ESET Cyber Security

Podręcznik użytkownika

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Digital Security
Progress. Protected.

Produkt ESET Cyber Security 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 Cyber Security

Program ESET Cyber Security jest implementacją nowego podejścia do pełni zintegrowanej ochrony komputera. Najnowsza wersja aparatu skanowania ThreatSense® działa szybko i dokładnie oraz utrzymuje najwyższy poziom bezpieczeństwa komputera. Użytkownik ma do dyspozycji inteligentny system stale broniący komputer przed atakami i szkodliwymi aplikacjami.

Program ESET Cyber Security jest kompletnym oprogramowaniem zabezpieczającym opracowanym dzięki naszym długotrwałym wysiłkom mającym na celu połączenie maksymalnej ochrony i minimalnego wpływu na pracę komputera. Oparte na sztucznej inteligencji zaawansowane technologie wchodzące w skład programu ESET Cyber Security potrafią z wyprzedzeniem eliminować infekcje, takie jak wirusy, robaki, konie trojańskie, spyware, adware, programy typu rootkit i pozostałe pochodzące z internetu ataki, a równocześnie mają niewielki wpływ na wydajność i pracę komputera.

Nowe funkcje w wersji 6

W wersji 6 programu ESET Cyber Security wprowadzono następujące aktualizacje i usprawnienia:

- **Obsługa architektury 64-bitowej**
- **Ochrona przed atakami typu „phishing”**— zapobiega pozyskiwaniu danych osobowych użytkownika za pośrednictwem fałszywych stron internetowych podszywających się pod strony godne zaufania.
- **Aktualizacje systemu**— program ESET Cyber Security w wersji 6 zawiera różne poprawki i usprawnienia, w tym powiadomienia dotyczące aktualizacji systemu operacyjnego. Więcej informacji na ten temat można znaleźć w sekcji Aktualizacje systemu.
- **Stany ochrony**— możliwość ukrywania powiadomień (np. *Ochrona programów poczty e-mail wyłączona* lub *Wymagane jest ponowne uruchomienie komputera*) w oknie Stan ochrony.
- **Skanowane nośniki**— nośniki określonego typu mogą być wyłączone ze skanowania w czasie rzeczywistym (Dyski lokalne, Nośniki wymienne, Nośniki sieciowe).
- **Połączenia sieciowe**— wyświetla połączenia sieciowe na komputerze i umożliwia tworzenie reguł do tych połączeń.

Dodatkowe informacje na temat nowych funkcji w programie ESET Cyber Security znajdują się w przedstawionym poniżej artykule bazy danych firmy ESET:

Wymagania systemowe

Aby zapewnić optymalne działanie programu ESET Cyber Security, komputer powinien spełniać następujące wymagania dotyczące sprzętu i oprogramowania:

	Wymagania systemowe:
Architektura procesora	Intel 64-bit, M1, M2
System operacyjny	macOS 10.12 lub nowszy
Pamięć	300 MB

Wolne miejsce na dysku	200 MB

Oprócz wsparcia dla procesorów Intel, produkt ESET Cyber Security w wersji 6.10.900.0 i nowszej posiada wsparcie dla czipów Apple M1 i M2 z wykorzystaniem rozwiązania Rosetta 2

Instalacja

Przed rozpoczęciem procesu instalacji zamknij wszystkie otwarte programy. Program ESET Cyber Security zawiera komponenty, które mogą wchodzić w konflikt z innymi programami antywirusowymi zainstalowanymi na komputerze. Firma ESET zdecydowanie zaleca usunięcie innych programów antywirusowych w celu uniknięcia potencjalnych problemów.

Aby uruchomić kreatora instalacji, wykonaj jeden z następujących kroków:

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

Kreator instalacji przeprowadzi użytkownika przez podstawowe kroki konfiguracji. Na początku instalacji program instalacyjny automatycznie sprawdzi przez Internet dostępność najnowszej wersji produktu. Jeżeli będzie dostępna nowsza wersja, przed przystąpieniem do procesu instalacji zostanie wyświetlona opcja jej pobrania.

Po zaakceptowaniu Umowy licencyjnej użytkownika końcowego można wybrać jeden z następujących trybów instalacji:

- Instalacja typowa
- Instalacja zaawansowana

Instalacja typowa

Tryb instalacji typowej obejmuje opcje konfiguracyjne odpowiednie dla większości użytkowników. Ustawienia te stanowią najlepszy kompromis między maksymalnym bezpieczeństwem a najwyższą wydajnością. Instalacja typowa jest wybierana domyślnie i zaleca się ją w przypadku braku specjalnych wymagań w kwestii określonych ustawień.

1.W oknie **ESET LiveGrid** wybierz preferowaną opcję i kliknij przycisk **Kontynuuj**. Jeśli później zdecydujesz, że chcesz zmienić to ustawienie, będzie można to zrobić za pomocą **konfiguracji LiveGrid**. Aby uzyskać więcej informacji na temat usługi ESET LiveGrid®, odwiedź nasz słowniczek.
2.W oknie **Potencjalnie niepożądane aplikacje** wybierz preferowaną opcję (zobacz Co to jest potencjalnie niepożądana aplikacja?) i kliknij przycisk **Kontynuuj**. Jeśli później zdecydujesz, że chcesz zmienić to ustawienie, użyj **Ustawień zaawansowanych**.
3.Kliknij pozycję **Zainstaluj**. Jeśli zostanie wyświetlony monit o wprowadzenie hasła do systemu macOS, wprowadź je i kliknij przycisk **Zainstaluj oprogramowanie**.

Po zainstalowaniu produktu ESET Cyber Security:

macOS Big Sur (11)

1.Zezwól na rozszerzenia systemu.

2.Zezwalanie na pełny dostęp do dysku.

3.Zezwól programowi ESET na dodawanie konfiguracji serwerów proxy. Otrzymasz następujące powiadomienie: **"**ESET Cyber Security**" chce dodawać konfiguracje proxy**. Po otrzymaniu tego powiadomienia kliknij przycisk **Zezwól**. Jeśli klikniesz przycisk **Nie zezwalaj**, ochrona dostępu do stron internetowych nie będzie działać.

macOS 10.15 i starsze

1.W systemie macOS 10.13 lub nowszym zostanie wyświetlone systemowe powiadomienie **Rozszerzenie systemu zablokowane** oraz powiadomienie **Komputer nie jest chroniony** z programu ESET Cyber Security. Aby uzyskać dostęp do wszystkich funkcji programu ESET Cyber Security, należy zezwolić na rozszerzenia jądra na urządzeniu. Aby zezwolić na rozszerzenia jądra na urządzeniu, przejdź do pozycji **Preferencje systemowe** > **Zabezpieczenia i prywatność**, a następnie kliknij pozycję **Zezwól**, aby zezwolić na oprogramowanie systemowe producenta **ESET, spol. s.r.o.** Aby uzyskać więcej szczegółowych informacji, przeczytaj artykuł z Bazy wiedzy.

2.W systemie macOS 10.14 lub nowszym zostanie wyświetlone powiadomienie **Komputer jest częściowo chroniony** z ESET Cyber Security. Aby uzyskać dostęp do wszystkich funkcji programu ESET Cyber Security, zezwól na **Pełny dostęp do dysku** programowi ESET Cyber Security. Kliknij pozycję **Otwórz preferencje systemowe** > **Bezpieczeństwo i prywatność**. Przejdź do karty **Prywatność** i wybierz opcję **Pełny dostęp do dysku**. Kliknij ikonę kłódki, aby umożliwić edycję. Kliknij ikonę plusa i wybierz aplikację ESET Cyber Security. Komputer wyświetli monit o ponowne uruchomienie. Kliknij pozycję **Później**. Nie uruchamiaj jeszcze ponownie komputera. Kliknij **Uruchom ponownie** w oknie powiadomienia programu ESET Cyber Security lub uruchom ponownie komputer. Aby uzyskać więcej szczegółowych informacji, przeczytaj artykuł z Bazy wiedzy.

Po zainstalowaniu programu ESET Cyber Security należy przeskanować komputer w poszukiwaniu szkodliwego

kodu. W głównym menu programu należy kliknąć kolejno opcje **Skanowanie komputera** > **Skanowanie inteligentne**. Więcej informacji o skanowaniu komputera na żądanie można znaleźć w sekcji Skanowanie komputera na żądanie.

Instalacja zaawansowana

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

- **Serwer proxy**

Jeżeli używasz serwera proxy, zaznacz opcję **Korzystam z serwera proxy** i określ jego ustawienia. W następnym oknie w polu **Adres** wpisz adres IP lub URL serwera proxy. W polu **Port** wprowadź numer portu, na którym serwer proxy przyjmuje połączenia (domyślnie 3128). Jeżeli serwer proxy wymaga uwierzytelniania, w polach **Nazwa użytkownika** i **Hasło** podaj prawidłowe dane umożliwiające dostęp do serwera. Jeśli serwer proxy nie jest używany, należy wybrać opcję **Nie korzystam z serwera proxy**. Jeżeli nie masz pewności, czy używasz serwera proxy, wybierz pozycję **Użyj ustawień systemowych (zalecane)**, aby użyć bieżących ustawień systemu.

- **Uprawnienia**

Można zdefiniować uprzywilejowanych użytkowników lub grupy z uprawnieniami do edytowania konfiguracji programu. Należy wybrać użytkowników z listy po lewej, a następnie **dodać** ich do listy **Użytkownicy uprzywilejowani**. Aby wyświetlić wszystkich użytkowników systemu, należy wybrać opcję **Pokaż wszystkich użytkowników**. Jeśli lista Użytkownicy uprzywilejowani pozostanie pusta, wszyscy użytkownicy będą uznani za uprzywilejowanych.

- **ESET LiveGrid®**

Aby uzyskać więcej informacji na temat usługi ESET LiveGrid, odwiedź nasz słowniczek.

- **Potencjalnie niepożądane aplikacje**

Aby uzyskać więcej informacji na temat potencjalnie niepożądanych aplikacji, odwiedź nasz słowniczek.

Po zainstalowaniu produktu ESET Cyber Security:

macOS Big Sur (11)

1. Zezwól na rozszerzenia systemu.
2. Zezwalanie na pełny dostęp do dysku.
3. Zezwól programowi ESET na dodawanie konfiguracji serwerów proxy. Otrzymasz następujące powiadomienie: **"**ESET Cyber Security**" chce dodawać konfiguracje proxy**. Po otrzymaniu tego powiadomienia kliknij przycisk **Zezwól**. Jeśli klikniesz przycisk **Nie zezwalaj**, ochrona dostępu do stron internetowych nie będzie działać.

macOS 10.15 i starsze

1. W systemie macOS 10.13 lub nowszym zostanie wyświetlone systemowe powiadomienie **Rozszerzenie systemu zablokowane** oraz powiadomienie **Komputer nie jest chroniony** z programu ESET Cyber Security. Aby uzyskać dostęp do wszystkich funkcji programu ESET Cyber Security, należy zezwolić na rozszerzenia jądra na urządzeniu. Aby zezwolić na rozszerzenia jądra na urządzeniu, przejdź do pozycji **Preferencje systemowe** > **Zabezpieczenia i prywatność**, a następnie kliknij pozycję **Zezwól**, aby zezwolić na oprogramowanie systemowe producenta **ESET, spol. s.r.o.** Aby uzyskać więcej szczegółowych informacji, przeczytaj artykuł z Bazy wiedzy.

2.W systemie macOS 10.14 lub nowszym zostanie wyświetlone powiadomienie **Komputer jest częściowo chroniony** z ESET Cyber Security. Aby uzyskać dostęp do wszystkich funkcji programu ESET Cyber Security, zezwól na **Pełny dostęp do dysku** programowi ESET Cyber Security. Kliknij pozycję **Otwórz preferencje systemowe** > **Bezpieczeństwo i prywatność**. Przejdź do karty **Prywatność** i wybierz opcję **Pełny dostęp do dysku**. Kliknij ikonę kłódki, aby umożliwić edycję. Kliknij ikonę plusa i wybierz aplikację ESET Cyber Security. Komputer wyświetli monit o ponowne uruchomienie. Kliknij pozycję **Później**. Nie uruchamiaj jeszcze ponownie komputera. Kliknij **Uruchom ponownie** w oknie powiadomienia programu ESET Cyber Security lub uruchom ponownie komputer. Aby uzyskać więcej szczegółowych informacji, przeczytaj artykuł z Bazy wiedzy.

Po zainstalowaniu programu ESET Cyber Security należy przeskanować komputer w poszukiwaniu szkodliwego kodu. W głównym menu programu należy kliknąć kolejno opcje **Skanowanie komputera** > **Skanowanie inteligentne**. Więcej informacji o skanowaniu komputera na żądanie można znaleźć w sekcji Skanowanie komputera na żądanie.

Zezwól na rozszerzenia systemu

W systemie macOS 11 (Big Sur) rozszerzenia jądra zostały zastąpione rozszerzeniami systemu. Wymagają one zatwierdzenia przez użytkownika przed załadowaniem nowych rozszerzeń systemu innych firm.

Po instalacji w systemie macOS 11 lub nowszym produktu ESET Cyber Security zostanie wyświetlone systemowe powiadomienie Rozszerzenie systemu zablokowane oraz powiadomienie Komputer nie jest chroniony z programu ESET Cyber Security. Aby uzyskać dostęp do wszystkich funkcji programu ESET Cyber Security, należy zezwolić na rozszerzenia systemu na urządzeniu.

Uaktualnienie z poprzedniego systemu macOS do Big Sur.
Jeśli masz już zainstalowany produkt ESET Cyber Security i zamierzasz przeprowadzić aktualizację systemu do macOS Big Sur, musisz zezwolić na rozszerzenia jądra ESET ręcznie po uaktualnieniu. Wymagany jest fizyczny dostęp do komputera klienckiego — podczas zdalnego uzyskiwania dostępu przycisk Zezwól jest wyłączony.

Podczas instalowania produktu ESET w systemie macOS Big Sur lub nowszym należy zezwolić na rozszerzenia systemu ESET ręcznie. Wymagany jest fizyczny dostęp do komputera klienckiego — podczas zdalnego uzyskiwania dostępu ta opcja jest wyłączona.

Zezwól na rozszerzenia systemu ręcznie

1.W jednym z okien dialogowych alertów kliknij pozycję **Otwórz preferencje systemowe** lub **Otwórz preferencje zabezpieczeń.**

2.Kliknij ikonę kłódki w lewym dolnym rogu, aby zezwolić na zmiany w oknie ustawień.

3.Użyj czytnika Touch ID lub kliknij pozycję **Użyj hasła** i wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **Odblokuj**.

4.Kliknij pozycję **Szczegóły**.

5.Wybierz obie opcje ESET Cyber Security**.app.**

6.Kliknij **OK**.

Aby uzyskać szczegółowe wytyczne krok po kroku, odwiedź nasz artykuł bazy wiedzy. (Artykuły bazy wiedzy nie są dostępne we wszystkich językach).

Zezwalanie na pełny dostęp do dysku

W systemie macOS 10.14 wyświetli się powiadomienie **Komputer jest częściowo chroniony** z programu ESET Cyber Security. Aby uzyskać dostęp do wszystkich funkcji ESET Cyber Security, zezwól programowi ESET Cyber Security na **Pełny dostęp do dysku**.

1. W oknie dialogowym alertów kliknij pozycję **Otwórz preferencje systemowe.**
2. Kliknij ikonę kłódki w lewym dolnym rogu, aby zezwolić na zmiany w oknie ustawień.
3. Użyj czytnika Touch ID lub kliknij pozycję **Użyj hasła** i wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **Odblokuj**.
4. Wybierz z listy pozycję ESET Cyber Security**.app**.
5. Zostanie wyświetlone powiadomienie o ponownym uruchomieniu ESET Cyber Security. Kliknij przycisk Później.
6. Z listy wybierz pozycję **Ochrona systemu plików w czasie rzeczywistym ESET**.

> **Ochrona systemu plików w czasie rzeczywistym ESET nie jest dostępna**
> Jeśli na liście nie ma opcji **Ochrony systemu plików w czasie rzeczywistym**, należy zezwolić na rozszerzenia systemu dla produktu ESET.

7. Kliknij przycisk Uruchom ponownie w oknie dialogowym alertu ESET Cyber Security lub uruchom ponownie komputer. Aby uzyskać bardziej szczegółowe informacje, odwiedź nasz artykuł bazy wiedzy.

Aktywacja produktu

Okno Aktywacja produktu jest automatycznie wyświetlane po zakończeniu instalacji. Aby uzyskać do niego dostęp w dowolnej chwili, kliknij ikonę ESET Cyber Security znajdującą się na pasku menu systemu macOS (u góry ekranu), a następnie kliknij opcję **Aktywacja produktu**.

- **Klucz licencyjny** — niepowtarzalny ciąg znaków w formacie XXXX-XXXX-XXXX-XXXX-XXXX lub XXXX-XXXXXXXX służący do identyfikacji właściciela licencji oraz do aktywacji licencji. Przy użyciu klucza licencyjnego należy aktywować program kupiony w pudełkowej wersji detalicznej. Klucz ten znajduje się zazwyczaj wewnątrz lub na tylnej stronie opakowania produktu.
- **Nazwa użytkownika i hasło** — jeżeli masz nazwę użytkownika i hasło, ale nie wiesz, w jaki sposób aktywować program ESET Cyber Security, kliknij opcję **Mam nazwę użytkownika i hasło. Co muszę zrobić?**. Zostanie otwarty portal my.eset.com, w którym można skonwertować poświadczenia na klucz licencyjny.
- **Bezpłatna licencja próbna** — wybierz tę opcję, aby wypróbować program ESET Cyber Security przed jego kupnem. Aby tymczasowo aktywować program ESET Cyber Security, wpisz adres e-mail. Dane licencji testowej otrzymasz w wiadomości e-mail. Każdy klient może aktywować licencję tymczasową tylko raz.
- **Kup licencję** — jeżeli nie masz licencji i chcesz ją nabyć, kliknij pozycję Kup licencję. Spowoduje to przekierowanie do witryny lokalnego dystrybutora firmy ESET.

- **Aktywuj później** — kliknij tę opcję, jeśli nie chcesz aktywować programu teraz.

Odinstalowanie

Aby odinstalować program ESET Cyber Security, należy wykonać jedną z tych procedur:

- Włożenie płyty instalacyjnej CD/DVD programu ESET Cyber Security do napędu komputera i otwarcie jej z poziomu biurka lub okna programu **Finder** i dwukrotne kliknięcie opcji **Odinstaluj**
- Otwarcie pliku instalacyjnego programu ESET Cyber Security (*.dmg*) i dwukrotne kliknięcie opcji **Odinstaluj**
- Uruchomienie programu **Finder**, otwarcie folderu **Applications** (Aplikacje) na dysku twardym, kliknięcie z wciśniętym klawiszem CTRL ikony **ESET Cyber Security** i wybranie opcji **Show Package Contents** (Pokaż zawartość pakietu). Otwarcie folderu **Contents** > **Helpers** i dwukrotne kliknięcie ikony **Uninstaller**.

Podstawowe informacje

Główne okno programu ESET Cyber Security jest podzielone na dwie podstawowe części. W głównym oknie z prawej strony są wyświetlane informacje dotyczące opcji zaznaczonej w menu głównym z lewej strony.

W menu głównym dostępne są te sekcje:

- **Ekran główny**— zawiera informacje o stanie ochrony komputera oraz stron internetowych i poczty.
- **Skanowanie komputera**— służy do konfigurowania i uruchamiania funkcji Skanowanie komputera na żądanie.
- **Aktualizacja**— wyświetla informacje o aktualizacji modułów wykrywania.
- **Ustawienia**— ta sekcja umożliwia dostosowanie poziomu zabezpieczeń komputera.
- **Narzędzia** — zapewnia dostęp do modułów Pliki dziennika, Harmonogram, Kwarantanna, Uruchomione procesy i innych funkcji programu.
- **Pomoc** — zapewnia dostęp do plików pomocy, internetowej bazy wiedzy, formularza internetowego służącego do kontaktu z pomocą techniczną oraz do innych dodatkowych informacji.

Skróty klawiszowe

Skróty klawiszowe dostępne w programie ESET Cyber Security:

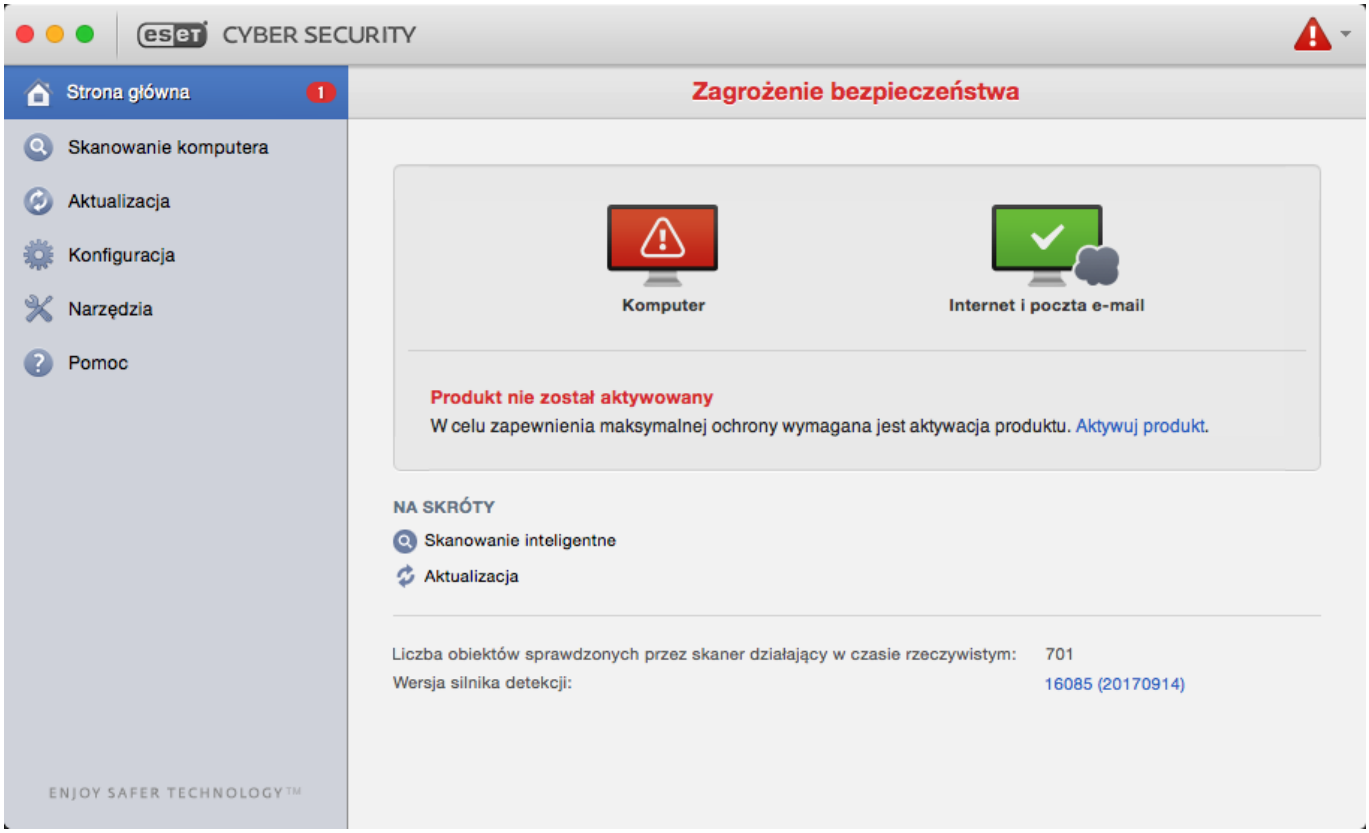
- cmd+, — wyświetla preferencje programu ESET Cyber Security.
- cmd+O — przywraca domyślny rozmiar głównego okna interfejsu graficznego programu ESET Cyber Security i umieszcza to okno na środku ekranu.
- cmd+Q — ukrywa główne okno interfejsu graficznego programu ESET Cyber Security. Można je otworzyć, klikając ikonę programu ESET Cyber Security na pasku menu systemu macOS (u góry ekranu).
- cmd+W — zamyka główne okno interfejsu graficznego programu ESET Cyber Security.

Następujące skróty klawiszowe działają tylko wówczas, gdy włączona jest opcja **Użyj standardowego menu** w sekcji **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Interfejs**:

- cmd+alt+L — otwiera sekcję Pliki dziennika.
- cmd+alt+S — otwiera sekcję Harmonogram.
- cmd+alt+Q — otwiera sekcję Kwarantanna.

Sprawdzanie stanu ochrony

Aby sprawdzić stan ochrony, w menu głównym należy kliknąć opcję **Strona główna**. W oknie głównym zostanie wyświetlone podsumowanie informacji o działaniu modułów programu ESET Cyber Security.



Postępowanie w przypadku, gdy program nie działa poprawnie

Gdy moduł działa prawidłowo, wyświetlana jest zielona ikona. Gdy moduł nie działa prawidłowo, wyświetlany jest czerwony wykrzyknik lub pomarańczowa ikona powiadomienia. Pojawią się także dodatkowe informacje o module oraz proponowane rozwiązanie problemu. Aby zmienić stan poszczególnych modułów, należy kliknąć niebieskie łącze pod każdym powiadomieniem.

Jeśli nie uda rozwiązać się problemu przy użyciu proponowanego rozwiązania, można wyszukać inne rozwiązanie w bazie wiedzy firmy ESET lub skontaktować się z działem obsługi klienta firmy ESET. Dział obsługi klienta firmy ESET udzieli szybkiej odpowiedzi na pytania i pomoże w znalezieniu rozwiązania problemów dotyczących programu ESET Cyber Security.

Ochrona komputera

Konfiguracja komputera znajduje się w menu **Ustawienia** > **Komputer**. Pokazuje ona stan ustawień **Ochrona systemu plików w czasie rzeczywistym** oraz **Blokowanie nośników wymiennych**. Aby wyłączyć poszczególne moduły, należy przełączyć odpowiadające im przyciski na ustawienie **WYŁĄCZONA**. Należy pamiętać, że może to obniżyć poziom ochrony komputera. Aby przejść do szczegółowych ustawień każdego modułu, należy kliknąć przycisk **Ustawienia...**.

Ochrona antywirusowa i antyspyware

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

Ogólne

W sekcji **Ogólne** (**Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ogólne**) można włączyć wykrywanie następujących typów aplikacji:

- **Potencjalnie niepożądane aplikacje** — Grayware lub potencjalnie niepożądane aplikacje (PUA) to szeroka kategoria oprogramowania, które nie jest tak jednoznacznie niebezpieczne z założenia jak wirusy, konie trojańskie czy inne rodzaje szkodliwego oprogramowania. 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 aplikacji tego typu można znaleźć w słowniczku.
- **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. Są to między innymi narzędzia do dostępu zdalnego, dlatego ta opcja jest domyślnie wyłączona.
- **Podejrzane aplikacje** — należą do nich aplikacje skompresowane jako programy spakowane lub funkcje ochrony. Tego rodzaju funkcje ochrony są często wykorzystywane przez autorów szkodliwego oprogramowania do 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.

Aby skonfigurować wyłączenia w ramach systemu plików lub Internetu i poczty e-mail, kliknij przycisk **Ustawienia...**.

Wyłączenia

W sekcji **Wyłączenia** można wykluczyć pewne pliki i foldery, aplikacje lub adresy IP/IPv6 ze skanowania.

Pliki i foldery znajdujące się na karcie **System plików** będą wyłączone we wszystkich skanerach: przy uruchamianiu systemu, działającym w czasie rzeczywistym i na żądanie (skanowanie komputera).

- **Ścieżka** – ścieżka dostępu do wyłączonych plików i folderów.
- **Zagrożenie** – gdy obok wyłączonego pliku widać nazwę zagrożenia, oznacza to, że plik będzie pomijany tylko przy wyszukiwaniu tego zagrożenia, a nie całkowicie. Jeśli później plik zostanie zarażony innym szkodliwym oprogramowaniem, moduł antywirusowy to wykryje.
-  – tworzy nowe wyłączenie. Należy wprowadzić ścieżkę do obiektu (można używać symboli wieloznacznych * i ?) albo zaznaczyć folder lub plik w strukturze drzewa.

-  – usuwa zaznaczone elementy.
- **Domyślne** – anuluje wszystkie wyłączenia.

Na karcie **Strony internetowe i poczta e-mail** można wyłączyć ze skanowania protokołów niektóre **aplikacje** lub **adresy IP/IPv6**.

Ochrona uruchamiania

Funkcja sprawdzania plików przy uruchamianiu automatycznie skanuje pliki podczas uruchamiania systemu. Domyślnie skanowanie to jest przeprowadzane regularnie jako zaplanowane zadanie po zalogowaniu się użytkownika lub po pomyślnej aktualizacji modułów wykrywania. Aby zmodyfikować ustawienia technologii ThreatSense związane ze skanowaniem podczas uruchamiania, kliknij przycisk **Ustawienia**. Więcej informacji na temat konfiguracji technologii ThreatSense można znaleźć w tej sekcji.

Ochrona systemu plików w czasie rzeczywistym

Funkcja ochrony systemu plików w czasie rzeczywistym sprawdza wszystkie typy nośników i wywołuje skanowanie po wystąpieniu różnych zdarzeń. Jeśli jest używana technologia ThreatSense (opisana 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.

Domyślnie każdy plik jest skanowany po **otwarciu**, **utworzeniu** lub **wykonaniu**. Zalecamy zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalny poziom ochrony komputera w czasie rzeczywistym. Ochrona w czasie rzeczywistym jest włączana przy uruchamianiu systemu i zapewnia nieprzerwane skanowanie. W szczególnych przypadkach (np. jeśli wystąpi konflikt z innym skanerem działającym w czasie rzeczywistym) ochronę w czasie rzeczywistym można wyłączyć, klikając ikonę dostępną na pasku menu programu ESET Cyber Security (u góry ekranu), a następnie zaznaczając opcję **Wyłącz ochronę systemu plików w czasie rzeczywistym**. Ochronę systemu plików w czasie rzeczywistym można również wyłączyć w głównym oknie programu (kliknij opcję **Ustawienia** > **Komputer** i przełącz opcję **Ochrona systemu plików w czasie rzeczywistym** na ustawienie **WYŁĄCZONA**).

Ze sprawdzania przez skaner Real-time można wyłączyć następujące typy nośników:

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

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

Aby zmodyfikować zaawansowane ustawienia ochrony w czasie rzeczywistym, należy przejść do opcji **Ustawienia** > **Wprowadź preferencje aplikacji...** (lub nacisnąć klawisze *cmd+,*) i wybrać opcję **Ochrona w czasie rzeczywistym**, a następnie kliknąć przycisk **Ustawienia...** obok pozycji **Opcje zaawansowane** (opisanej w sekcji Zaawansowane opcje skanowania).

Opcje zaawansowane

W tym oknie można zdefiniować typy obiektów skanowanych przy użyciu technologii ThreatSense. Więcej informacji na temat **archiwów samorozpakowujących**, **programów spakowanych** oraz **zaawansowanej heurystyki** można znaleźć w sekcji Ustawienia parametrów technologii ThreatSense.

Nie zaleca się wprowadzania zmian w sekcji **Domyślne ustawienia archiwów**, chyba że jest to konieczne do rozwiązania konkretnego problemu, ponieważ większa liczba poziomów zagnieżdżania archiwów może spowodować obniżenie wydajności systemu.

Parametry technologii ThreatSense dotyczące wykonywanych plików — domyślnie podczas wykonywania plików jest używana funkcja **Zaawansowana heurystyka**. Zalecamy pozostawienie włączonych opcji inteligentnej optymalizacji oraz ESET Live Grid w celu ograniczenia wpływu na wydajność systemu.

Zwiększ zgodność woluminów sieciowych — ta opcja zwiększa wydajność w przypadku uzyskiwania dostępu do plików poprzez sieć. Należy ją włączyć, jeśli uzyskanie dostępu do dysków sieciowych trwa zbyt długo. Opcja korzysta z systemowego koordynatora plików w systemie macOS 10.10 i nowszych. Nie wszystkie aplikacje obsługują funkcję koordynatora plików — nie obsługuje jej na przykład program Microsoft Word 2011, a obsługuje ją program Word 2016.

Modyfikowanie ustawień ochrony w czasie rzeczywistym

Ochrona w czasie rzeczywistym jest najważniejszym komponentem programu ESET Cyber Security zapewniającym bezpieczeństwo systemu. Dlatego modyfikowanie parametrów tej funkcji należy przeprowadzać z dużą ostrożnością. Zmienianie ustawień ochrony jest zalecane tylko w określonych przypadkach, Na przykład w przypadku konfliktu z inną aplikacją.

Po zainstalowaniu programu ESET Cyber Security wszystkie ustawienia są optymalizowane w celu zapewnienia maksymalnego poziomu bezpieczeństwa systemu. Aby przywrócić ustawienia domyślne, należy kliknąć opcję **Domyślne** w lewej dolnej części okna **Ochrona w czasie rzeczywistym** (**Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ochrona w czasie rzeczywistym**).

Sprawdzanie skuteczności ochrony w czasie rzeczywistym

Aby zweryfikować, czy funkcja ochrony w czasie rzeczywistym działa i wykrywa wirusy, należy pobrać plik testowy eicar.com, a następnie sprawdzić, czy program ESET Cyber Security wykryje, że ten plik stanowi zagrożenie. Jest to specjalny nieszkodliwy plik wykrywany przez wszystkie programy antywirusowe. Został on utworzony przez instytut EICAR (ang. European Institute for Computer Antivirus Research) w celu testowania działania programów antywirusowych.

Co należy zrobić, jeśli ochrona w czasie rzeczywistym nie działa

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

Ochrona w czasie rzeczywistym jest wyłączona

Jeśli ochrona w czasie rzeczywistym została przypadkowo wyłączona przez użytkownika, należy ją włączyć ponownie. Aby ponownie włączyć ochronę w czasie rzeczywistym, w menu głównym należy kliknąć kolejno opcje **Ustawienia** > **Komputer** i przełączyć opcję **Ochrona systemu plików w czasie rzeczywistym** na ustawienie **WŁĄCZONA**. Ochronę systemu plików w czasie rzeczywistym można włączyć również w oknie preferencji aplikacji w sekcji **Ochrona w czasie rzeczywistym**, wybierając opcję **Włącz ochronę systemu plików w czasie rzeczywistym**.

Ochrona w czasie rzeczywistym nie wykrywa ani nie leczy infekcji

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

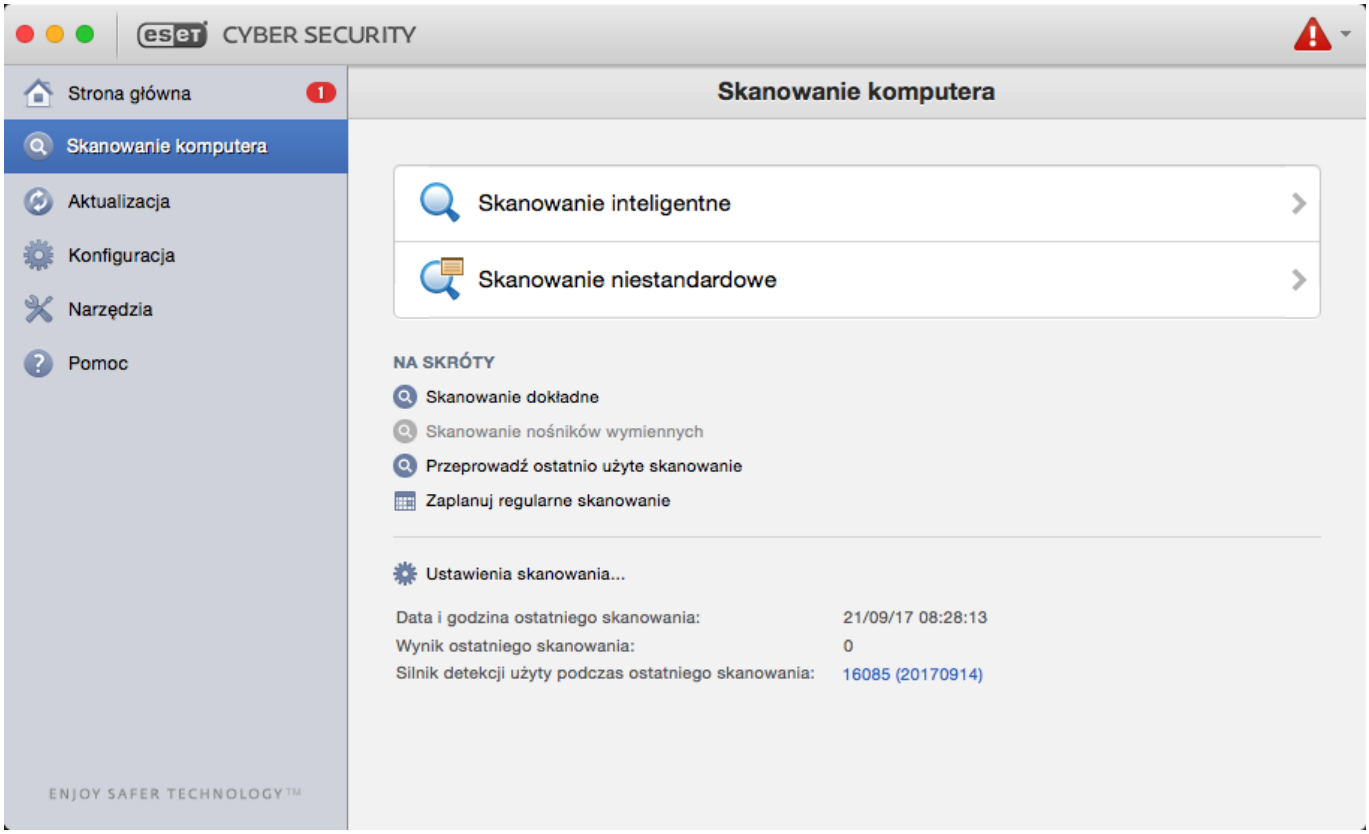
Ochrona w czasie rzeczywistym nie jest uruchamiana

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

Skanowanie komputera na żądanie

Jeśli istnieje podejrzenie, że komputer jest zainfekowany (działa w sposób nieprawidłowy), należy uruchomić funkcję **Skanowanie inteligentne**, aby sprawdzić, czy na komputerze nie ma infekcji. Aby zapewnić maksymalną ochronę, skanowanie komputera powinno być uruchamiane regularnie w ramach rutynowych działań związanych z bezpieczeństwem, a nie tylko w przypadku podejrzenia wystąpienia infekcji. Regularne skanowanie umożliwia wykrywanie zagrożeń, które podczas zapisywania zarażonych plików na dysku nie zostały wykryte przez skaner działający w czasie rzeczywistym. Jest to możliwe, jeśli w momencie wystąpienia infekcji skaner działający w czasie rzeczywistym był wyłączony lub moduły wykrywania były nieaktualne.

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



Typ skanowania

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

Skanowanie inteligentne

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

Skanowanie niestandardowe

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

Aby wybrać skanowane obiekty, użyj opcji **Skanowanie komputera** > **Skanowanie niestandardowe**, a następnie

zaznacz określone **skanowane obiekty** w strukturze drzewa. Obiekty do skanowania można również wskazać bardziej precyzyjnie, wprowadzając ścieżkę do folderu lub plików, które mają zostać objęte skanowaniem. Aby tylko przeskanować system bez wykonywania dodatkowych działań związanych z leczeniem, wybierz opcję **Skanuj bez leczenia**. Ponadto można wybrać jeden z trzech poziomów leczenia, klikając kolejno opcje **Ustawienia** > **Leczenie**.

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

Skanowane obiekty

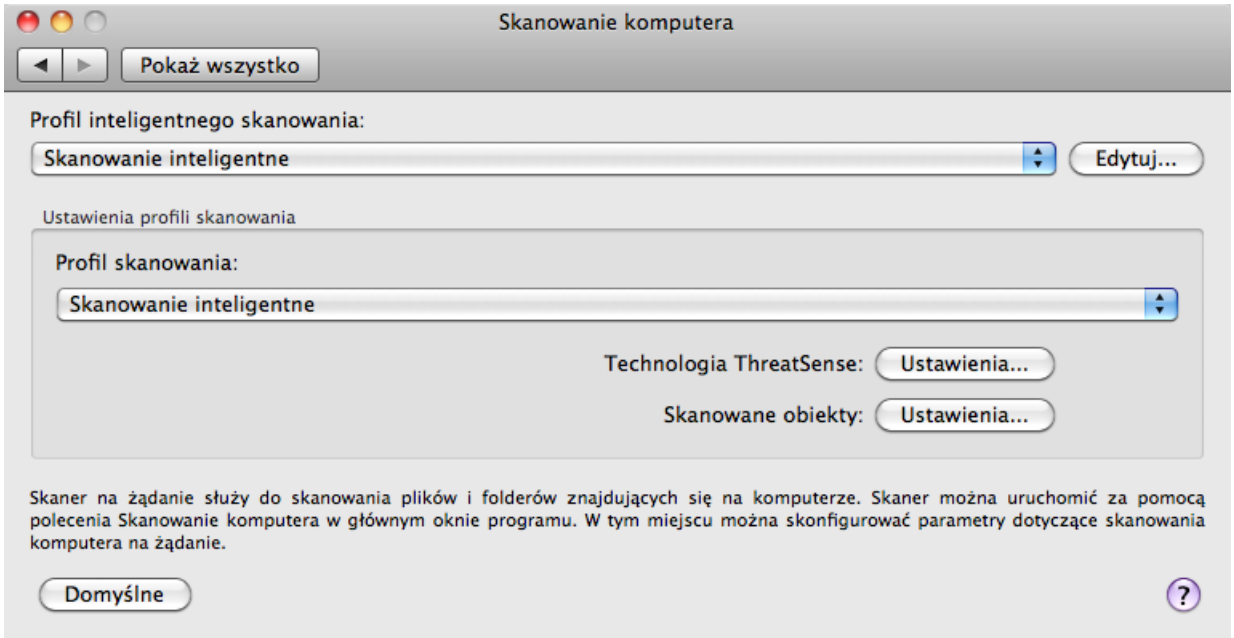
Struktura drzewa skanowanych obiektów umożliwia wybór plików i folderów, które mają być skanowane w poszukiwaniu wirusów. Foldery mogą również zostać zaznaczone zgodnie z ustawieniami profilu.

Skanowany obiekt można również dokładniej określić, wprowadzając ścieżkę do folderu lub plików, które mają zostać objęte skanowaniem. Aby wybrać skanowane obiekty w strukturze drzewa zawierającej wszystkie foldery na komputerze, należy zaznaczyć pole wyboru przy danym pliku lub folderze.

Profile skanowania

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

Aby utworzyć nowy profil, w menu głównym należy kliknąć kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** (lub nacisnąć klawisze *cmd+,*) > **Skanowanie komputera**, a następnie opcję **Edytuj...** obok listy bieżących profili.



Informacje na temat tworzenia profilu skanowania dostosowanego do indywidualnych potrzeb można znaleźć w

sekcji Ustawienia parametrów technologii ThreatSense, w której opisano poszczególne parametry ustawień skanowania.

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

Aby po ukończeniu skanowania na żądanie system operacyjny został zamknięty, a komputer wyłączony, należy użyć opcji **Wyłącz komputer po skanowaniu**.

Ustawienia parametrów technologii ThreatSense

ThreatSense to opracowana przez firmę ESET technologia będąca połączeniem kilku złożonych metod wykrywania zagrożeń. Technologia działa w sposób proaktywny, co oznacza, że zapewnia ochronę już od pierwszych godzin rozprzestrzeniania się nowego zagrożenia. Stosowana jest w niej kombinacja kilku metod (analiza kodu, emulacja kodu, sygnatury rodzajowe itp.), które razem znacznie zwiększają bezpieczeństwo systemu. Aparat skanowania umożliwia sprawdzanie kilku strumieni danych jednocześnie, co zwiększa do maksimum skuteczność i wskaźnik wykrywalności. Technologia ThreatSense przeciwdziała również programom typu rootkit.

Za pomocą ustawień technologii ThreatSense można określić kilka parametrów skanowania:

- typy i rozszerzenia plików, które mają być skanowane;
- kombinacje różnych metod wykrywania;
- poziomy leczenia itp.

Aby otworzyć okno ustawień, kliknij kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji** (lub naciśnij *cmd+,*), a następnie kliknij przycisk **Ustawienia technologii ThreatSense** dostępny w modułach **Ochrona uruchamiania**, **Ochrona w czasie rzeczywistym** oraz **Skanowanie komputera**, w których jest stosowana technologia ThreatSense (patrz poniżej). Różne scenariusze zabezpieczeń mogą wymagać różnych konfiguracji. Dlatego parametry technologii ThreatSense można konfigurować indywidualnie dla następujących modułów ochrony:

- **Ochrona uruchamiania** — automatyczne sprawdzanie plików wykonywanych podczas uruchamiania.
- **Ochrona w czasie rzeczywistym** — ochrona systemu plików w czasie rzeczywistym.
- **Skanowanie komputera** — skanowanie komputera na żądanie
- **Ochrona dostępu do stron internetowych**
- **Ochrona poczty e-mail**

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

Obiekty

Sekcja **Obiekty** umożliwia określenie, które pliki będą skanowane w poszukiwaniu infekcji.

- **Łącza symboliczne** — (tylko skanowanie komputera) skanowane są pliki zawierające ciąg tekstowy interpretowany i otwierany przez system operacyjny jako ścieżka do innego pliku lub katalogu.
- **Pliki poczty e-mail** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki poczty e-mail.
- **Skrzynki pocztowe** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są skrzynki pocztowe użytkowników znajdujące się w systemie. Niewłaściwe stosowanie tej opcji może prowadzić do konfliktu z używanym programem poczty e-mail. Więcej informacji o zaletach i wadach tej opcji można znaleźć w następującym artykule bazy wiedzy.
- **Archiwa** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki skompresowane w archiwach (.rar, .zip, .arj, .tar itd.).
- **Archiwa samorozpakowujące** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki znajdujące się w archiwach samorozpakowujących.
- **Pliki spakowane** — w przeciwieństwie do standardowych typów archiwów, pliki spakowane są rozpakowywane w pamięci. Wybranie tej opcji powoduje, że skanowane są również standardowe statyczne pliki spakowane (np. UPX, yoda, ASPack, FGS).

Opcje

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

- **Heurystyka** — heurystyka wykorzystuje algorytm analizujący (szkodliwe) działania podejmowane przez programy. Główną zaletą heurystyki jest możliwość wykrywania nowego szkodliwego oprogramowania, które wcześniej nie istniało.
- **Zaawansowana heurystyka** — zaawansowana heurystyka jest oparta na unikatowym algorytmie heurystycznym opracowanym przez firmę ESET. Został on zoptymalizowany pod kątem wykrywania robaków i koni trojańskich napisanych w językach programowania wysokiego poziomu. Zaawansowana heurystyka znacznie zwiększa możliwości programu w zakresie wykrywania zagrożeń.

Leczenie

Ustawienia leczenia określają sposób czyszczenia zainfekowanych plików przez skaner. Istnieją 3 poziomy leczenia:

- **Brak leczenia** — zainfekowane pliki nie są automatycznie leczone. Program wyświetla okno z ostrzeżeniem, a użytkownik sam wybiera żądane działanie.
- **Leczenie standardowe** — program próbuje automatycznie wyleczyć lub usunąć zarażony plik. Jeśli automatyczny wybór właściwego działania nie jest możliwy, program umożliwia użytkownikowi wybór dostępnych działań. Dostępne czynności są wyświetlane również wtedy, gdy wykonanie wstępnie zdefiniowanej czynności nie jest możliwe.

• **Leczenie dokładne** — program leczy lub usuwa wszystkie zainfekowane pliki (w tym archiwa). Jedyny wyjątek stanowią pliki systemowe. Jeśli wyleczenie pliku nie jest możliwe, do użytkownika wysyłane jest powiadomienie z prośbą o wybranie działania.

Pliki archiwum

W domyślnym trybie Leczenie standardowe całe pliki archiwum są usuwane tylko wtedy, gdy wszystkie pliki w archiwum są zainfekowane. Pliki archiwum, w których znajdują się zarówno pliki niezainfekowane, jak i zainfekowane, nie są usuwane. Jeśli zainfekowany plik archiwum zostanie wykryty w trybie Leczenie dokładne, usuwane jest całe archiwum, nawet jeśli zawiera również niezainfekowane pliki.

Skanowanie archiwów

W domyślnym trybie Leczenie standardowe całe pliki archiwum są usuwane tylko wtedy, gdy wszystkie pliki w archiwum są zainfekowane. Pliki archiwum, w których znajdują się zarówno pliki niezainfekowane, jak i zainfekowane, nie są usuwane. Jeśli zainfekowany plik archiwum zostanie wykryty w trybie Leczenie dokładne, usuwane jest całe archiwum, nawet jeśli zawiera również niezainfekowane pliki.

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.

Domyślnie skanowane są wszystkie pliki — niezależnie od rozszerzenia. Do listy plików wyłączonych ze skanowania można dodać dowolne rozszerzenie. Przy użyciu przycisków + i − można włączać i wyłączać skanowanie plików o określonych rozszerzeniach.

Wyłączenie plików ze skanowania jest czasami konieczne, jeśli skanowanie pewnych typów plików uniemożliwia prawidłowe działanie programu. Na przykład wskazane może być wyłączenie plików o rozszerzeniach *log*, *cfg* i *tmp*. Prawidłowy format wprowadzania rozszerzeń plików to:

log

cfg

tmp

Limity

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

• **Maksymalny rozmiar:** Określa maksymalny rozmiar obiektów do skanowania. Po określeniu maksymalnego rozmiaru moduł antywirusowy będzie skanować tylko obiekty o rozmiarze mniejszym niż określony. Tę opcję powinni modyfikować tylko zaawansowani użytkownicy, mający określone powody do wyłączenia większych obiektów ze skanowania.

• **Maksymalny czas skanowania:** Określa maksymalny czas przyznany na skanowanie obiektu. Jeśli użytkownik

określi tę wartość, moduł antywirusowy zatrzyma skanowanie obiektu po upływie ustalonego czasu — niezależnie od tego, czy skanowanie będzie zakończone.

• **Maksymalny poziom zagnieżdżania:** Określa maksymalną głębokość skanowania archiwów. Nie zaleca się zmieniania wartości domyślnej (równej 10); w normalnych warunkach nie powinno być powodów do jej modyfikacji. Jeśli skanowanie zostanie przedwcześnie zakończone z powodu liczby zagnieżdżonych archiwów, archiwum pozostanie niesprawdzone.

• **Maksymalny rozmiar pliku:** Opcja ta umożliwia określenie maksymalnego rozmiaru plików znajdujących się w archiwach (po ich rozpakowaniu), które mają być skanowane. Jeśli nałożenie tego limitu spowoduje przedwczesne zakończenie skanowania, archiwum pozostanie niesprawdzone.

Inne

Włącz inteligentną optymalizację

Włączenie inteligentnej optymalizacji powoduje wybranie ustawień zapewniających najwyższą skuteczność skanowania bez jego znacznego spowolnienia. Poszczególne moduły ochrony działają w sposób inteligentny, stosując różne metody skanowania. Funkcja inteligentnej optymalizacji dostępna w produkcie nie ma ostatecznej postaci. Programiści firmy ESET stale wprowadzają zmiany, które następnie są integrowane z programem ESET Cyber Security w ramach regularnych aktualizacji. Jeśli opcja Inteligentna optymalizacja jest wyłączona, podczas skanowania są wykorzystywane jedynie ustawienia określone przez użytkownika w mechanizmie ThreatSense danego modułu.

Skanuj alternatywny strumień danych (tylko skaner na żądanie)

Alternatywne strumienie danych używane w systemie plików to skojarzenia plików i folderów, których nie można sprawdzić za pomocą standardowych technik skanowania. Wiele infekcji stara się uniknąć wykrycia, udając alternatywne strumienie danych.

Wykrycie infekcji

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

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

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

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

Ogólnym przykładem sposobu działania programu ESET Cyber Security w momencie infekcji może być sytuacja, w której infekcja zostaje wykryta przez działający w czasie rzeczywistym monitor systemu plików z ustawionym domyślnym poziomem leczenia. Ochrona w czasie rzeczywistym podejmuje wtedy próbę wyleczenia lub usunięcia

pliku. W przypadku braku wstępnie zdefiniowanej czynności, którą ma wykonywać moduł ochrony w czasie rzeczywistym, zostanie wyświetlony monit o wybranie opcji w oknie alertu. Zazwyczaj dostępne są opcje **Wylecz**, **Usuń** i **Brak czynności**. Nie zaleca się wybierania opcji **Brak czynności**, ponieważ powoduje to pozostawienie zarażonych plików w obecnym stanie. Z tej opcji można skorzystać tylko w sytuacji, w której użytkownik ma pewność, że dany plik jest nieszkodliwy i został błędnie wykryty.

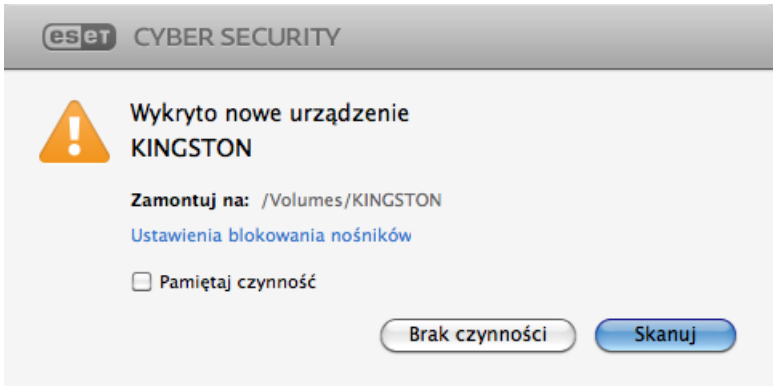
Leczenie i usuwanie
Leczenie należy zastosować w przypadku zarażonego pliku, do którego wirus dołączył szkodliwy kod. W takiej sytuacji należy najpierw podjąć próbę wyleczenia zainfekowanego pliku w celu przywrócenia go do stanu pierwotnego. Jeśli plik zawiera wyłącznie szkodliwy kod, zostanie usunięty w całości.

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

Skanowanie i blokowanie nośników wymiennych

Program ESET Cyber Security pozwala skanować na żądanie włożone nośniki pamięci wymiennej (CD, DVD, USB itp.). W systemie macOS 10.15 ESET Cyber Security umożliwia również skanowanie innych zewnętrznych urządzeń multimedialnych.

Skanowanie nośników wymiennych w systemie macOS 11 lub nowszym
W systemie macOS 11 lub nowszym, program ESET Cyber Security skanuje tylko nośniki pamięci.



Na nośnikach wymiennych może znajdować się szkodliwy kod stanowiący zagrożenie dla komputera. Aby zablokować nośniki wymienne, kliknij przycisk **Ustawienia blokowania nośników** (patrz powyższy obrazek) lub z menu głównego wybierz kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Nośnik** w głównym oknie programu, a następnie wybierz opcję **Włącz blokowanie nośników wymiennych**. Aby zezwolić na dostęp do określonych typów nośników, usuń zaznaczenie woluminów tych nośników.

Dostęp do napędu CD-ROM

Aby zezwolić na dostęp do zewnętrznego napędu CD-ROM podłączonego do komputera za pomocą kabla USB, należy usunąć zaznaczenie opcji **Napęd CD-ROM**.

Ochrona przed atakami typu „phishing”

Termin phishing określa przestępczą działalność wykorzystującą socjotechnikę (manipulowanie użytkownikiem w celu zdobycia poufnych informacji). Phishing jest często wykorzystywany do zdobywania danych wrażliwych takich jak numery kont bankowych, numery kart kredytowych, numery PIN oraz nazwy użytkownika i hasła.

Zalecamy, aby funkcja ochrony przed atakami typu „phishing” była włączona (**Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ochrona przed atakami typu „phishing”**). Wszystkie potencjalne ataki typu „phishing” pochodzące z niebezpiecznych witryn internetowych lub domen zostaną zablokowane, a o atakach będą użytkownika informować ostrzeżenia.

Ochrona stron internetowych i poczty e-mail

Aby z menu głównego przejść do ochrony stron internetowych i poczty e-mail, kliknij kolejno opcje **Ustawienia** > **Strony internetowe i poczta e-mail**. Z tego miejsca można również uzyskać dostęp do szczegółowych ustawień poszczególnych modułów, klikając pozycję **Ustawienia**.

- **Ochrona dostępu do stron internetowych** — monitoruje komunikację HTTP między przeglądarkami internetowymi a zdalnymi serwerami.
- **Ochrona programów poczty e-mail** — zapewnia sprawdzanie komunikacji e-mail przychodzącej za pośrednictwem protokołów POP3 oraz IMAP.
- **Ochrona przed atakami typu „phishing”** — blokuje potencjalne ataki typu „phishing” pochodzące z witryn internetowych lub domen.

Wyjątki skanowania
ESET Cyber Security nie skanuje zawartości używającej zaszyfrowanych protokołów HTTPS, POP3S i IMAPS.

Ochrona dostępu do stron internetowych

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

Filtrowanie stron internetowych można ustawić, definiując numery portów do komunikacji HTTP i/lub adresy URL.

Porty

Na karcie **Porty** można definiować numery portów używane przez komunikację HTTP. Domyślnie wstępnie zdefiniowane są numery portów 80, 8080 i 3128.

Lista adresów URL

Sekcja **Lista adresów 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 wyłączonych adresów będzie uzyskiwany bez skanowania pod kątem złośliwego kodu.

Aby zezwolić na dostęp tylko do adresów URL wymienionych na liście **Dozwolony adres URL**, należy wybrać opcję **Ogranicz adresy URL**.

Aby aktywować listę, należy wybrać opcję **Włączona** obok jej nazwy. Aby otrzymywać powiadomienia podczas wprowadzania adresu z bieżącej listy, należy wybrać opcję **Powiadamianie**.

W przypadku każdej listy można używać symboli specjalnych *(gwiazdka) i ?(znaku zapytania). Gwiazdka zastępuje dowolny ciąg znaków, a znak zapytania — dowolny symbol. Szczególną uwagę należy zachować podczas określania adresów wyłączonych, ponieważ lista powinna zawierać wyłącznie zaufane i bezpieczne adresy. Należy również zapewnić prawidłowe stosowanie na liście symboli * i ?.

Ochrona poczty e-mail

W ramach ochrony poczty e-mail sprawdzana jest komunikacja przychodząca za pośrednictwem protokołów POP3 oraz IMAP. Podczas analizowania wiadomości przychodzących program ESET Cyber Security stosuje wszystkie 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.

Technologia **ThreatSense: Ustawienia**— zaawansowana konfiguracja skanera umożliwia skonfigurowanie obiektów do skanowania, metod wykrywania itp. Aby wyświetlić okno z ustawieniami skanera, kliknij pozycję **Ustawienia**.

Dołącz informację do stopki wiadomości e-mail— 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:

- **Nigdy**— powiadomienia nie będą dodawane do żadnych wiadomości.
- **Tylko zainfekowane wiadomości**— jako sprawdzone będą oznaczane tylko wiadomości zawierające szkodliwe oprogramowanie.
- **Wszystkie przeskanowane wiadomości**— powiadomienia będą dodawane do wszystkich przeskanowanych wiadomości.

Dołącz notatkę do tematu otrzymanej i przeczytanej zainfekowanej wiadomości— 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 dla odbiorcy oraz, w przypadku wykrycia infekcji, udostępnia ważne informacje o poziomie zagrożenia danej wiadomości e-mail lub jej nadawcy.

Szablon komunikatu dołączanego do tematu zainfekowanej wiadomości e-mail — ten szablon można edytować, aby zmodyfikować format przedrostka tematu zainfekowanej wiadomości e-mail.

- %avstatus% — dodaje informację o stanie zainfekowania wiadomości e-mail (np.: wyleczona, zainfekowana itd.).
- %virus% — dodaje nazwę zagrożenia.
- %aspmstatus% — zmienia temat na podstawie wyniku skanowania antyspamowego.
- %product% — dodaje nazwę produktu ESET (w tym przypadku: ESET Cyber Security).
- %product_url% — dodaje łącze do witryny ESET (www.eset.com)

W dolnej części tego okna można włączyć lub wyłączyć sprawdzanie komunikacji przychodzącej za pośrednictwem protokołów POP3 oraz IMAP. Więcej informacji zawierają następujące tematy:

- Sprawdzanie protokołu POP3
- Sprawdzanie protokołu IMAP

Sprawdzanie protokołu POP3

Protokół POP3 jest najpopularniejszym protokołem używanym do odbioru poczty e-mail w programach poczty e-mail. Program ESET Cyber Security 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 filtrowanie protokołów działało prawidłowo, należy upewnić się, że moduł jest włączony. 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.

W przypadku wybrania opcji **Włącz sprawdzanie protokołu POP3** cały ruch protokołu POP3 jest monitorowany pod kątem szkodliwego oprogramowania.

Sprawdzanie protokołu IMAP

Protokół Internet Message Access Protocol (IMAP) jest kolejnym protokołem internetowym służącym do odbierania poczty e-mail. Protokół IMAP ma pod pewnymi względami przewagę nad protokołem POP3, np. wiele klientów może być podłączonych równocześnie do tej samej skrzynki odbiorczej przy zachowaniu informacji o stanie wiadomości (czy została ona przeczytana lub usunięta albo czy udzielono już na nią odpowiedzi). Program ESET Cyber Security 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 upewnić się, że sprawdzanie protokołu IMAP jest włączone. 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. Numery portów należy oddzielić przecinkami.

W przypadku wybrania opcji **Włącz sprawdzanie protokołu IMAP** cały ruch protokołu IMAP jest monitorowany pod kątem szkodliwego oprogramowania.

Aktualizacja

Regularne aktualizowanie programu ESET Cyber Security jest niezbędne dla utrzymania maksymalnego poziomu bezpieczeństwa. Moduł aktualizacji zapewnia aktualność programu poprzez pobieranie najnowszej modułów wykrywania.

Klikając w menu głównym opcję **Aktualizacja**, można sprawdzić bieżący stan aktualizacji programu ESET Cyber Security, w tym datę i godzinę ostatniej pomyślnej aktualizacji, oraz ustalić, czy w danej chwili należy przeprowadzić aktualizację. Aby rozpocząć procedurę aktualizacji ręcznie, należy kliknąć pozycję **Zaktualizuj moduły**.

W normalnych okolicznościach, po prawidłowym pobraniu aktualizacji w oknie Aktualizacja pojawia się komunikat **Aktualizacja nie jest konieczna — zainstalowane moduły są aktualne**. Jeśli nie można zaktualizować modułów, zalecamy sprawdzenie ustawień aktualizacji. Najczęstszą przyczyną takiego błędu są wprowadzone nieprawidłowo dane uwierzytelniania (nazwa użytkownika i hasło) lub niewłaściwie skonfigurowane ustawienia połączenia.

W oknie aktualizacji wyświetlany jest też numer wersji silnika detekcji. Numer wersji zawiera łącze do strony internetowej firmy ESET, na której znajdują się informacje o aktualizacji silnika detekcji.

Ustawienia aktualizacji

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

Opcje zaawansowane

Aby wyłączyć powiadomienia wyświetlane po każdej udanej aktualizacji, należy wybrać opcję **Nie wyświetlaj powiadomień o pomyślnych aktualizacjach**.

Aby pobrać tworzone moduły, które są w ostatnich fazach testów, włącz opcję **Aktualizacja w wersji wstępnej**.

Takie aktualizacje często zawierają rozwiązania problemów z programem. Opcja **Opóźniona aktualizacja** umożliwia pobieranie aktualizacji po kilku godzinach od ich opublikowania. Dzięki temu można upewnić się, że na komputerach klienckich nie zostaną zainstalowane aktualizacje, w przypadku których występują błędy po opublikowaniu.

Program ESET Cyber Security zapisuje migawki modułów wykrywania i modułów programu przeznaczone do użycia z funkcją **Cofanie aktualizacji**. Aby program ESET Cyber Security zapisywał te migawki automatycznie, opcja **Utwórz migawki plików aktualizacji** musi pozostać włączona. W razie podejrzeń, że nowa aktualizacja modułów wykrywania i/lub modułów programu może być niestabilna lub uszkodzona, można użyć funkcji cofania, aby przywrócić poprzednią wersję oraz wyłączyć aktualizacje na określony czas. Aby przywrócić najstarszą dostępną wersję aktualizacji, kliknij **Cofanie zmian**. Można także włączyć aktualizacje, które zostały wcześniej wyłączone na czas nieokreślony. Gdy używa się funkcji Cofanie aktualizacji w celu przywrócenia poprzedniej aktualizacji, można skorzystać z menu rozwijanego **Ustaw następujący okres zawieszenia** w celu określenia czasu trwania zawieszenia aktualizacji. Wybranie opcji **do odwołania** spowoduje, że normalne aktualizacje nie zostaną wznowione do momentu ich ręcznego przywrócenia. Aby ręcznie przywrócić aktualizacje, kliknij **Zezwól**. Należy zachować ostrożność przy ustawianiu czasu trwania zawieszenia aktualizacji.

Automatycznie ustaw maksymalny wiek silnika detekcji danych — umożliwia ustawienie maksymalnego czasu (w dniach), po upływie którego moduły wykrywania zostaną zgłoszone jako nieaktualne. Wartość domyślna to 7 dni.

Tworzenie zadań aktualizacji

Aktualizacje można uruchamiać ręcznie, klikając w menu głównym opcję **Aktualizuj**, a następnie klikając opcję **Zaktualizuj moduły**.

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

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

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

Uaktualnianie programu ESET Cyber Security do nowszej wersji

Używanie najnowszej kompilacji programu ESET Cyber Security gwarantuje maksymalne bezpieczeństwo. Aby sprawdzić dostępność nowej wersji, w menu głównym należy kliknąć opcję **Menu główne**. Jeśli jest dostępna nowa kompilacja, zostanie wyświetlona wiadomość. Aby wyświetlić okno z informacją o numerze wersji nowej kompilacji oraz dziennikiem zmian, kliknij przycisk **Więcej informacji...**

Kliknij przycisk **Tak**, aby pobrać najnowszą kompilację, lub przycisk **Nie teraz**, aby zamknąć okno i pobrać uaktualnienie później.

W przypadku kliknięcia opcji **Tak** plik zostanie zapisany w folderze pobierania (lub w folderze domyślnym ustawionym w przeglądarce internetowej). Po zakończeniu pobierania uruchom plik i wykonaj instrukcje dotyczące instalacji. Nazwa użytkownika wraz z hasłem zostanie automatycznie przeniesiona do nowej instalacji. Zalecamy regularne sprawdzanie dostępności aktualizacji — zwłaszcza w przypadku instalowania programu ESET Cyber Security z płyty CD lub DVD.

Aktualizacje systemu

Funkcja aktualizacji systemu macOS to ważny komponent, którego zadaniem jest zapewnienie użytkownikom ochrony przed szkodliwym oprogramowaniem. Ze względu na zapewnienie maksymalnego bezpieczeństwa zalecamy instalowanie aktualizacji natychmiast po ich udostępnieniu. Program ESET Cyber Security informuje o brakujących aktualizacjach zgodnie z określonym poziomem. Dostępność powiadomień o aktualizacjach można dostosować w obszarze **Ustawienia** > **Wprowadź preferencje aplikacji...** (lub naciskając *cmd+,*) > **Alerty i powiadomienia > Ustawienia...**, zmieniając opcje **Warunki wyświetlania** związane z pozycją **Aktualizacje systemu operacyjnego**.

- **Pokazuj wszystkie aktualizacje** — za każdym razem, gdy brakować będzie jakiejś aktualizacji systemu, zostanie wyświetlone powiadomienie
- **Pokazuj tylko zalecane** — wyświetlane będą wyłącznie powiadomienia dotyczące zalecanych aktualizacji

Jeśli użytkownik nie chce być powiadamiany o brakujących aktualizacjach, wystarczy odznaczyć pole wyboru obok pozycji **Aktualizacje systemu operacyjnego**.

W oknie powiadomień jest wyświetlany przegląd aktualizacji dostępnych dla systemu operacyjnego macOS oraz aplikacji aktualizowanych za pośrednictwem wbudowanego w systemie macOS narzędzia — Aktualizacje oprogramowania. Aktualizację można uruchomić bezpośrednio z okna powiadomień lub korzystając z sekcji **Menu główne** w programie ESET Cyber Security po kliknięciu opcji **Zainstaluj brakującą aktualizację**.

W oknie powiadomień znajduje się nazwa aplikacji, wersja, rozmiar, właściwości (flagi) oraz informacje dodatkowe dotyczące dostępnych aktualizacji. W kolumnie Flagi znajdują się następujące informacje:

- **[zalecane]** — zainstalowanie tej aktualizacji jest zalecane przez producenta systemu operacyjnego w celu zwiększenia bezpieczeństwa i stabilności systemu
- **[ponowne uruchomienie]** — po zainstalowaniu wymagane jest ponowne uruchomienie komputera
- **[wyłączenie]** — po zainstalowaniu konieczne jest wyłączenie komputera, a następnie ponowne włączenie go

W oknie powiadomień widać aktualizacje pobrane za pomocą narzędzia wiersza polecenia o nazwie „softwareupdate”. Aktualizacje pobrane za pomocą tego narzędzia mogą różnić się od aplikacji wyświetlanych przez aplikację „Aktualizacje oprogramowania”. W celu zainstalowania wszystkich dostępnych aktualizacji wyświetlanych w oknie „Brakujące aktualizacje systemu”, a także tych, które nie są wyświetlane przez aplikację „Aktualizacje oprogramowania” należy skorzystać z narzędzia wiersza polecenia „softwareupdate”. Więcej informacji na temat tego narzędzia można przeczytać w podręczniku dotyczącym narzędzia „softwareupdate” po wpisaniu tekstu man softwareupdate w oknie Terminal. Ta czynność jest zalecana wyłącznie w przypadku użytkowników zaawansowanych.

Narzędzia

Menu **Narzędzia** zawiera moduły upraszczające administrowanie programem i udostępniające dodatkowe opcje dla użytkowników zaawansowanych.

Pliki dziennika

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

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

1. **Wykryte zagrożenia** — po wybraniu tej opcji można zapoznać się ze wszystkimi informacjami na temat zdarzeń związanych z wykryciem infekcji.
2. **Zdarzenia** — ta opcja pomaga administratorom systemu i użytkownikom w rozwiązywaniu problemów. Wszystkie ważne czynności podejmowane przez program ESET Cyber Security są zapisywane w dziennikach zdarzeń.
3. **Skanowanie komputera** — w tym dzienniku są wyświetlane wyniki wszystkich ukończonych operacji skanowania. Dwukrotne kliknięcie dowolnego wpisu powoduje wyświetlenie szczegółowych informacji na temat danej operacji skanowania komputera na żądanie.
4. **Filtrowane strony internetowe** — lista stron internetowych zablokowanych w ramach ochrony dostępu do stron internetowych. W dziennikach odnotowane są: godzina, adres URL, stan, adres IP, nazwa użytkownika oraz aplikacja, która nawiązała połączenie z daną stroną internetową.

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

Administracja dziennikami

Dostęp do konfiguracji zapisywania w dziennikach w programie ESET Cyber Security można uzyskać z poziomu okna głównego. Kliknij kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji** (lub naciśnij *cmd+,*) > **Pliki dziennika**. Można określić następujące opcje plików dziennika:

- **Automatycznie usuwaj starsze rekordy dzienników** — wpisy dziennika starsze niż podana liczba dni (domyślnie 90 dni) są usuwane automatycznie.
- **Automatycznie optymalizuj pliki dzienników** — umożliwia automatyczną defragmentację plików dziennika w przypadku przekroczenia określonego procentu nieużywanych rekordów (domyślnie 25%).

Wszystkie istotne informacje wyświetlane w graficznym interfejsie użytkownika, komunikaty o zagrożeniach i zdarzeniach mogą być zapisywane w formatach tekstowych czytelnych dla człowieka, takich jak zwykły tekst lub

CSV (Comma-separated values). Jeśli pliki mają być dostępne do przetwarzania za pomocą narzędzi innych firm, należy zaznaczyć pole wyboru obok pozycji **Włącz zapisywanie w plikach tekstowych**.

Aby zdefiniować folder docelowy, w którym zapisywane będą pliki dziennika, należy kliknąć opcję **Ustawienia** obok pozycji **Opcje zaawansowane**.

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

- Zdarzenia takie jak *Nieprawidłowa nazwa użytkownika i hasło*, *Nie udało się zaktualizować modułów* itp. są zapisywane w pliku eventslog.txt.
- Zagrożenia wykryte przez funkcję Skaner przy uruchamianiu, Ochrona w czasie rzeczywistym lub Skanowanie komputera są zapisywane w pliku o nazwie threatslog.txt.
- Wyniki wszystkich ukończonych skanów są zapisywane w formacie scanlog.NUMER.txt.

Aby skonfigurować filtry w ramach opcji **Domyślne rekordy dziennika skanowania komputera**, należy kliknąć przycisk **Edytuj**, a następnie zaznaczyć lub usunąć zaznaczenie żądanych typów dzienników. Dodatkowe objaśnienia dotyczące typów dzienników można znaleźć w sekcji Filtrowanie dziennika.

Filtrowanie dziennika

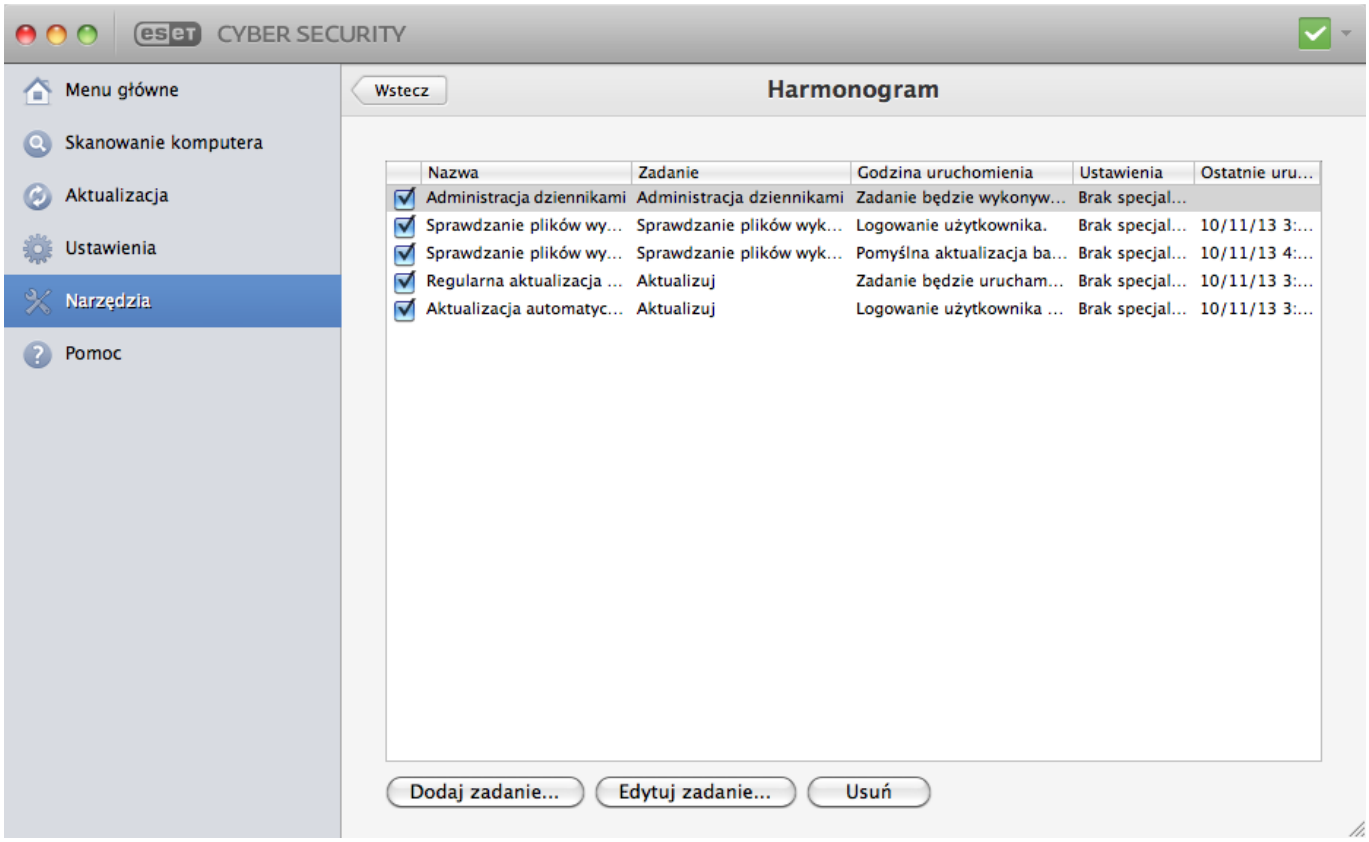
W dziennikach przechowywane są informacje o ważnych zdarzeniach systemowych. Funkcja filtrowania dziennika pozwala wyświetlać rekordy na temat określonego typu zdarzeń.

Najczęściej używane typy dzienników wymieniono poniżej:

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

Harmonogram

Opcja **Harmonogram** znajduje się w menu głównym programu ESET Cyber Security, w kategorii **Narzędzia**. Okno **Harmonogram** zawiera listę wszystkich zaplanowanych zadań oraz właściwości konfiguracyjne, takie jak wstępnie zdefiniowany dzień, godzina i używany profil skanowania.



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

Domyślnie w oknie Harmonogram są wyświetlane następujące zaplanowane zadania:

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

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

Tworzenie nowych zadań

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

- **Uruchamianie aplikacji**
- **Aktualizacja**
- **Konserwacja dziennika**

- **Skanowanie komputera na żądanie**
- **Sprawdzanie plików przy uruchamianiu systemu**

Uruchamianie aplikacji

Po wybraniu opcji **Uruchom aplikację** można uruchamiać programy jako użytkownik systemu o nazwie „nikt”. Uprawnienia do uruchamiania aplikacji za pośrednictwem Harmonogramu są definiowane w systemie macOS. Aby zamiast użytkownika domyślnego użyć innego użytkownika, wpisz jego nazwę z dwukropkiem przed poleceniem. Na potrzeby tej funkcji można też użyć użytkownika **root**.

Przykład: Uruchamianie zadania jako użytkownik

W tym przykładzie zaplanujemy uruchomienie aplikacji Kalkulator o określonej godzinie przez użytkownika **UserOne**:

1. W **Harmonogramie** wybierz pozycję **Dodaj zadanie**.
2. Wpisz nazwę zadania. Wybierz pozycję **Uruchamianie aplikacji** jako **Zaplanowane zadanie**. W oknie **Uruchom zadanie** wybierz pozycję **Raz**, aby uruchomić to zadanie jednorazowo. Kliknij przycisk **Dalej**.
3. Kliknij przycisk Przeglądaj i wybierz aplikację Kalkulator.
4. Wpisz **UserOne:** przed ścieżką aplikacji (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator'), a następnie kliknij przycisk **Dalej**.
5. Wybierz czas wykonania zadania, a następnie kliknij przycisk **Dalej**.
6. Wybierz opcję alternatywną na wypadek, gdyby nie można było uruchomić zadania, i kliknij przycisk **Dalej**.
7. Kliknij przycisk **Zakończ**.
8. Harmonogram ESET uruchomi aplikację Kalkulator o wybranej porze.

Przykład: Zadanie aktualizacji

W tym przykładzie utworzymy zadanie aktualizacji, które będzie uruchamiane o określonej porze.

1. Z menu rozwijanego **Zaplanowane zadanie** wybierz opcję **Aktualizacja**.
2. W polu **Nazwa zadania** wprowadź nazwę zadania.
3. W menu rozwijanym **Uruchom zadanie** wybierz częstotliwość, z jaką ma być wykonywane zadanie. Zależnie od wybranej częstotliwości zostaną wyświetlone różne parametry aktualizacji, które należy określić. W przypadku wybrania opcji **Zdefiniowane przez użytkownika** zostanie wyświetlony monit o określenie daty i godziny w formacie narzędzia cron (więcej szczegółów zawiera sekcja Tworzenie zadań zdefiniowanych przez użytkownika).
4. W następnym kroku zdefiniuj czynność podejmowaną w przypadku, gdy nie można wykonać lub zakończyć zadania w zaplanowanym czasie.
5. W ostatnim kroku zostanie wyświetlone okno z podsumowaniem informacji o bieżącym zaplanowanym zadaniu. Kliknij przycisk **Zakończ**. Nowe zaplanowane zadanie zostanie dodane do listy aktualnie zaplanowanych zadań.

Domyślnie w programie ESET Cyber Security istnieją wstępnie zdefiniowane zaplanowane zadania zapewniające prawidłowe działanie produktu. Są one domyślnie ukryte i nie należy ich zmieniać. Aby wyświetlić te zadania, w menu głównym kliknij kolejno **Ustawienia** > **Wprowadź preferencje aplikacji** (lub naciśnij klawisze *cmd+,*) > **Harmonogram**, a następnie wybierz opcję **Pokaż zadania systemowe**.

Skanowanie jako właściciel katalogu

Katalogi można skanować jako ich właściciel:

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -
f %u "$VOLUME"` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -
f /tmp/scan_log "$VOLUME"; done
```

Można także skanować folder `/tmp` jako aktualnie zalogowany użytkownik:

```
root:sudo -u \#`stat -
f %u /dev/console` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan'
 /tmp
```

Tworzenie zadań zdefiniowanych przez użytkownika

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

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

Przykład:

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

Znaki specjalne obsługiwane w wyrażeniach programu cron:

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

Nazwy dni (Monday-Sunday) i nazwy miesięcy (January-December) nie są obsługiwane.

> **Wykonywanie poleceń**
> W przypadku zdefiniowania zarówno dnia miesiąca, jak i dnia tygodnia polecenie zostanie wykonane tylko wtedy, gdy wartości obu pól będą dopasowane.

Kwarantanna

Głównym celem kwarantanny jest bezpieczne przechowywanie zarażonych plików. Pliki należy poddawać kwarantannie w przypadku, gdy nie można ich wyleczyć, gdy ich usunięcie nie jest bezpieczne lub zalecane albo gdy są one nieprawidłowo wykrywane przez program ESET Cyber Security.

Kwarantanną można objąć dowolny plik. Takie działanie jest zalecane, jeśli plik zachowuje się w podejrzany sposób, ale nie jest wykrywany przez skaner antywirusowy. Pliki poddane kwarantannie można przesyłać do analizy w laboratorium firmy ESET.

Pliki przechowywane w folderze kwarantanny mogą być wyświetlane w tabeli zawierającej datę i godzinę przeniesienia do kwarantanny, ścieżkę do pierwotnej lokalizacji zarażonego pliku, rozmiar pliku w bajtach, powód (np. dodanie przez użytkownika) oraz liczbę zagrożeń (np. jeśli plik jest archiwum zawierającym wiele infekcji). Folder kwarantanny z plikami poddanymi kwarantannie () pozostaje w systemie nawet po odinstalowaniu ESET Cyber Security. Pliki poddane kwarantannie są przechowywane w bezpiecznej, zaszyfrowanej postaci. Można je przywrócić po ponownym zainstalowaniu programu ESET Cyber Security.

Poddawanie plików kwarantannie

Program ESET Cyber Security automatycznie poddaje kwarantannie usunięte pliki (jeśli nie usunięto zaznaczenia odpowiedniej opcji w oknie alertu). Podejrzany plik można ręcznie poddać kwarantannie, klikając opcję **Kwarantanna...** . Można również użyć menu kontekstowego — należy nacisnąć klawisz Ctrl, kliknąć puste pole, wybrać opcję **Kwarantanna**, wybrać plik, który ma być poddany kwarantannie, i kliknąć przycisk **Otwórz**.

Przywracanie plików z kwarantanny

Pliki poddane kwarantannie można przywracać do ich pierwotnej lokalizacji. Aby to zrobić, należy wybrać plik objęty kwarantanną i kliknąć opcję **Przywróć**. Funkcja przywracania jest również dostępna w menu kontekstowym. w oknie Kwarantanna należy kliknąć żądany plik, trzymając wciśnięty klawisz CTRL, a następnie kliknąć opcję **Przywróć**. Menu kontekstowe zawiera także opcję **Przywróć do...** umożliwiającą przywrócenie pliku do lokalizacji innej niż ta, z której został usunięty.

Przesyłanie pliku z kwarantanny

Jeśli poddano kwarantannie podejrzany plik, który nie został wykryty przez program, lub plik został błędnie uznany za zarażony (na przykład podczas analizy heurystycznej kodu) i następnie poddany kwarantannie, należy przesłać plik do laboratorium firmy ESET. Aby przesłać plik z kwarantanny, należy kliknąć go, trzymając wciśnięty klawisz CTRL, i wybrać z menu kontekstowego opcję **Prześlij plik do analizy**.

Uruchomione procesy

Lista **Uruchomione procesy** zawiera procesy działające na komputerze. Program ESET Cyber Security udostępnia szczegółowe informacje o uruchomionych procesach, aby zapewnić użytkownikom ochronę przy użyciu technologii ESET Live Grid.

- **Proces** — nazwa procesu obecnie działającego na komputerze. Wszystkie uruchomione procesy można

również wyświetlić przy użyciu Monitora aktywności (znajdującego się w folderze */Applications/Utilities*).

• **Poziom ryzyka** — w większości przypadków program ESET Cyber Security i technologia ESET Live Grid przypisują obiektom (plikom, procesom itd.) poziomy ryzyka przy użyciu zestawu reguł heurystycznych, które badają charakterystykę każdego obiektu, a następnie oszacowują możliwość jego szkodliwego działania. Na podstawie tych reguł heurystycznych obiektom są przypisywane poziomy ryzyka. Znane aplikacje oznaczone kolorem zielonym na pewno nie są zainfekowane (są na białej liście) i zostaną wykluczone ze skanowania. Przyspiesza to skanowanie na żądanie i skanowanie w czasie rzeczywistym. Gdy aplikacja zostanie oznaczona jako nieznana (kolor żółty), nie oznacza to, że jest złośliwa. Zwykle jest to po prostu nowsza aplikacja. W razie wątpliwości dotyczących pliku można przesłać go do analizy w laboratorium firmy ESET. Jeśli okaże się, że plik to złośliwa aplikacja, jej sygnatura zostanie dodana w jednej z najbliższych aktualizacji.

• **Liczba użytkowników** — liczba użytkowników korzystających z danej aplikacji. Ta informacja jest zbierana przez system ESET Live Grid.

• **Czas wykrycia** — czas, który upłynął od momentu wykrycia aplikacji przez system ESET LiveGrid®.

• **Identyfikator pakietu aplikacji** — nazwa producenta lub procesu aplikacji.

Po kliknięciu procesu w dolnej części okna zostaną wyświetlone następujące informacje:

• **Plik** — lokalizacja aplikacji na komputerze

• **Rozmiar pliku** — fizyczny rozmiar pliku na dysku

• **Opis pliku** — charakterystyka pliku oparta na jego opisie w systemie operacyjnym

• **Identyfikator pakietu aplikacji** — nazwa producenta lub procesu aplikacji

• **Wersja pliku** — informacja pochodząca od wydawcy aplikacji

• **Nazwa produktu** — nazwa aplikacji i/lub nazwa handlowa

Połączenia sieciowe

Połączenia sieciowe to lista aktywnych połączeń sieciowych na komputerze. Program ESET Cyber Security udostępnia szczegółowe informacje o każdym połączeniu i umożliwia tworzenie reguł blokujących te połączenia.

Utwórz regułę blokowania dla tego połączenia

Program ESET Cyber Security umożliwia tworzenie reguł blokowania do każdego połączenia w menedżerze **Połączenia sieciowe**. Regułę blokowania można utworzyć, klikając połączenie prawym przyciskiem myszy i wybierając polecenie **Utwórz regułę blokowania dla tego połączenia**.

1. Wybierz **Profil** połączenia, do którego chcesz utworzyć regułę, i wpisz nazwę reguły. Wybierz aplikację, do której powinna być stosowana ta reguła, lub zaznacz pole wyboru, aby ta reguła była stosowana do wszystkich aplikacji.

2. Wybierz czynność dotyczącą połączenia: odrzucenie (zablokowanie) połączenia lub zezwolenie na nie. Wybierz kierunek łączności, do którego ma być stosowana reguła. Do reguły można utworzyć plik dziennika, klikając pozycję **Zapisuj reguły w dzienniku**.

3. Wybierz protokół połączenia i typy portów. Wybierz port usługi lub określ zakres portów w formacie od-do.

4. Wybierz miejsce docelowe i wprowadź informacje w wymaganym polu, w zależności od miejsca

docelowego.

System Live Grid

System monitorowania zagrożeń Live Grid zapewnia natychmiastowe i ciągłe informowanie programu ESET o nowych infekcjach. Dwukierunkowy system monitorowania zagrożeń Live Grid ma jeden cel — poprawę ochrony, którą możemy zaoferować użytkownikom. Najlepszą metodą zapewnienia wykrywania nowych zagrożeń natychmiast po ich pojawieniu się jest połączenie w sieć jak największej liczby naszych klientów i wykorzystanie ich jako zwiadowców wykrywających zagrożenia. Istnieją dwie możliwości:

1. Użytkownik może zdecydować, aby nie włączać systemu monitorowania zagrożeń Live Grid. Nie ograniczy to funkcji oprogramowania. Nadal będzie ono oferować najlepszą możliwą ochronę.
2. Można skonfigurować system monitorowania zagrożeń Live Grid tak, aby przesyłał anonimowe informacje na temat nowych zagrożeń i miejsc, w których znajduje się nowy kod stanowiący zagrożenie. Taki plik można wysłać do firmy ESET do szczegółowej analizy. Badanie tych zagrożeń ułatwia firmie ESET aktualizację silnika detekcji i ciągłe zwiększanie zdolności programu do ich wykrywania.

System monitorowania zagrożeń Live Grid będzie gromadzić informacje dotyczące nowo wykrytych zagrożeń związanych z danym komputerem. Te informacje mogą zawierać próbkę lub kopię pliku, w którym wystąpiło zagrożenie, ścieżkę dostępu do tego pliku, nazwę pliku, datę i godzinę, proces, za którego pośrednictwem zagrożenie pojawiło się na komputerze, oraz informacje o systemie operacyjnym komputera.

Wprawdzie istnieje możliwość sporadycznego ujawnienia w laboratorium firmy ESET pewnych informacji na temat użytkownika i komputera (nazwy użytkowników w ścieżce do pliku itp.), jednak informacje te nie będą używane do ŻADNYCH celów innych niż ułatwienie nam natychmiastowej reakcji na nowe zagrożenia.

Aby uzyskać dostęp do konfiguracji systemu Live Grid z menu głównego, kliknij kolejno pozycje **Ustawienia** > **Wprowadź preferencje aplikacji...** (lub naciśnij klawisz *cmd+,*) > **Live Grid**. W celu uaktywnienia systemu Live Grid wybierz polecenie **Włącz system monitorowania zagrożeń Live Grid**, a następnie kliknij opcję **Ustawienia...** widoczną w pobliżu pozycji **Opcje zaawansowane**.

Konfiguracja systemu Live Grid

Domyślnie program ESET Cyber Security jest skonfigurowany do przesyłania podejrzanych plików do szczegółowej analizy w laboratorium firmy ESET. Aby pliki nie były przesyłane automatycznie, wystarczy usunąć zaznaczenie opcji **Przesyłaj pliki**.

Po wykryciu podejrzanego pliku na komputerze można go przesłać do analizy w laboratorium. W tym celu w głównym oknie programu kliknij kolejno opcje **Narzędzia** > **Prześlij plik do analizy**. Jeśli plik okaże się szkodliwą aplikacją, informacje potrzebne do jej wykrywania zostaną dodane do kolejnej aktualizacji.

Przesyłaj anonimowe statystyki— system monitorowania zagrożeń ESET Live Grid zbiera anonimowe informacje o komputerze dotyczące nowo wykrytych zagrożeń. Obejmują one nazwę infekcji, datę i godzinę jej wykrycia, wersję programu zabezpieczającego firmy ESET, wersję systemu operacyjnego oraz ustawienia regionalne. Zazwyczaj statystyki te są wysyłane na serwery firmy ESET raz lub dwa razy dziennie.

Filtr wyłączenia— umożliwia wykluczenie określonych typów plików z przesyłania. Warto na przykład wykluczyć pliki, które mogą zawierać poufne informacje, takie jak dokumenty lub arkusze kalkulacyjne. Najpopularniejsze

typy plików należących do tej kategorii (doc, rtf itd.) są wykluczone domyślnie. Do listy wykluczonych plików można dodawać inne typy plików.

Kontaktowy adres e-mail (opcjonalnie)— adres e-mail użytkownika zostanie użyty, jeśli do przeprowadzenia analizy będą potrzebne dodatkowe informacje. Uwaga: użytkownik nie otrzyma odpowiedzi od firmy ESET, jeśli nie będą potrzebne dodatkowe informacje.

Przesyłanie pliku do analizy

Jeżeli znajdziesz podejrzany plik na komputerze, możesz go przesłać do analizy w laboratorium firmy ESET.

Zanim prześlesz próbki do firmy ESET

Nie przesyłaj próbki, jeżeli nie spełnia co najmniej jednego z następujących kryteriów:

- Próbka nie jest w ogóle wykrywana przez produkt ESET.
- Plik jest błędnie wykrywany jako zagrożenie.
- Nie akceptujemy plików osobistych jako próbek (w celu przeskanowania pod kątem szkodliwego oprogramowania przez ESET). Laboratorium ESET nie skanuje plików użytkowników na żądanie.
- Wpisz opisowy temat wiadomości i podaj jak najwięcej informacji na temat podejrzanego pliku (może to być np. zrzut ekranu lub adres witryny internetowej, z której został on pobrany).

Aby przesłać próbkę, użyj formularza przesyłania próbki dostępnego w produkcie. Aby go znaleźć, wybierz pozycje **Narzędzia** > **Prześlij plik do analizy**.

W formularzu **Prześlij próbkę do analizy** wypełnij następujące elementy:

Plik — ścieżka do pliku, który użytkownik zamierza przesłać.

Komentarz – opisz powód, dla którego przesyłasz plik.

Kontaktowy adres e-mail — adres ten jest wysyłany do firmy ESET razem z podejrzanymi plikami. Może on zostać wykorzystany w celu nawiązania kontaktu, jeśli analiza wymaga dodatkowych informacji. Wprowadzenie adresu kontaktowego jest opcjonalne.

ESET może nie odpowiedzieć na zgłoszenie

Jeśli nie są wymagane dodatkowe informacje, firma ESET nie odpowiada na zgłoszenia. Nasze serwery codziennie odbierają dziesiątki tysięcy plików, dlatego nie da się odpowiedzieć każdemu nadawcy.
Jeśli okaże się, że próbka jest szkodliwą aplikacją lub witryną internetową, możliwość jej wykrycia zostanie dodana do jednej z przyszłych aktualizacji produktu ESET.

Interfejs użytkownika

Opcje konfiguracji interfejsu użytkownika umożliwiają dostosowanie środowiska pracy do potrzeb użytkownika. Dostęp do tych opcji można uzyskać z menu głównego, klikając kolejno **Ustawienia** > **Wprowadź preferencje aplikacji...** (lub naciskając klawisze *cmd+,*) > **Interfejs**.

- Aby wyświetlić podczas uruchamiania systemu ekran powitalny programu ESET Cyber Security, zaznacz opcję

Pokaż ekran powitalny przy uruchamianiu.

• Opcja **Pokazuj aplikację w Doku** umożliwia wyświetlenie ikony programu ESET Cyber Security w Doku systemu macOS i przełączanie między programem ESET Cyber Security a innymi działającymi aplikacjami przez naciśnięcie klawiszy *cmd+tab*. Zmiany staną się aktywne po ponownym uruchomieniu programu ESET Cyber Security (zwykle w wyniku ponownego uruchomienia komputera).

• Opcja **Użyj standardowego menu** umożliwia korzystanie z określonych skrótów klawiszowych (patrz Skróty klawiszowe) i wyświetlanie standardowych elementów menu (Interfejs użytkownika, Ustawienia i Narzędzia) na pasku menu systemu macOS (u góry ekranu).

• Aby włączyć wyświetlanie etykiet narzędzi dla pewnych opcji programu ESET Cyber Security, zaznacz opcję **Pokaż etykiety narzędzi**.

• Z kolei opcja **Pokaż ukryte pliki** umożliwia wyświetlanie i zaznaczanie ukrytych plików w części **Skanowane obiekty** znajdującej się w oknie **Skanowanie komputera**.

• Domyślnie ikona programu ESET Cyber Security jest wyświetlana w obszarze elementów dodatkowych po prawej stronie paska menu systemu macOS (u góry ekranu). Aby wyłączyć tę funkcję, należy usunąć zaznaczenie pola **Pokazuj ikonę w elementach dodatkowych paska menu**. Zmiana stanie się aktywna po ponownym uruchomieniu programu ESET Cyber Security (zwykle w wyniku ponownego uruchomienia komputera).

Alerty i powiadomienia

Sekcja **Alerty i powiadomienia** umożliwia konfigurowanie sposobu obsługi alertów o zagrożeniach i powiadomień systemowych w programie ESET Cyber Security.

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

Wybranie opcji **Wyświetlaj powiadomienia na pulpicie** powoduje wyświetlanie na ekranie komputera okien alertów niewymagających interwencji ze strony użytkownika (domyślnie — w prawym górnym rogu ekranu). Za pomocą ustawienia **Automatycznie powiadomienia zamykaj po** X **s** można określić czas, przez jaki powiadomienia są widoczne (domyślnie 5 sekund).

Od wersji 6.2 programu ESET Cyber Security możliwe jest również wyłączanie wyświetlania niektórych **stanów ochrony** na ekranie głównym (w oknie **Stan ochrony**). Więcej informacji na ten temat można znaleźć w sekcji Stany ochrony.

Wyświetlanie alertów

Program ESET Cyber Security wyświetla okna dialogowe alertu informujące o nowej wersji programu, nowej aktualizacji systemu operacyjnego, wyłączeniu niektórych komponentów programu, usunięciu dzienników itp. Poszczególne powiadomienia można wyłączyć, zaznaczając opcję **Nie pokazuj ponownie tego okna dialogowego**.

Opcja **Lista okien dialogowych** (**Ustawienia** > **Wprowadź preferencje aplikacji...** > **Alerty i powiadomienia** > **Ustawienia...**) wyświetla listę wszystkich okien dialogowych alertu, wywoływanych przez program ESET Cyber Security. Aby włączyć lub wyłączyć poszczególne powiadomienia, należy zaznaczyć pole wyboru po lewej stronie pozycji **Nazwa okna dialogowego**. Można ponadto zdefiniować **warunki wyświetlania** określające, kiedy mają być wyświetlane powiadomienia o nowych wersjach programu i o aktualizacjach systemu operacyjnego.

Stany ochrony

Aktualny stan ochrony programu ESET Cyber Security można zmienić aktywując lub dezaktywując stany w obszarze **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Alerty i powiadomienia** > **Wyświetl na ekranie Stan ochrony: Konfiguracja**. Stany poszczególnych funkcji programu będą wyświetlane w oknie głównym programu ESET Cyber Security (okno **Stan ochrony**) lub zostaną ukryte.

Istnieje możliwość ukrycia stanów następujących funkcji programu:

- Ochrona przed atakami typu „phishing”
- Ochrona dostępu do stron internetowych
- Ochrona programów poczty e-mail
- Aktualizacja systemu operacyjnego
- Wygaśnięcie licencji
- Wymagane ponowne uruchomienie komputera

Uprawnienia

Ustawienia programu ESET Cyber Security mogą odgrywać dużą rolę w całościowej polityce bezpieczeństwa firmy. Nieupoważnione modyfikacje mogą stanowić zagrożenie dla stabilności i ochrony systemu. Dlatego można zdefiniować użytkowników mających uprawnienia do edytowania konfiguracji programu.

Aby określić uprzywilejowanych użytkowników, kliknij kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji** (lub naciśnij klawisze *cmd+,*) > **Uprawnienia**. Wybierz użytkowników lub grupy z listy po lewej stronie i kliknij przycisk **Dodaj**. Aby wyświetlić wszystkich użytkowników lub wszystkie grupy w systemie, wybierz opcję **Pokaż wszystkich użytkowników/grupy**. Aby usunąć użytkownika, zaznacz jego nazwę na liście **Wybrani użytkownicy** po prawej stronie, a następnie kliknij przycisk **Usuń**.

Informacje o zwiększaniu uprawnień
Jeśli lista Wybrani użytkownicy pozostanie pusta, wszyscy użytkownicy będą uznani za uprzywilejowanych.

Menu kontekstowe

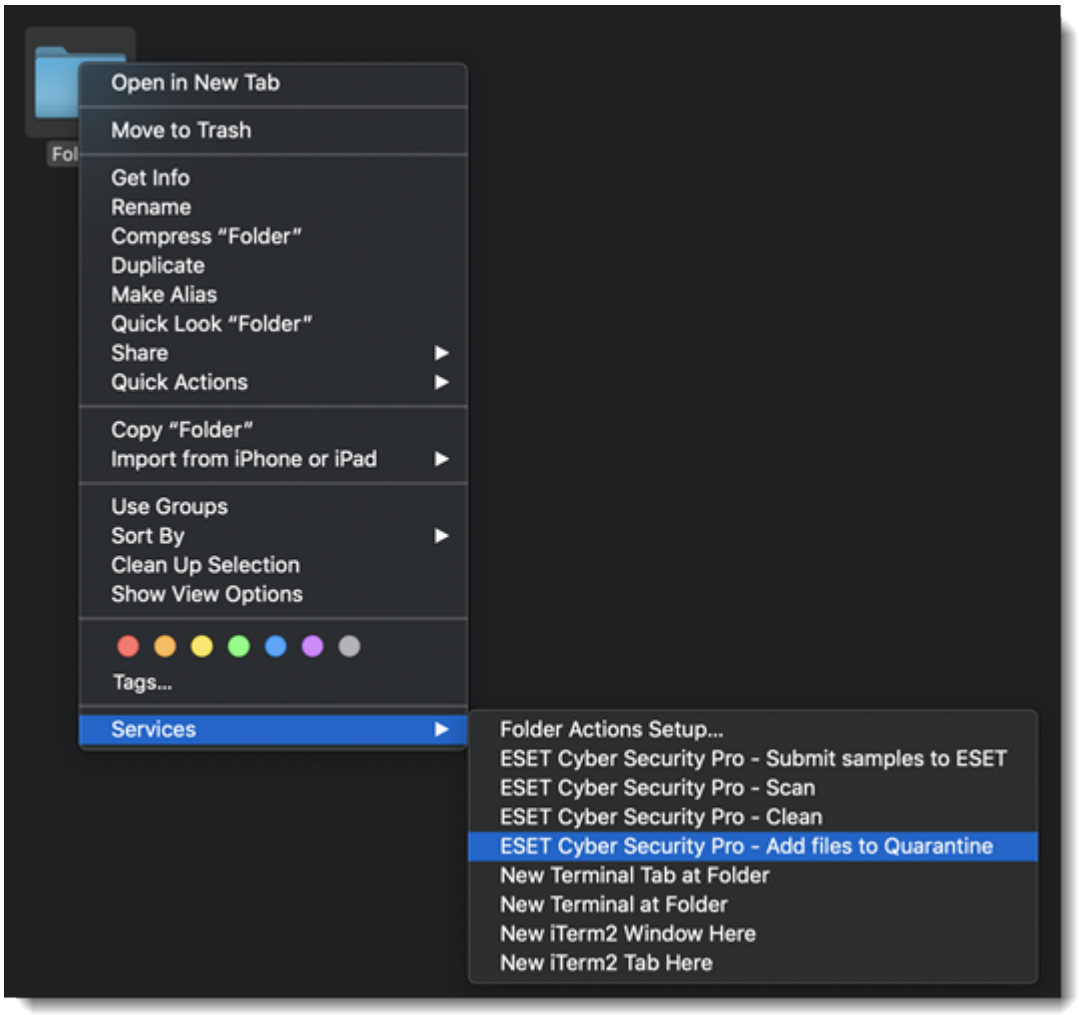
Integrację menu kontekstowego można włączyć, wybierając kolejno opcje **Ustawienia** > **Wprowadź preferencje aplikacji** (lub naciskając klawisze *cmd+,*) > sekcję **Menu kontekstowe** i wybierając opcję **Zintegruj z menu kontekstowym**. W celu uaktywnienia zmian konieczne jest wylogowanie się lub ponowne uruchomienie komputera. Opcje menu kontekstowego będą dostępne w oknie programu **Finder** po naciśnięciu klawisza CTRL i kliknięciu dowolnego pliku.

Można wybrać opcje, które zostaną wyświetlone w menu kontekstowym. Opcja **Tylko skanowanie** umożliwi skanowanie wybranego pliku, natomiast opcja **Tylko leczenie** umożliwia wyleczenie wybranego pliku z menu kontekstowego. Leczenie należy zastosować w przypadku zarażonego pliku, do którego wirus dołączył szkodliwy kod. W takiej sytuacji należy najpierw podjąć próbę wyleczenia zainfekowanego pliku w celu przywrócenia go do

stanu pierwotnego. Jeśli plik zawiera wyłącznie szkodliwy kod, zostanie usunięty w całości.

Wybranie opcji **Wszystkie** umożliwia wykonanie następujących zadań z poziomu menu kontekstowego:

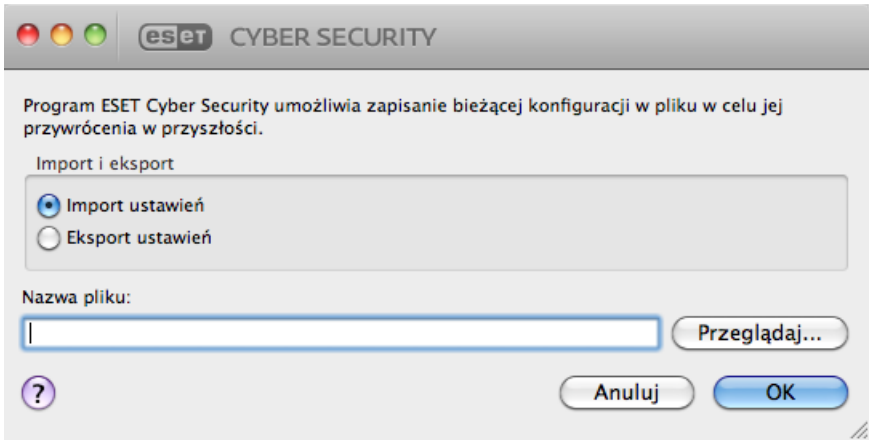
- Prześlij próbki do firmy ESET
- Skanuj
- Bezpieczny
- Dodawanie plików do kwarantanny



Import i eksport ustawień

Aby zaimportować istniejącą konfigurację lub wyeksportować konfigurację produktu ESET Cyber Security, należy kliknąć opcje **Ustawienia** > **Importowanie lub eksportowanie ustawień**.

Funkcja importu i eksportu jest przydatna, gdy konieczne jest utworzenie kopii zapasowej bieżącej konfiguracji programu ESET Cyber Security w celu jej użycia w późniejszym czasie. Opcja Eksportuj ustawienia jest również przydatna dla użytkowników, którzy chcą używać preferowanej konfiguracji programu ESET Cyber Security w wielu systemach. Plik konfiguracyjny można łatwo zaimportować w celu przeniesienia żądanych ustawień.



Aby importować konfigurację, należy zaznaczyć opcję **Importuj ustawienia** i kliknąć przycisk **Przeglądaj** w celu przejścia do pliku konfiguracyjnego do zaimportowania. Aby eksportować, należy zaznaczyć opcję **Eksportuj ustawienia** i za pomocą przeglądania wybrać lokalizację na komputerze, w której ma zostać zapisany plik konfiguracyjny.

Ustawienia serwera proxy

Ustawienia serwera proxy można skonfigurować w menu **Ustawienia** > **Wprowadź preferencje aplikacji...** (można również nacisnąć klawisze *cmd+,*) i wybrać opcję **Serwer proxy**. Określenie serwera proxy na tym poziomie powoduje zdefiniowanie globalnych ustawień serwera proxy dla wszystkich funkcji programu ESET Cyber Security. Wprowadzone w tym miejscu parametry są używane przez wszystkie moduły, które wymagają połączenia internetowego. Program ESET Cyber Security obsługuje uwierzytelnianie podstawowe oraz NTLM (NT LAN Manager).

Aby określić ustawienia serwera proxy na tym poziomie, wybierz pozycję **Użyj serwera proxy**, a następnie wprowadź w polu **Serwer proxy** adres IP lub adres URL serwera proxy. W polu Port należy określić port, na którym serwer proxy akceptuje połączenia (domyślnie 3128). Aby program sam wypełnił oba pola, należy kliknąć pozycję **Wykryj**.

Jeśli do komunikacji z serwerem proxy wymagane jest uwierzytelnianie, należy wprowadzić odpowiednie informacje w polach **Nazwa użytkownika** i **Hasło**.

Umowa licencyjna użytkownika końcowego

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 DOKUMENTU POLITYKA PRYWATNOŚCI.**

Umowę Licencyjną Użytkownika Końcowego

Niniejsza Umowa licencyjna użytkownika końcowego (w dalszej części nazywana „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 (w dalszej części nazywaną „firmą ESET” lub „Dostawcą”), a licencjobiorcą, który jest osobą fizyczną lub prawną (w dalszej części nazywanym „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. Jeśli Licencjobiorca nie wyraża zgody na którykolwiek warunek określony w niniejszej Umowie, 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 (w dalszej części nazywane „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 systemie komputerowym 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 Business Edition.** W przypadku zamiaru zainstalowania i użycia Oprogramowania 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 w Oprogramowaniu zmian w

formie aktualizacji (w dalszej części nazywanych „Aktualizacjami”), przy czym nie jest on ograniczony żadnymi terminami wprowadzenia takich zmian ani nie jest zobowiązany do ich wprowadzenia. 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.

b) **Przekazywanie szkodliwego oprogramowania i informacji o komputerze do Dostawcy**. Oprogramowanie obejmuje funkcje, które gromadzą przykłady nowych wirusów komputerowych, innych szkodliwych programów komputerowych oraz podejrzanych, problematycznych, potencjalnie niepożądanych lub niebezpiecznych obiektów, takich jak pliki, adresy URL, pakiety IP oraz ramki Ethernet (odtąd ogólnie „Szkodliwe oprogramowanie”), po czym wysyłają je do Dostawcy. Wysyłane dane obejmują m.in. informacje o procesie instalacji, komputerze lub platformie, na której zainstalowano Oprogramowanie, w tym informacje o działaniu i funkcjonalności Oprogramowania (odtąd ogólnie „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. Licencjobiorca niniejszym wyraża zgodę na otrzymywanie powiadomień i wiadomości, w tym między innymi informacji marketingowych.

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. 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 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. 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 (zwane dalej „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 (zwane dalej „Przepisami o kontroli eksportu");

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 (zwane dalej „Przepisami o sankcjach").

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.

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. W przypadku rozbieżności pomiędzy wersjami językowymi niniejszej Umowy pierwszeństwo ma wersja angielska. Zmiana niniejszej Umowy musi mieć formę pisemną i musi zostać zatwierdzona podpisem złożonym przez upoważnionego przedstawiciela Dostawcy lub przez osobę wyraźnie upoważnioną do reprezentowania Dostawcy na zasadzie pełnomocnictwa.

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.

EULA ID: HOM-ECS-20-01

Zasady ochrony prywatności

Firma ESET, spol. s r. o. z siedzibą pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Bratysławy I w sekcji Sro, pozycja nr 3586/B, numer w rejestrze gospodarczym: 31333532 jako administrator danych (dalej "ESET" lub "my") pragnie zachować przejrzystość w odniesieniu do danych osobowych oraz poufności informacji swoich klientów. W związku z tym publikujemy niniejsze Zasady ochrony prywatności wyłącznie w celu przekazania klientowi (dalej "Użytkownik" lub "Ty") informacji na następujące tematy: 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
  - Odane 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);
  - Oinformacje o urządzeniach w sieci lokalnej, takie jak typ, producent, model i/lub nazwa urządzenia;
  - Oinformacje dotyczące korzystania z Internetu, takie jak adres IP, informacje geograficzne, pakiety IP, adresy URL i ramki sieci Ethernet;

Opliki 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