności, które znajdują się w Oprogramowaniu. Licencjobiorca niniejszym przyjmuje do wiadomości, że w razie naruszenia postanowień niniejszej Umowy przez podjęcie próby odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji albo w inny sposób prawa do wszelkich informacji uzyskanych przez Licencjobiorcę w wyniku podjęcia takiej próby zostaną uznane za automatycznie i nieodwołalnie przeniesione w całości na Dostawcę już w momencie powstania takich informacji i to niezależnie od praw przysługujących Dostawcy w związku z naruszeniem przez Licencjobiorcę warunków określonych w niniejszej Umowie.

8. **Zastrzeżenie praw**. Dostawca niniejszym zastrzega sobie wszelkie prawa do Oprogramowania, z wyjątkiem praw wyraźnie udzielonych Licencjobiorcy, występującemu w charakterze Użytkownika końcowego, na podstawie niniejszej Umowy.

9. **Różne wersje językowe, Oprogramowanie obsługujące wiele urządzeń i wiele kopii Oprogramowania**. Jeśli Oprogramowanie może obsługiwać wiele platform lub języków bądź jeśli Licencjobiorca uzyskał wiele kopii Oprogramowania, Oprogramowania można używać tylko na tych systemach komputerowych i w tych wersjach, na które Licencjobiorca uzyskał Licencje. Licencjobiorca nie może sprzedawać wersji ani kopii Oprogramowania, których nie używa, jak również nie może ich oddawać w użytkowanie, udzielać na nie podlicencji, wypożyczać ich ani przenosić do nich praw na inne osoby.

10. **Rozpoczęcie i zakończenie obowiązywania Umowy.** Niniejsza Umowa wchodzi w życie z datą wyrażenia przez Licencjobiorcę zgody na warunki określone w tej Umowie. Licencjobiorca może rozwiązać niniejszą Umowę w dowolnej chwili przez trwałe odinstalowanie i zniszczenie Oprogramowania, wszystkich jego kopii zapasowych i wszelkich powiązanych materiałów dostarczonych przez Dostawcę lub jego partnerów handlowych bądź przez zwrócenie tych produktów na własny koszt. Prawo Licencjobiorcy do korzystania z Oprogramowania i wszelkich jego funkcji może podlegać Polityce EOL. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, prawo Licencjobiorcy do korzystania z Oprogramowania wygaśnie. Bez względu na powód rozwiązania niniejszej Umowy po zakończeniu jej obowiązywania nadal obowiązują postanowienia zawarte w punktach 7, 8, 11, 13, 19 i 21.

11. **OŚWIADCZENIA UŻYTKOWNIKA KOŃCOWEGO**. LICENCJOBIORCA (WYSTĘPUJĄCY W CHARAKTERZE UŻYTKOWNIKA KOŃCOWEGO) PRZYJMUJE OPROGRAMOWANIE W STANIE TAKIM, W JAKIM ZOSTAŁO MU ONO DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA. ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE OPROGRAMOWANIE NIE BĘDZIE NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW

OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA OSOBA NIE GWARANTUJE, ŻE FUNKCJE OPROGRAMOWANIA SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE OPROGRAMOWANIA BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. LICENCJOBIORCA BIERZE NA SIEBIE WSZELKĄ ODPOWIEDZIALNOŚĆ I RYZYKO ZA DOBÓR OPROGRAMOWANIA ODPOWIEDNIEGO DO OSIĄGNIĘCIA CELÓW LICENCJOBIORCY ORAZ ZA PRZEPROWADZENIE INSTALACJI OPROGRAMOWANIA, ZA JEGO UŻYCIE I ZA WYNIKI TEGO UŻYCIA.

12. **Brak innych zobowiązań**. W niniejszej Umowie określono wszystkie zobowiązania Dostawcy i jego licencjodawców.

13. **OGRANICZENIE ODPOWIEDZIALNOŚCI**. O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA, ANI DOSTAWCA, ANI JEGO PRACOWNICY CZY LICENCJODAWCY NIE PONOSZĄ ŻADNEJ ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK UTRATY ZYSKÓW, PRZYCHODÓW, ŹRÓDEŁ PRZYCHODÓW LUB DANYCH, SZKODY MAJĄTKOWE LUB OBRAŻENIA CIAŁA, ZAKŁÓCENIA DZIAŁALNOŚCI PRZEDSIĘBIORSTWA, UTRATY DANYCH HANDLOWYCH CZY JAKIEKOLWIEK SZKODY SZCZEGÓLNE, BEZPOŚREDNIE, POŚREDNIE, UBOCZNE, GOSPODARCZE, MORALNE LUB WYNIKOWE, JAK RÓWNIEŻ NIE BĘDĄ PONOSIĆ KOSZTÓW NABYCIA ZASTĘPCZYCH TOWARÓW LUB USŁUG ANI POKRYWAĆ RÓŻNIC MIĘDZY CENAMI KONTRAKTOWYMI A CENAMI TRANSAKCJI. ZASTRZEŻENIE OKREŚLONE W POWYŻSZYM ZDANIU MA ZASTOSOWANIE BEZ WZGLĘDU NA PRZYCZYNĘ POWSTANIA SZKODY I NA TO, CZY EWENTUALNE ROSZCZENIE ZOSTAŁO ZGŁOSZONE NA PODSTAWIE UMOWY, PRZEPISÓW O CZYNACH NIEDOZWOLONYCH, PRZEPISÓW DOTYCZĄCYCH ZANIEDBAŃ CZY NA JAKIEJKOLWIEK INNEJ PODSTAWIE ORAZ CZY ZOSTAŁO ONO ZGŁOSZONE W ZWIĄZKU Z INSTALACJĄ, UŻYCIEM CZY Z NIEMOŻNOŚCIĄ UŻYCIA OPROGRAMOWANIA. ZASTRZEŻENIE TO MA ZASTOSOWANIE TAKŻE WÓWCZAS, GDY DOSTAWCA LUB JEGO LICENCJODAWCY BĄDŹ PODMIOTY STOWARZYSZONE ZOSTALI POWIADOMIENI O MOŻLIWOŚCI WYSTĄPIENIA DANEJ SZKODY. W PRZYPADKU JURYSDYKCJI, KTÓRE NIE ZEZWALAJĄ NA WYŁĄCZENIE ODPOWIEDZIALNOŚCI ODSZKODOWAWCZEJ, LECZ DOPUSZCZAJĄ JEJ OGRANICZENIE, ODPOWIEDZIALNOŚĆ DOSTAWCY, JEGO PRACOWNIKÓW, LICENCJODAWCÓW LUB PODMIOTÓW STOWARZYSZONYCH JEST OGRANICZONA DO KWOTY ZAPŁACONEJ PRZEZ LICENCJOBIORCĘ ZA LICENCJE.

14. Jeśli którekolwiek postanowienie niniejszej Umowy jest sprzeczne z ustawowymi prawami konsumenckimi jakiejkolwiek osoby, postanowienie to nie może być interpretowane w sposób naruszający te prawa.

15. **Pomoc techniczna**. Usługi pomocy technicznej świadczą wedle własnego uznania i bez udzielania jakichkolwiek gwarancji firma ESET lub inne firmy, którym firma ESET zleca świadczenie takich usług. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, nie będą świadczone żadne usługi pomocy technicznej. Przed skorzystaniem z usługi pomocy technicznej Użytkownik końcowy musi utworzyć kopię zapasową wszystkich istniejących danych, programów i aplikacji. Ani firma ESET, ani inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, nie mogą wziąć na siebie odpowiedzialności za uszkodzenie lub utratę danych, własności, oprogramowania lub urządzeń, jak również nie mogą odpowiadać za utratę zysków spowodowaną świadczeniem usług pomocy technicznej. Firma ESET i/lub inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, zastrzegają sobie prawo do odmowy wykonania usługi, jeśli uznają, że nie mieści się ona w zakresie oferowanych usług pomocy technicznej. Firma ESET zastrzega sobie prawo do odmowy, wstrzymania lub zaprzestania świadczenia usług pomocy technicznej, jeśli uzna to za stosowne. Informacje dotyczące licencji, Informacje i inne dane zgodne z Polityką prywatności mogą być wymagane na potrzeby świadczenia pomocy technicznej.

16. **Przeniesienie Licencji**. Jeśli odpowiednie postanowienia niniejszej Umowy tego nie zabraniają, Oprogramowanie można przenosić między poszczególnymi systemami komputerowymi. O ile nie jest to sprzeczne z warunkami określonymi w niniejszej Umowie, za zgodą Dostawcy Użytkownik końcowy może trwale przenieść Licencję i wszelkie prawa przysługujące mu na podstawie niniejszej Umowy na innego Użytkownika końcowego, pod warunkiem że (i) nie zachowa dla siebie żadnych kopii Oprogramowania; (ii) przeniesienie praw będzie bezpośrednie, tj. prawa zostaną przeniesione bezpośrednio na nowego Użytkownika końcowego; (iii) nowy Użytkownik końcowy przejmie na siebie wszystkie prawa i obowiązki wynikające z niniejszej Umowy, które miały dotąd zastosowanie do Użytkownika końcowego przenoszącego Licencję; (iv) nowy Użytkownik końcowy otrzyma

od Użytkownika końcowego przenoszącego Licencję dokumentację, która umożliwi mu stwierdzenie zgodnie z zapisami w punkcie 17, czy Oprogramowanie jest oryginalne.

17. **Weryfikowanie oryginalności Oprogramowania.** Użytkownik końcowy może wykazać swoje uprawnienia do korzystania z Oprogramowania w jeden z poniższych sposobów: (i) na podstawie certyfikatu licencyjnego wystawionego przez Dostawcę lub inną firmę wskazaną przez Dostawcę; (ii) na podstawie pisemnej umowy licencyjnej, jeśli została ona zawarta; (iii) na podstawie wiadomości e-mail od Dostawcy z danymi dotyczącymi licencji (nazwą użytkownika i hasłem). Informacje dotyczące licencji oraz dane identyfikujące Użytkownika końcowego zgodne z Polityką prywatności mogą być wymagane w celu weryfikacji oryginalności Oprogramowania.

18. **Udzielanie Licencji organom władzy publicznej i rządowi USA**. Organy władzy publicznej, w tym rząd Stanów Zjednoczonych Ameryki Północnej, otrzymują Licencje na Oprogramowanie zgodnie z postanowieniami niniejszej Umowy, tj. z uwzględnieniem wszystkich praw i obowiązków określonych w niniejszej Umowie.

19. **Zgodność z przepisami o kontroli handlu**.

a) Licencjobiorca nie będzie, bezpośrednio ani pośrednio, eksportować, reeksportować, przekazywać lub w inny sposób udostępniać Oprogramowania jakiejkolwiek osobie, nie będzie używać go w jakikolwiek sposób, ani też nie będzie uczestniczyć w jakichkolwiek działaniach, które mogłyby spowodować, że firma ESET lub jej spółki holdingowe, spółki zależne oraz spółki zależne dowolnych z jej spółek holdingowych, jak również podmioty kontrolowane przez jej spółki holdingowe („Podmiotami stowarzyszonymi"), naruszyłyby przepisy o kontroli handlu, obejmujące:

i. wszelkie przepisy prawne, które kontrolują, ograniczają lub nakładają wymogi licencyjne na eksport, reeksport lub transfer towarów, oprogramowania, technologii lub usług, wydane lub przyjęte przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność

ii. wszelkie gospodarcze, finansowe (handlowe lub inne) sankcje, ograniczenia, embarga, zakazy importu lub eksportu, zakazy przekazywania funduszy lub aktywów bądź świadczenia usług, lub też równoważne środki nałożone przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność.

(Akty prawne, o których mowa w pkt i i ii powyżej, łącznie nazywane są „Przepisami dotyczącymi kontroli handlu").

b) Firma ESET ma prawo zawiesić swoje zobowiązania wynikające z niniejszych warunków lub wypowiedzieć je ze skutkiem natychmiastowym w następujących przypadkach:

i. Gdy firma ESET stwierdzi na podstawie stosownego uzasadnienia, że Użytkownik naruszył lub może naruszyć postanowienia punktu 19 a) Umowy.

ii. Gdy Użytkownik końcowy i/lub Oprogramowanie podlegają przepisom o kontroli handlu i w związku z tym firma ESET stwierdzi na podstawie stosownego uzasadnienia, że dalsze wykonywanie zobowiązań wynikających z Umowy mogłoby spowodować, że firma ESET lub jej Podmioty stowarzyszone naruszyłyby przepisy o kontroli handlu lub byłyby narażone na negatywne konsekwencje wynikające z tych przepisów.

c) Żadne z postanowień Umowy nie ma na celu ani nie powinno być interpretowane lub odczytywane jako

nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

20. **Zawiadomienia**. Wszystkie zawiadomienia oraz zwroty Oprogramowania i Dokumentacji należy kierować na adres: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez uszczerbku dla praw firmy ESET do komunikowania użytkownikowi wszelkich zmian w niniejszej Umowie, Polityce Prywatności, Polityce EOL oraz Dokumentacji zgodnie z punktem 22 niniejszej Umowy. Firma ESET może wysyłać wiadomości e-mail, powiadomienia w aplikacji za pośrednictwem Oprogramowania lub poprzez publikację komunikatów na naszej stronie internetowej. Użytkownik wyraża zgodę na otrzymywanie od firmy ESET informacji prawnych w formie elektronicznej, w tym wszelkich komunikatów dotyczących zmian Warunków, Warunków szczególnych lub Polityki Prywatności, wszelkich propozycji/akceptacji umowy lub zaproszeń do pertraktacji, powiadomień lub innych komunikatów prawnych. Taką komunikację elektroniczną uznaje się za otrzymaną na piśmie, chyba że obowiązujące przepisy prawa wyraźnie wymagają innej formy komunikacji.

21. **Prawo właściwe**. Niniejsza Umowa podlega przepisom prawnym obowiązującym w Słowacji i powinna być interpretowana zgodnie z tymi przepisami. Użytkownik końcowy i Dostawca niniejszym stwierdzają, że do niniejszej Umowy nie mają zastosowania przepisy dotyczące konfliktu praw ani Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów. Licencjobiorca wyraźnie stwierdza, że wszelkie spory lub roszczenia względem Dostawcy wynikające z zawarcia niniejszej Umowy, jak również wszelkie spory lub roszczenia związane z użyciem Oprogramowania będą rozstrzygane przez Sąd Rejonowy dla okręgu Bratislava I. Licencjobiorca wyraźnie poddaje się jurysdykcji tego sądu.

22. **Postanowienia ogólne**. Uznanie któregokolwiek z postanowień niniejszej Umowy za nieważne lub niewykonalne nie wpływa na ważność innych postanowień niniejszej Umowy, które pozostają wówczas w mocy zgodnie z warunkami określonymi w niniejszej Umowie. Niniejsza Umowa została zawarta w języku angielskim. W przypadku sporządzenia tłumaczenia niniejszej Umowy dla wygody lub do innych celów oraz w przypadku rozbieżności pomiędzy wersjami językowymi niniejszej Umowy pierwszeństwo ma wersja angielska.

Firma ESET zastrzega sobie prawo do wprowadzania zmian w Oprogramowaniu oraz modyfikowania warunków niniejszej Umowy, Aneksów, Załączników, Polityki Prywatności, Polityki EOL oraz Dokumentacji lub dowolnej ich części w dowolnym czasie poprzez aktualizowanie odpowiednich dokumentów (i) w celu odzwierciedlenia zmian wprowadzonych w zakresie Oprogramowania oraz w sposobie prowadzenia działalności przez firmę ESET, (ii) ze względów prawnych, regulacyjnych lub bezpieczeństwa lub (iii) w celu zapobiegania nadużyciom lub szkodom. Licencjobiorca zostanie powiadomiony o wszelkich zmianach w niniejszej Umowie za pośrednictwem poczty e-mail, powiadomienia w aplikacji lub innych kanałów komunikacji elektronicznej. Jeśli Licencjobiorca nie zgadza się z proponowanymi zmianami w Umowie, może ją rozwiązać zgodnie z punktem 10 w ciągu 30 dni od otrzymania powiadomienia o zmianie. O ile Licencjobiorca nie wypowie Umowy w tym terminie, proponowane zmiany zostaną uznane za zaakceptowane i wejdą w życie wobec Licencjobiorcy od dnia otrzymania powiadomienia o zmianie.

Niniejsza Umowa stanowi całość porozumienia między Dostawcą a Licencjobiorcą w sprawie Oprogramowania i zastępuje wszelkie wcześniejsze oświadczenia, negocjacje, zobowiązania, wymiany zdań lub reklamy związane z Oprogramowaniem.

EULAID: EULA-PRODUCT-LG-MAC; 3537.0

Polityka prywatności

Firma ESET, spol. s r. o., z siedzibą pod adresem Einsteinova 24, 851 01 Bratysława, Słowacja, zarejestrowana w Rejestrze Handlowym prowadzonym przez Sąd Rejonowy dla okręgu Bratislava I, w sekcji Sro pod numerem

3586/B, numer w rejestrze przedsiębiorców: 31333532, jako administrator danych (dalej „ESET” lub „my”) pragnie zachować przejrzystość w kwestii przetwarzania danych osobowych oraz zachowania poufności informacji swoich klientów. W związku z tym publikujemy niniejsze Zasady ochrony prywatności wyłącznie w celu przekazania klientowi (dalej „Użytkownik końcowy” lub „Ty”) informacji na następujące tematy:

- przetwarzanie danych osobowych,
- poufność danych,
- prawa osób, których dane dotyczą.

przetwarzanie danych osobowych.

Usługi zaimplementowane w produkcie firmy ESET są przez nas świadczone zgodnie z postanowieniami Umowy licencyjnej użytkownika końcowego („Umowa EULA”), ale niektóre z nich mogą wymagać szczególnej uwagi. Chcemy przekazać szczegółowe informacje na temat gromadzenia danych związanych ze świadczonymi przez nas usługami. Oferujemy szereg usług przedstawionych w umowie EULA i dokumentacji produktu, takich jak aktualizacja/uaktualnianie, ESET LiveGrid®, ochrona przed niewłaściwym użyciem danych, pomoc techniczna itp. Abyśmy mogli dostarczać nasze usługi, musimy gromadzić następujące informacje:

- Statystyki (dotyczące aktualizacji i inne) obejmujące informacje na temat procesu instalacji oraz komputera użytkownika końcowego (np. platformy, na której jest zainstalowany nasz produkt), a także informacje o działaniu i funkcjach naszych produktów, takie jak system operacyjny, dane dotyczące sprzętu, identyfikatory instalacji, identyfikatory licencji, adres IP, adres MAC oraz ustawienia konfiguracji produktu.
- Skróty jednokierunkowe związane z infekcjami używane przez system reputacji ESET LiveGrid®, które poprawiają wydajność naszych rozwiązań do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.
- Próbki podejrzanego kodu i metadanych używane przez system reputacji ESET LiveGrid®, które pozwalają produktom ESET reagować natychmiast na potrzeby użytkowników końcowych i zapewnić ochronę przed najnowszymi zagrożeniami. Korzystamy następujących danych otrzymanych od użytkowników końcowych
  - dane dotyczące infekcji, takie jak próbki potencjalnych wirusów i innych szkodliwych programów, a także podejrzane, potencjalnie niepożądane i potencjalnie niebezpieczne obiekty (np. pliki wykonywalne i wiadomości e-mail zgłoszone jako spam lub oznaczone przez nasz produkt);
  - informacje o urządzeniach w sieci lokalnej, takie jak typ, producent, model i/lub nazwa urządzenia;
  - informacje dotyczące korzystania z Internetu, takie jak adres IP, informacje geograficzne, pakiety IP, adresy URL i ramki sieci Ethernet;
  - pliki zrzutu awaryjnego i informacje w nich zawarte.

Nie mamy zamiaru gromadzić danych spoza tego zakresu, jednak czasami nie da się tego uniknąć. Przypadkowo zebrane dane mogą być zawarte w samym szkodliwym oprogramowaniu (i zebrane bez wiedzy i zgody użytkownika końcowego) lub mogą stanowić część nazwy pliku lub adresu URL. Nie zamierzamy wykorzystywać tych danych w naszych systemach ani przetwarzać ich w celu określonym w tej Polityce prywatności.

- Informacje dotyczące licencji, takie jak identyfikator licencji oraz dane osobowe, takie jak imię, nazwisko, adres oraz adres e-mail, są wymagane do celów związanych z rozliczeniami, weryfikacją autentyczności licencji oraz świadczeniem przez nas usług.
- Aby zapewnić możliwość świadczenia pomocy technicznej lub pomocy innego rodzaju mogą być wymagane

informacje kontaktowe i dane zawarte w zgłoszeniach do działu pomocy. W zależności od wybranego przez Użytkownika końcowego sposobu komunikacji możemy gromadzić następujące dane: adres e-mail, numer telefonu, informacje o licencji, szczegółowe informacje o produkcie oraz opis zgłoszenia do pomocy technicznej. Możemy poprosić o podanie innych informacji, aby ułatwić świadczenie usługi pomocy technicznej.

Poufność danych

ESET jest firmą działającą na całym świecie za pośrednictwem swoich spółek stowarzyszonych oraz partnerów będących częścią sieci dystrybucji, usług i pomocy technicznej. Przetwarzane przez nas informacje mogą być przesyłane między nami a naszymi partnerami oraz spółkami stowarzyszonymi z tytułu realizacji Umowy EULA, na przykład świadczenia usług lub udzielania pomocy technicznej albo w celach rozliczeniowych. W zależności od lokalizacji Użytkownika końcowego i wybranych przez niego usług możemy być zmuszeni do wysyłania jego danych do kraju, który nie uzyskał decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony. Każdorazowo proces ten przebiega zgodnie z przepisami o ochronie danych i odbywa się wyłącznie w razie konieczności. W każdym przypadku, bez wyjątków, muszą być ustanowione standardowe klauzule umowne, wiążące reguły korporacyjne lub inne odpowiednie zabezpieczenia.

Dokładamy wszelkich starań, aby nie dopuścić do przechowywania danych dłużej, niż jest to konieczne w związku ze sprzedażą usług na mocy umowy EULA. Okres przechowywania przez nas danych może być dłuższy niż okres ważność licencji użytkownika. Ma to umożliwić użytkownikowi łatwe i wygodne odnowienie licencji. Statystyki i inne dane zgromadzone przez usługę ESET LiveGrid® (w postaci zminimalizowanej i pseudonimizowanej) mogą być nadal przetwarzane w celach statystycznych.

Firma ESET stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu zabezpieczeń odpowiedniego do zagrożeń. Dokładamy wszelkich starań, aby zapewnić ciągłą poufność, integralność, dostępność i odporność przetwarzanych systemów i usług. W przypadku naruszenia ochrony danych zagrażającego prawom i wolnościom Użytkownika końcowego jesteśmy jednak gotowi do powiadomienia o tym fakcie organów nadzorczych oraz właścicieli danych. Jako osoba, której dane dotyczą, użytkownik ma prawo do wniesienia skargi do organu nadzorczego.

Prawa osób, których dane dotyczą

Firma ESET podlega prawu słowackiemu i obowiązują ją przepisy Unii Europejskiej o ochronie danych. Zgodnie z warunkami zapisanymi w obowiązujących przepisach dotyczących ochrony danych osobowych, każdemu właścicielowi danych przysługują następujące prawa:

- prawo do uzyskania wglądu w swoje dane osobowe gromadzone przez firmę ESET;
- prawo do wprowadzenia zmian w swoich danych osobowych, jeśli są nieprawidłowe (Użytkownik końcowy ma także prawo do uzupełnienia niekompletnych danych osobowych);
- prawo do usunięcia swoich danych osobowych;
- prawo do ograniczenia zakresu przetwarzania swoich danych osobowych;
- prawo do niewyrażenia zgody na przetwarzanie danych;
- prawo do wniesienia skargi;
- prawo do przeniesienia danych.

Jeżeli użytkownik chce skorzystać z prawa przysługującego mu jako osobie, której dane dotyczą, a także w przypadku pytań lub wątpliwości, użytkownik może przesłać do nas wiadomość na adres:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk