ESET Mobile Security

Podręcznik użytkownika

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Digital Security
Progress. Protected.

Prawa autorskie ©2024 ESET, spol. s r.o.

Produkt ESET Mobile Security został opracowany przez ESET, spol. s r.o.

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

Wszelkie prawa zastrzeżone. Żadna część tej dokumentacji nie może być powielana, przechowywana w systemie wyszukiwania lub przesyłana w jakiejkolwiek formie lub za pomocą jakichkolwiek środków elektronicznych, mechanicznych, fotokopiowania, nagrywania, skanowania lub w inny sposób bez pisemnej zgody autora.

Firma ESET, spol. s r.o. zastrzega sobie prawo do zmiany dowolnej z opisanych aplikacji bez uprzedniego powiadomienia.

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

WER. 26.01.2024

1 Wstęp 1
1.1 Nowości 1
1.2 Minimalne wymagania systemowe 1
2 Kreator uruchamiania 2
3 Odinstalowanie 4
4 Łączenie z ESET HOME 5
5 Antywirus 7
5.1 Dzienniki skanowania 10
5.2 Ustawienia zaawansowane 10
5.3 Adware Detector 12
6 Raport zabezpieczeń 12
7 Dziennik aktywności 14
8 Anti-Theft 15
8.1 Ustawienia funkcji Anti-Theft 16
8.2 Optymalizacja 17
8.3 Portal internetowy 18
8.4 ESET HOME hasło 18
9 Anti-Phishing 19
9.1 Ochrona SMS i ochrona powiadomień 21
10 Blokada aplikacji 22
10.1 Nie pamiętam kodu PIN blokady aplikacji 23
11 Ochrona płatności 24
12 Filtr połączeń 25
12.1 Dodawanie nowej reguły 26
13 Inspekcja sieci 27
14 Audyt zabezpieczeń 28
14.1 Monitorowanie urządzenia 28
14.2 Audyt aplikacji 28
15 Ustawienia 29
16 Dział obsługi klienta 30
17 Umowa licencyjna użytkownika końcowego 31
18 Zasady ochrony prywatności 40

Wprowadzenie

ESET Mobile Security to kompletne rozwiązanie zabezpieczające, które chroni urządzenie przed pojawiającymi się zagrożeniami i stronami wyłudzającymi dane oraz umożliwia zdalne przejęcie kontroli nad urządzeniem w przypadku jego utraty lub kradzieży.

Główne funkcje to:

- Antywirus
- Funkcja Anti-Theft
- Ochrona przed atakami typu „phishing”
- Integracja z portalem ESET HOME
- Filtr połączeń
- Audyt zabezpieczeń
- Raport zabezpieczeń
- Inspekcja sieci
- Blokada aplikacji
- Ochrona płatności

Nowości

Nowe funkcje w ESET Mobile Security w wersji 8:

Dodane

- Obsługę Androida 14
- Antismishing (ochrona SMS i ochrona powiadomień)
- Używanie symboli wieloznacznych w filtrze połączeń

Ulepszono:

- Nowy wygląd ekranu głównego
- Nowy wygląd menu głównego

Minimalne wymagania systemowe

Aby zainstalować aplikację ESET Mobile Security, urządzenie z systemem Android musi spełniać następujące minimalne wymagania systemowe:

- System operacyjny: Android 6 (Marshmallow) lub nowszy
- Rozdzielczość ekranu dotykowego: co najmniej 240x320 pikseli
- Procesor: 500+ MHz ARM7+
- RAM: 512+ MB
- Połączenie internetowe

Wykluczenia dotyczące pomocy technicznej

- Urządzenia z dwiema kartami SIM oraz urządzenia z pełną kontrolą nad systemem nie są obsługiwane. Funkcje Anti-Theft oraz Filtr połączeń nie są dostępne na tabletach nieobsługujących połączeń i wiadomości.
- Android Gor nie jest obsługiwany
- Oprogramowanie ESET Mobile Security wymaga, aby usługi Google Play działały poprawnie. Oprogramowanie ESET Mobile Security nie jest obsługiwane na urządzeniach bez usług Google Play, takich jak niektóre urządzenia Huawei.
- Funkcja Anti-Theft zaufanych kart SIM nie jest dostępna na urządzeniach CDMA.
- Niektóre z wymienionych funkcji zależą od systemu operacyjnego.

Kreator uruchamiania

Po zakończeniu instalacji postępuj zgodnie z instrukcjami wyświetlanymi na ekranie w kreatorze uruchamiania:

Włączanie uprawnień dla aplikacji ESET Mobile Security

Ten przewodnik jest oparty na domyślnych ustawieniach Androida. Proces włączania uprawnień może się różnić w zależności od producenta urządzenia.

1. Naciśnij pozycję **Kraj** i wybierz odpowiedni kraj.
2. Naciśnij pozycję **Język**, aby wybrać odpowiedni język.
3. Naciśnij pozycję **Dalej** i zaakceptuj Umowę licencyjną użytkownika końcowego i Politykę prywatności.
4. W razie potrzeby zezwól na następujące opcje i naciśnij przycisk **Dalej**.

- **Zezwól ESET LiveGrid©** — aby dowiedzieć się więcej na temat **ESET LiveGrid©**, odwiedź sekcję Ustawienia zaawansowane.
- **Zezwól analitykom na ulepszanie naszych produktów**—ESET Mobile Security będzie przesyłać anonimowe informacje o aplikacji (dane dotyczące wydajności, statystyki działania), które pomogą nam w doskonaleniu aplikacji i usług. Aby dowiedzieć się więcej o gromadzonych przez nas informacjach, odwiedź rozdział Polityka prywatności.
- **Zezwalaj na wykorzystanie danych do celów marketingowych**

5. Sprawdź szczegóły aktywacji po instalacji ESET Mobile Security, korzystając z łącza pobierania wysłanego na Twój adres e-mail z konta ESET HOME. Naciśnij **Kontynuuj** i postępuj zgodnie z instrukcjami, aby

aktywować ESET Mobile Security z poziomu konta ESET HOME. Jeśli nie wyrażasz zgody, naciśnij **Odrzuć** i wykonaj poniższe czynności.

6. Zaloguj się na swoje konto ESET HOME, aby połączyć urządzenie mobilne z kontem i aktywować aplikację ESET Mobile Security.

Kontynuuj za pomocą konta Google.

a.Wybierz swoje konto Google.
b.Jeśli łączysz się po raz pierwszy z istniejącym kontem ESET HOME za pomocą konta Google, zostanie wyświetlony monit o wpisanie hasła ESET HOME. Naciśnij pozycję **Potwierdź hasło**.

Kontynuuj za pomocą Apple ID.

a.Wpisz swój identyfikator Apple ID i hasło.
b.Naciśnij pozycję **Zaloguj się**.
c.Wpisz kod wysłany na urządzenie Apple.
d.Naciśnij pozycję **Kontynuuj**.
e.Jeśli ufasz przeglądarce internetowej, kliknij pozycję **Zaufaj**.
f.Naciśnij **Kontynuuj,** aby uzyskać dostęp do konta ESET HOME za pomocą konta Apple ID.
g.Naciśnij ikonę **X** w lewym górnym rogu, aby powrócić do ESET Mobile Security.

Zeskanuj kod QR

Ta opcja wymaga innego urządzenia z aplikacją ESET HOME.
a.Otwórz aplikację ESET HOME na innym urządzeniu.

b.Naciśnij przycisk menu ☰ > **Skanuj kod QR**.
c.Naciśnij **Zeskanuj kod QR**. Może zostać wyświetlony monit o zezwolenie aplikacji ESET HOME na robienie zdjęć i nagrywanie filmów. Naciśnij opcję **Podczas korzystania z aplikacji** lub **Tylko tym razem**.
d.Użyj aparatu, aby zeskanować kod QR.
e.Naciśnij **Podłącz urządzenie**.
f.Naciśnij przycisk **Zakończ**w programie ESET Mobile Security.

Utwórz konto lub zaloguj się

Utwórz konto ESET HOME
a.Wprowadź swój adres e-mail i hasło.

> **Wymagania dotyczące hasła**
> Hasło musi składać się z co najmniej 10 znaków i zawierać co najmniej jedną małą literę, jedną wielką literę i jedną cyfrę.

b.Naciśnij **Utwórz konto**, a otrzymasz link potwierdzający za pośrednictwem poczty e-mail.
c.Nazwij swoje urządzenie i naciśnij **Dalej**.
d.Aby program ESET Mobile Security działał poprawnie, dotknij przycisku **Kontynuuj** i zezwól na uprawnienie Dostęp do wszystkich plików.
e.Dotknij przycisku **Rozpocznij pierwsze skanowanie**.
f.Aby dokończyć rejestrację, naciśnij link w wiadomości e-mail z potwierdzeniem.
Zaloguj się w ESET HOME
a.Dotknij opcji **Zaloguj się** pod przyciskiem **Utwórz konto**.
b.Wpisz swój adres e-mail i hasło.
c.Naciśnij pozycję **Zaloguj się**.
Po zalogowaniu się na swoje konto ESET HOME musisz utworzyć nazwę urządzenia. Ułatwi to jego identyfikację na koncie ESET HOME. Wprowadź nazwę i naciśnij przycisk **Dalej**.

Pomiń

Jeśli nie posiadasz konta ESET HOME lub nie chcesz łączyć urządzenia mobilnego z kontem ESET HOME, kliknij **Pomiń**. Możesz zalogować się na swoje konto ESET HOME później w aplikacji ESET Mobile Security. Jeśli pominiesz ten krok, zostanie wyświetlony monit o wybranie konta e-mail, na które będą przesyłane informacje o rejestracji licencji ESET oraz wiadomości od działu pomocy technicznej. Naciśnij pozycję **Wybierz adres e-mail**, aby wyświetlić listę dostępnych kont e-mail. Na liście kont wybierz adres e-mail lub naciśnij pozycję **Dodaj konto** w celu dodania nowego konta e-mail do urządzenia. Naciśnij pozycję **OK**, aby kontynuować. Aby użyć innego konta e-mail bez dodawania konta do urządzenia, naciśnij kolejno pozycje **Wybierz adres e-mail** > **Anuluj**. Powtórz ten proces dwukrotnie. Wpisz adres e-maill i naciśnij pozycję **Dalej**, aby kontynuować.

7. Ostatnie kroki kreatora uruchamiania różnią się w zależności od wersji Androida na urządzeniu.

Android 6–10

a.Aby włączyć skanowanie urządzeń, ESET Mobile Security wymaga wielu uprawnień. Na ekranie **Zezwól na dostęp** zapoznaj się z uprawnieniami dla programu ESET Mobile Security i naciśnij przycisk **Kontynuuj**.
b.Naciśnij pozycję **Zezwól**, aby zezwolić na dostęp programu ESET Mobile Security. W przypadku wybrania pozycji **Pomiń** program ESET Mobile Security nie będzie mógł skanować urządzenia pod kątem zagrożeń do momentu przyznania uprawnień i wyświetlane będzie powiadomienie o naruszeniu zabezpieczeń.

Android 11 i późniejsze wersje

a.Naciśnij pozycję **Kontynuuj**.
b.Wybierz ESET Mobile Security.
c.Włącz przełącznik obok nazwy programu ESET Mobile Security.
d.Kreator uruchamiania został ukończony. Naciśnij opcję **Rozpocznij pierwsze skanowanie**.

Ochrona baterii

Wielu producentów urządzeń wprowadziło funkcję ochrony baterii lub opcje oszczędzania baterii w urządzeniach z systemem Android 6 i jego nowszych wersjach. Włączenie tej funkcji powoduje wyłączenie ochrony Anti-Phishing w programie ESET Mobile Security. W przypadku urządzeń z tą funkcją trzeba utworzyć wyjątek, aby ochrona przed atakami typu „phishing” dostępna w programie ESET Mobile Security mogła działać przy włączonej opcji oszczędzania baterii. Aby utworzyć wyjątek, skorzystaj z dokumentacji producenta urządzenia.

Odinstalowanie

Program ESET Mobile Security można odinstalować przy użyciu kreatora **odinstalowywania** dostępnego w menu głównym programu ESET Mobile Security.

Uwaga

Odinstalowanie ESET Mobile Security zwolni jedno stanowisko z licencji.

1.Naciśnij Menu ☰.

2.Naciśnij przycisk **Ustawienia**.

3.Naciśnij przycisk **Odinstaluj**.

4.Jeśli ochrona Anti-Theft jest włączona, zostanie wyświetlona prośba, aby wprowadzić numer PIN lub zeskanować odcisk palca zabezpieczający program ESET Mobile Security.

5.Naciśnij przycisk **Odinstaluj**.

Można też wykonać poniższe kroki, aby ręcznie odinstalować produkt:

Android 7 i późniejsze wersje:

1.Wróć do obszaru Ustawienia i naciśnij pozycję **Zarządzaj aplikacjami** > **ESET Mobile Security** > **Odinstaluj**. Jeśli ochrona Anti-Theft jest włączona, może zostać wyświetlony monit z prośbą o dezaktywowanie administratora urządzenia w aplikacji ESET Mobile Security przed odinstalowaniem.

Lub

1.W programie ESET Mobile Security dotknij przycisku menu głównego , aby otworzyć menu główne.

2.Wybierz pozycję **Ustawienia**.

3.Naciśnij przycisk **Odinstaluj**.

4.Naciśnij przycisk **Odinstaluj** jeszcze raz, aby potwierdzić wybór.

Android 6:

1.Naciśnij ikonę programu uruchamiającego na ekranie głównym systemu Android (lub przejdź do pozycji **Ekran** główny > **Menu**) i naciśnij kolejno pozycje **Ustawienia** > **Zabezpieczenia** > **Administratorzy urządzenia**. Wybierz pozycję **ESET Mobile Security** i naciśnij pozycję **Dezaktywuj**. Naciśnij pozycję **Odblokuj** i wprowadź numer PIN lub zeskanuj odcisk palca. Możesz pominąć ten krok, jeśli aplikacja nie jest już zdefiniowana jako administrator urządzenia.

2.Wróć do obszaru **Ustawienia** i naciśnij kolejno pozycje **Zarządzaj aplikacjami** > **ESET Mobile Security** > **Odinstaluj**.

Łączenie z ESET HOME

Aby użyć tej funkcji, uaktualnij aplikację ESET Mobile Security do wersji 6.3 lub nowszej.

> **Aktywacja ESET Mobile Security poprzez ESET HOME**
> Jeśli chcesz aktywować jedno urządzenie poprzez ESET HOME po raz drugi (na przykład po ponownej instalacji programu ESET Mobile Security), musisz najpierw ręcznie usunąć urządzenie z licencji ESET HOME. W przeciwnym razie nie będzie można aktywować tego urządzenia z poziomu ESET HOME.

Łączenie urządzenia z istniejącym kontem ESET HOME

1. Naciśnij przycisk menu .
2. Naciśnij **konto ESET HOME**.

Kontynuuj za pomocą konta Google.

a.Wybierz swoje konto Google.
b.Jeśli łączysz się po raz pierwszy z istniejącym kontem ESET HOME za pomocą konta Google, zostanie wyświetlony monit o wpisanie hasła ESET HOME. Naciśnij pozycję **Potwierdź hasło**.

Kontynuuj za pomocą Apple ID.

a.Wpisz swój identyfikator Apple ID i hasło.
b.Naciśnij pozycję **Zaloguj się**.
c.Wpisz kod wysłany na urządzenie Apple.
d.Naciśnij pozycję **Kontynuuj**.
e.Jeśli ufasz przeglądarce internetowej, kliknij pozycję **Zaufaj**.
f.Naciśnij **Kontynuuj,** aby uzyskać dostęp do konta ESET HOME za pomocą konta Apple ID.
g.Naciśnij ikonę **X** w lewym górnym rogu, aby powrócić do ESET Mobile Security.

Zeskanuj kod QR

Ta opcja wymaga innego urządzenia z aplikacją ESET HOME.
a.Otwórz aplikację ESET HOME na innym urządzeniu.
b.Naciśnij przycisk menu > **Skanuj kod QR**.
c.Naciśnij **Zeskanuj kod QR**. Może zostać wyświetlony monit o zezwolenie aplikacji ESET HOME na robienie zdjęć i nagrywanie filmów. Naciśnij opcję **Podczas korzystania z aplikacji** lub **Tylko tym razem**.
d.Użyj aparatu, aby zeskanować kod QR.
e.Naciśnij **Podłącz urządzenie**.
f.Naciśnij przycisk **Zakończ**w programie ESET Mobile Security.

Kontynuuj przy użyciu adresu e-mail

a.Wprowadź swój adres e-mail i hasło.
b.Naciśnij pozycję **Zaloguj się**.

3. Jeśli logujesz się na swoje konto ESET HOME po raz pierwszy na tym urządzeniu, nazwij urządzenie, aby ułatwić jego identyfikację w programie ESET HOME. Naciśnij pozycję **Dalej**.

4. Jeśli korzystasz z licencji darmowej lub testowej i masz dostępną licencję w ESET HOME, pojawi się propozycja aktywacji ESET Mobile Security.

a.Wybierz stosowną licencję.

b.Naciśnij pozycję **Aktywuj**

5. Naciśnij przycisk **Zakończ**.

Utwórz konto ESET HOME i podłącz do niego urządzenie

1. Naciśnij przycisk menu .

2. Naciśnij **konto ESET HOME**.

3. Naciśnij **Utwórz konto**.

4. Wprowadź swój adres e-mail i hasło.



Wymagania dotyczące hasła

Hasło musi mieć co najmniej 10 znaków i zawierać co najmniej jedną małą literę, jedną wielką literę i jedną cyfrę.

5. Naciśnij **Utwórz konto**, a otrzymasz link potwierdzający za pośrednictwem poczty e-mail.

6. Nazwij swoje urządzenie i naciśnij **Dalej**.

7. Aby program ESET Mobile Security działał poprawnie, dotknij przycisku **Kontynuuj** i zezwól na uprawnienie Dostęp do wszystkich plików.

8. Dotknij przycisku **Rozpocznij pierwsze skanowanie**.

9. Aby dokończyć rejestrację, naciśnij link w wiadomości e-mail z potwierdzeniem.

Odłączanie urządzenia od konta ESET HOME

1. Naciśnij przycisk menu ☰.

2. Naciśnij **konto ESET HOME**.

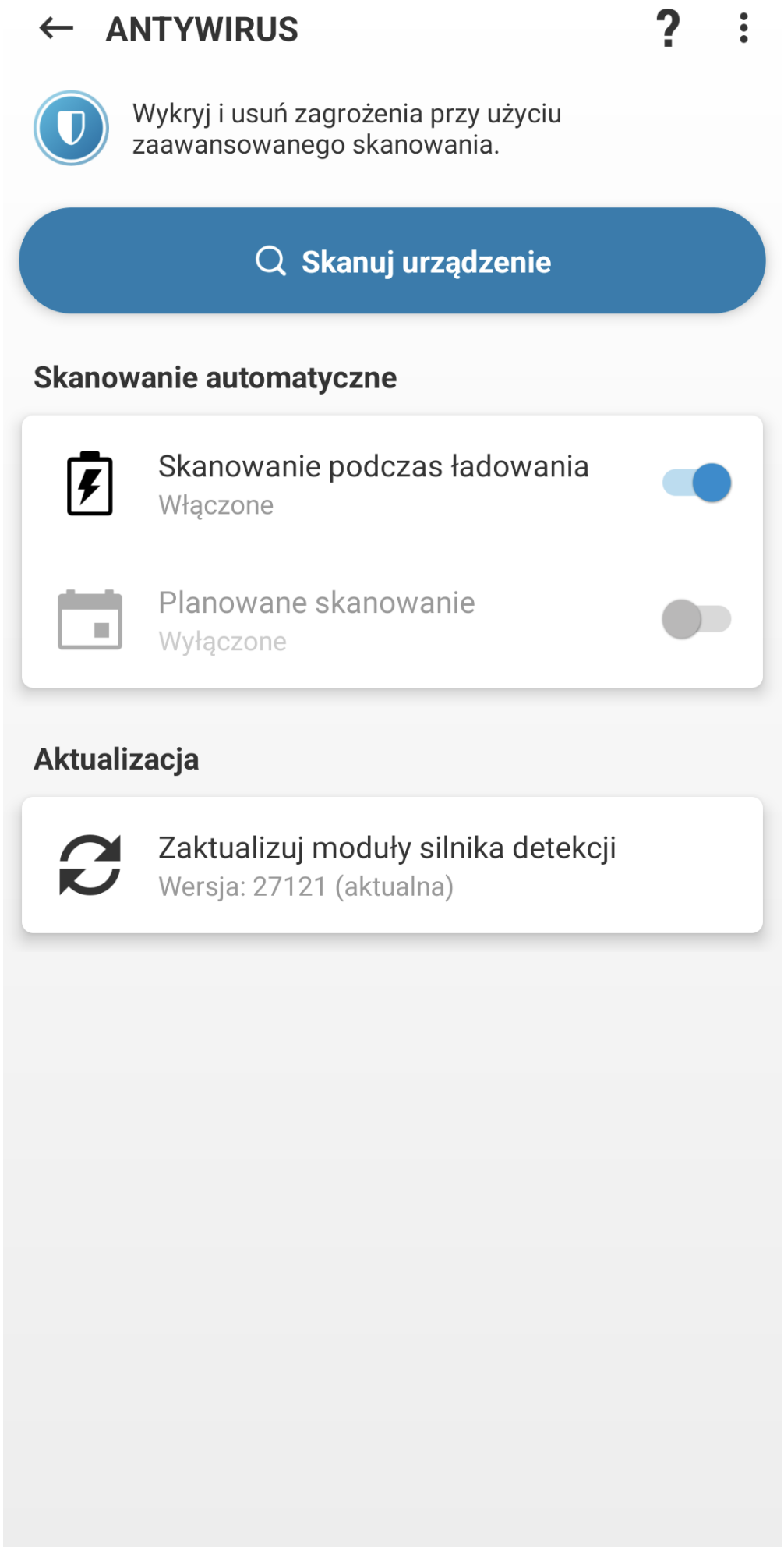
3. Naciśnij **Odłącz urządzenie**. Jeśli urządzenie nie zostało podłączone do konta ESET HOME, ta opcja jest niedostępna.

4. Użyj odcisku palca lub wpisz kod PIN.

5. Naciśnij **Odłącz**.

Antywirus

Moduł Antywirus chroni urządzenie przed szkodliwym kodem, blokując pojawiające się zagrożenia i usuwając je.


ANTYWIRUS
Wykryj i usuń zagrożenia przy użyciu zaawansowanego skanowania.
Skanuj urządzenie
Skanowanie automatyczne
Skanowanie podczas ładowania
Włączone
Planowane skanowanie
Wyłączone
Aktualizacja
Zaktualizuj moduły silnika detekcji
Wersja: 27121 (aktualna)

Ochrona w czasie rzeczywistym

Funkcja ochrony systemu plików w czasie rzeczywistym kontroluje wszystkie pliki w folderach pobierania pod kątem złośliwego kodu po ich otwarciu, utworzeniu lub uruchomieniu.

Domyślnie ochrona systemu plików w czasie rzeczywistym jest uruchamiana wraz z uruchomieniem systemu i zapewnia nieprzerwane skanowanie. Nie zalecamy wyłączania opcji Włącz ochronę systemu plików w czasie rzeczywistym w sekcji **Antywirus**. Jeśli musisz przejść do ustawień Ochrony w czasie rzeczywistym, naciśnij przycisk z trzema kropkami ⋮ w sekcji **Antywirus** > **Ustawienia zaawansowane** > **Ochrona w czasie rzeczywistym**.

Skanowanie urządzenia

Skanowanie na żądanie można wykonać w dowolnym momencie, dotykając przycisku **Skanuj urządzenie** w sekcji **Antywirus**. Domyślnie poziom skanowania jest ustawiony na Skanowanie inteligentne. Poziom skanowania można zmienić w **Ustawieniach zaawansowanych** programu antywirusowego. Naciśnij przycisk z trzema kropkami ⋮ > **Ustawienia zaawansowane** > **Poziom skanowania**.

Do wyboru są dwa poziomy skanowania:

- **Inteligentne** — umożliwia skanowanie zainstalowanych aplikacji, plików DEX (plików wykonywalnych systemu operacyjnego Android), plików SO (bibliotek) oraz archiwów przy maksymalnej głębokości skanowania sięgającej 3 archiwów zagnieżdżonych, a także zawartości kart SD.
- **Dokładne** — obejmuje wszystkie typy plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

Krótkie podsumowanie jest zapisywane w dzienniku dostępnym w sekcji Dzienniki skanowania. Aby przerwać trwające skanowanie, wybierz pozycję **Anuluj**. Wyniki i statystyki skanowania są wyświetlane podczas skanowania na panelu ustawień **skanujochrony antywirusowej**.

> **Skanowanie kart pamięci**
> ESET Mobile Security nie obsługuje skanowania kart pamięci na urządzeniach z systemem Android 6 i starszymi wersjami.

Nierozwiązane zagrożenia

Kiedy ESET Mobile Security wykryje zagrożenie, ta opcja będzie dostępna, dopóki nie wybierzesz reakcji na zagrożenie. Dostępne działania to usunięcie zagrożenia lub zignorowanie go.

Ignoruj zagrożenia

Jeżeli zdecydujesz się zignorować zagrożenie, pojawi się opcja **Ignoruj zagrożenia**. Ta opcja nadal będzie umożliwiać późniejsze usunięcie zignorowanego zagrożenia.

Skanowanie podczas ładowania

Po wybraniu tej opcji skanowanie jest uruchamiane automatycznie, gdy urządzenie jest w stanie bezczynności, a

ponadto jest w pełni naładowane i podłączone do ładowarki.

Planowane skanowanie

Planowane skanowanie umożliwia zaplanowanie skanowania urządzenia, aby było uruchamiane w ustalonym czasie. Aby zaplanować skanowanie, naciśnij przełącznik obok opcji **Planowane skanowanie** i określ daty oraz godziny uruchomienia skanowania.

Zaktualizuj moduły wykrywania

Domyślnie ESET Mobile Security zawiera zadanie zapewniające regularne aktualizowanie programu. Aby uruchomić aktualizację ręcznie, dotknij pozycji **Aktualizuj moduły wykrywania**.

> **Opłaty za transmisję danych**
> Aby zapobiec niepotrzebnemu wykorzystywaniu przepustowości, aktualizacje są publikowane w razie potrzeby. Aktualizacje są bezpłatne, chociaż operator sieci komórkowej może naliczać opłaty za transfer danych.

Więcej informacji na temat skanowania można uzyskać po kliknięciu poniższych linków:

- Dzienniki skanowania
- Ustawienia zaawansowane

Dzienniki skanowania

Sekcja Dzienniki skanowania zawiera szczegółowe dane na temat każdego zaplanowanego skanowania lub ręcznie uruchomionego skanowania urządzenia.

Zawartość każdego dziennika:

- Data i godzina skanowania
- Poziom skanowania (Inteligentne lub Dokładne)
- Czas trwania skanowania
- Liczba przeskanowanych plików
- Wyniki skanowania lub błędy napotkane w trakcie skanowania
- Liczba znalezionych zagrożeń i lista znalezionych zagrożeń

Ustawienia zaawansowane

Otwórz aplikację ESET Mobile Security i naciśnij ikonę menu ☰ > **Antywirus** > trzy kropki w prawym górnym rogu ⋮ > **Ustawienia zaawansowane**.

Poziom skanowania

Do wyboru są dwa poziomy skanowania:

- **Inteligentne** — umożliwia skanowanie zainstalowanych aplikacji, plików DEX (plików wykonywalnych systemu operacyjnego Android), plików SO (bibliotek) oraz archiwów przy maksymalnej głębokości skanowania sięgającej 3 archiwów zagnieżdżonych, a także zawartości kart SD.

- **Dokładne** — obejmuje wszystkie typy plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

Ochrona w czasie rzeczywistym

Skaner działający w czasie rzeczywistym uruchamia się automatycznie wraz z systemem i skanuje znajdujące się w nim pliki. Automatycznie skanuje folder pobierania oraz zainstalowane lub zaktualizowane aplikacje.

System reputacji ESET LiveGrid©

ESET LiveGrid© to system zapobiegający przed zagrożeniami, który zapewnia urządzeniu dodatkową ochronę. Stale monitoruje ona programy i procesy uruchamiane przez system, wykorzystując dane zebrane od milionów użytkowników produktów. Dzięki temu możemy oferować wszystkim użytkownikom produktów firmy ESET lepszą i bardziej precyzyjną ochroną proaktywną oraz szybsze skanowanie. Zalecamy włączenie tej funkcji.

System informacji zwrotnych ESET LiveGrid©

Ten system informacji zwrotnej umożliwia nam gromadzenie anonimowych statystyk, raportów o awariach i danych diagnostycznych dotyczących podejrzanych obiektów. Informacje te przetwarzamy automatycznie w celu tworzenia mechanizmu detekcji w chmurze.

Nośniki wymienne

ESET Mobile Security skanuje wszystkie nośniki wymienne podłączone do urządzenia (pamięci USB Flash, zewnętrzne dyski twarde itp.).

Wykryj potencjalnie niepożądane aplikacje

Potencjalnie niepożądana aplikacja jest programem zawierającym oprogramowanie typu adware powodującym instalowanie pasków narzędzi, śledzącym wyniki wyszukiwania lub mającym niejasne działanie. W niektórych sytuacjach może się okazać, że korzyści oferowane przez potencjalnie niepożądaną aplikację przeważają nad ryzykiem. Z tego powodu firma ESET przydziela takim aplikacjom kategorię niskiego ryzyka, aby je odróżnić od szkodliwego oprogramowania.

Wykryj potencjalnie niebezpieczne aplikacje

Istnieje wiele uznanych aplikacji, które mają na celu ułatwianie zarządzania urządzeniami pracującymi w sieci. Obejmuje ona takie programy, jak narzędzia do zdalnego dostępu, aplikacje do łamania haseł i programy rejestrujące znaki wprowadzane na klawiaturze. Potencjalnie niebezpieczne aplikacje to kategoria, do której należą niektóre legalne programy komercyjne. W nieodpowiednich rękach aplikacje te mogą być wykorzystywane do nieuprawnionych działań. Włączenie opcji **Wykryj potencjalnie niebezpieczne aplikacje** umożliwia

monitorowanie aplikacji tej kategorii i blokowanie ich zgodnie z uznaniem użytkownika.

Serwer aktualizacji

Ta opcja umożliwia włączenie aktualizacji urządzenia z **serwera wersji wstępnych**. Przedpremierowe aktualizacje przeszły gruntowne testy wewnętrzne i wkrótce będą dostępne publicznie. Możesz skorzystać z dostępu do najnowszych poprawek i metod wykrywania zagrożeń. Aktualizacje te mogą jednak nie zawsze działać stabilnie. Aby sprawdzić wersje bieżących modułów programu, dotknij ikony trzech kropek ⋮ na ekranie głównym programu ESET Mobile Security, a następnie dotknij kolejno pozycji **Informacje** > **ESET Mobile Security**. Zalecamy, aby użytkownicy podstawowi pozostawili domyślnie zaznaczoną opcję **Zwolnij serwer**.

Adware Detector

Funkcja Adware Detector jest odpowiedzią firmy ESET na aplikacje typu adware. Aplikacje typu adware mogą być faktycznymi aplikacjami (jak np. kalkulator lub latarka) lub tylko je udawać. Ich działanie opiera się na wyświetlaniu pełnoekranowych reklam nawet wtedy, gdy aplikacja jest zamknięta. W związku z tym użytkownik nie może zlokalizować, która aplikacja jest odpowiedzialna za wyświetlanie reklam.

Funkcja Adware Detector pomaga zidentyfikować aplikacje typu adware. Aby z niej korzystać, po pojawieniu się ekranu z reklamą wykonaj następujące czynności:

1. Otwórz ESET Mobile Security.
2. Na ekranie głównym aplikacji ESET Mobile Security naciśnij pozycję **Antywirus**.
3. Naciśnij ⋮ w prawym górnym rogu, aby wyświetlić menu.
4. W menu naciśnij **Adware Detector**.
5. Po wyświetleniu przez Adware Detector przewodnika dotyczącego wykrywania aplikacji typu adware naciśnij przycisk **Kontynuuj**.

Funkcja Adware Detector wyświetli aplikacje, które zostały uruchomione w ciągu ostatnich pięciu minut. Zidentyfikuj podejrzane aplikacje i naciśnij **Usuń**, aby usunąć je z urządzenia. Podejrzana aplikacja to zwykle ta, która nie powinna być otwarta lub nie była używana w tej chwili.

Raport zabezpieczeń

Ekran Raport zabezpieczeń udostępnia szczegółowy przegląd każdego modułu programu wraz z jego statusem i statystykami. Na ekranie **Raport zabezpieczeń** można też włączyć moduły, które nie są obecnie używane. Każda sekcja modułu programu zawiera następujące informacje.

Jeśli brakuje niektórych informacji, oznacza to, że było zero wystąpień.

Antywirus

- Skano\u00ADwa\u00ADnia aplikacji
- Znalezione zagrożenia

- Aktualizacje bazy danych
- Wykryto zagrożenie
- Przeskanowane pliki
- Zaktualizowane aplikacje

Blokada aplikacji

- Liczba chronionych aplikacji
- Liczba udanych odblokowań aplikacji
- Liczba nieudanych prób odblokowania

Anti-Phishing

- Przeskanowane łącza
- Przeskanowane powiadomienia
- Wykryte zagrożenia

Filtr połączeń

- Połączenia wychodzące
- Odebrane połączenia
- Zablokowane połączenia

Ochrona płatności

- Liczba chronionych aplikacji
- Liczba przeskanowań chronionych aplikacji
- Liczba znalezionych problemów
- Liczba uruchomień aplikacji bankowej lub płatniczej z poziomu aplikacji Bezpieczne uruchamianie

Audyt zabezpieczeń

- Alerty roamingowe wskazują liczbę ostrzeżeń o nawiązaniu połączenia z siecią roamingową
- Ostrzeżenia dotyczące otwartej sieci WI-FI

Inspekcja sieci

- Skanowania sieci
- Urządzenia znalezione w sieci
- Wykryte luki w zabezpieczeniach

ESET Mobile Security co miesiąc wyświetla krótki miesięczny raport w postaci komunikatu na pasku powiadomień systemu Android. Aby nie otrzymywać tych powiadomień, włącz opcję **Nie pokazuj powiadomienia o miesięcznym raporcie**.

Dziennik aktywności

Dziennik aktywności wyświetla codzienną aktywność aplikacji ESET Mobile Security na ekranie głównym ESET Mobile Security. Dziennik aktywności zawiera informacje o witrynach internetowych przeskanowanych przez aplikację ESET Mobile Security, aktualizacjach aplikacji ESET Mobile Security oraz aktualizacjach innych aplikacji, zainstalowanych aplikacjach, skanowaniach przeprowadzonych przez ESET Mobile Security itp.

Aby wyświetlić pełną historię dziennika aktywności, dotknij **>** ikony obok dziennika aktywności. W pełnym raporcie Dziennik aktywności można użyć filtrów do filtrowania działań według stanu lub funkcji ESET Mobile Security. Przykład: Ostrzeżenie, Ryzyko, Anti-Theft i Licencja. Można również filtrować działania według daty wystąpienia według najnowszych lub najstarszych.

Aby wyczyścić historię Dziennika aktywności:

1. Otwórz ESET Mobile Security.
2. Przesuń palcem w dół na ekranie głównym.
3. Dotknij **>** ikony obok **dziennika aktywności**.
4. Naciśnij ikonę menu .
5. Naciśnij pozycję **Wyczyść wszystko**.

Aby usunąć poszczególne rekordy z historii w Dzienniku aktywności:

1. Otwórz ESET Mobile Security.
2. Przesuń palcem w górę na ekranie głównym.
3. Dotknij **>** ikony obok **dziennika aktywności**.
4. Przesuń odpowiedni rekord w lewo.
5. Naciśnij opcję **Usuń**.

Funkcja Anti-Theft

Funkcja ESET Anti-Theft chroni urządzenie mobilne przed nieupoważnionym dostępem, umożliwia monitorowanie obcych działań oraz określa lokalizację urządzenia. W przypadku zgubienia urządzenia funkcja umożliwia również wyświetlanie wiadomości dla znalazcy.

ESET Anti-Theft wymaga następujących uprawnień:

- Dostęp do kamery w celu zrobienia zdjęć intruzowi.
- Dostęp do edycji plików w celu zdalnego usuwania poufnych danych.
- Dostęp do danych o lokalizacji, aby namierzyć urządzenie w przypadku jego zaginięcia.
- Dostęp do informacji o aktywności fizycznej, aby rozpoznać, kiedy urządzenie jest przenoszone.
- Dostęp do danych o lokalizacji w tle śledzenie urządzenia w przypadku jego zaginięcia, nawet gdy program ESET Mobile Security jest zamknięty lub nieużywany. Udzielając tego uprawnienia, wybierz opcję **Zezwalaj przez cały czas**, aby zapewnić pełną ochronę.
- Uprawnienia dostępu do informacji o użyciu, aby zezwolić na odbieranie połączeń na urządzeniu, jeśli zostanie zablokowane.
- Dostęp administratora urządzenia, aby zapobiec nieautoryzowanej dezinstalacji ESET Mobile Security. Po aktywowaniu administratora urządzenia zostaniesz poproszony o utworzenie kodu PIN w celu ochrony ważnych ustawień w programie ESET Mobile Security.
- Dostęp do informacji o telefonie, aby wykryć wyjęcie karty SIM. Twoje urządzenie zostanie zablokowane po wyjęciu karty SIM.

Aby skonfigurować ochronę Anti-Theft w aplikacji ESET Mobile Security, przeczytaj artykuł z bazy wiedzy „Konfigurowanie ochrony Anti-Theft w aplikacji ESET Mobile Security dla systemu Android”. (Artykuły z bazy wiedzy nie są dostępne we wszystkich językach).

Automatyczna blokada urządzenia

Poza blokowaniem urządzenia z poziomu portalu ESET HOME można skonfigurować program ESET Mobile Security, aby automatyczne blokował urządzenia po wykonaniu jednej z następujących czynności:

- **Wyjęcie karty SIM** — urządzenie zostanie zablokowane w przypadku wyjęcia zaufanej karty SIM. Aby wyjąć i sprawdzić jedną z zaufanych kart SIM, naciśnij pozycję **Zarządzaj zaufanymi kartami SIM**, wybierz kartę SIM, którą chcesz wyjąć, a następnie naciśnij ikonę kosza . Aby dodać zaufaną kartę SIM, włóż kartę SIM do urządzenia. Jeśli automatyczna blokada urządzenia jest włączona, odblokuj urządzenie. ESET Mobile Security wyświetli monit o potwierdzenie, że nowa karta SIM jest zaufana.

> **Dostępność funkcji automatycznej blokady po wyjęciu karty SIM**
> - Funkcja automatycznej blokady urządzenia po wyjęciu karty SIM nie jest dostępna na urządzeniach obsługiwanych wyłącznie przy użyciu technologii CDMA, WCDMA lub WiFi.

- **[X] nieudanych prób odblokowania** — po włączeniu tej funkcji urządzenie będzie automatycznie blokowane po ustalonej liczbie nieudanych prób odblokowania. Dozwoloną liczbę prób można zmienić w ustawieniach

funkcji Anti-Theft. W przypadku nieudanego odblokowania wskutek pomyłki można podać prawidłowe hasło w ciągu 30 sekund. Dostępny czas można zmienić w pozycji **Czas na poprawienie** w ustawieniach funkcji Anti-Theft. Można również całkowicie wyłączyć czas na poprawienie — urządzenie będzie wtedy blokowane natychmiast po ustalonej liczbie nieudanych prób odblokowania.

Gdy urządzenie jest zablokowane, można wyświetlić informację umożliwiającą skontaktowanie się z właścicielem urządzenia. Także pozwolić urządzeniu na robienie za pomocą obu aparatów zdjęć osób próbujących odblokować urządzenie.

Po zablokowaniu urządzenia

Gdy Twoje urządzenie zostanie zablokowane, możesz ustawić, aby zostały wykonane następujące czynności:

- Opcja **Pokaż dane kontaktowe** wyświetla dane **Właściciela kontaktu** po wprowadzeniu błędnego kodu blokady ekranu. Dotknij opcji **Edytuj dane kontaktowe**, aby wpisać dane kontaktowe wyświetlane po utracie urządzenia. Twój adres e-mail ESET HOME jest wpisywany domyślnie.

- Opcja **Zrób zdjęcie** zapisuje zdjęcia z tylnego i przedniego aparatu w Galerii urządzenia i portalu Anti-Theft w przypadku nieudanej próby odblokowania lub usunięcia karty SIM.

Jak odblokować urządzenie mobilne

Jeśli urządzenie mobilne zostało zablokowane za pośrednictwem portalu ESET Anti-Theft lub program ESET Mobile Security for Android zablokował urządzenie mobilne, potrzebny będzie dostęp do hasła do ESET HOME.

> **Odblokowywanie urządzenia zarządzanego przez kogoś innego**
> Jeśli ESET Mobile Security for Android jest zarządzane przez konto ESET HOME innej osoby, wpisz hasło do tego konta, aby odblokować urządzenie.

Instrukcje wizualne dotyczące odblokowywania urządzenia mobilnego można znaleźć w następującym artykule bazy wiedzy firmy ESET (dostępnym w języku angielskim i kilku innych językach).

Ustawienia funkcji Anti-Theft

Zablokuj po nieudanych próbach

Wybierz liczbę dozwolonych nieudanych prób odblokowania, po których urządzenie zostanie zablokowane. Aby ustawić liczbę prób odblokowania, naciśnij przycisk ⋮ na ekranie usługi Anti-Theft, wybierz **Ustawienia**, a następnie naciśnij pozycję **Zablokuj po nieudanych próbach** i wybierz liczbę dozwolonych prób.

Czas na poprawienie

Jeśli włączono funkcję "Zablokuj po nieudanych próbach", urządzenie będzie blokowane po wybranej liczbie nieudanych prób odblokowania. Wyłącz funkcję "Czas na poprawienie", aby urządzenie było blokowane natychmiast po wybranej liczbie nieudanych prób odblokowania, lub ustaw czas na odblokowanie urządzenia zanim zostanie ono zablokowane po wybranej liczbie nieudanych prób.

Przykład

Funkcja **Zablokuj po nieudanych próbach** jest włączona, a liczba dozwolonych nieudanych prób to 3. **Czas na poprawienie** jest ustawiony na 15 sekund.
Po trzykrotnym narysowaniu nieprawidłowego wzoru odblokowania użytkownik ma 15 sekund na narysowanie prawidłowego wzoru — w przeciwnym razie ESET Mobile Security zablokuje urządzenie.

Edytuj dane kontaktowe

Jeśli urządzenie zostanie oznaczone jako zgubione w portalu ESET Anti-Theft lub zablokowane po przekroczeniu liczby dozwolonych prób odblokowania, informacje z sekcji **Szczegóły kontaktu** zostaną wyświetlone na ekranie zablokowanego urządzenia, aby pomóc jego znalazcy skontaktować się z Tobą.

Te informacje mogą obejmować następujące elementy:

- Wyświetlany komunikat (opcjonalnie)
- Nazwa (opcjonalnie)
- Numer telefonu (inny niż własny)
- Adres e-mail (opcjonalnie)

Zarządzaj zaufanymi kartami SIM

Ta opcja umożliwia usunięcie lub zmianę nazwy włożonej karty SIM. Aby dodać nową zaufaną kartę SIM, włóż kartę SIM do urządzenia. Urządzenie zostanie zablokowane. Odblokuj urządzenie przy użyciu kodu zabezpieczającego. Zostanie wyświetlony monit o dodanie nowo włożonej karty SIM do listy zaufanych kart SIM. Jeśli nie dodasz tej karty SIM do listy, ochrona SIM pozostanie wyłączona.

Zmień typ blokady

Wybierz sposób odblokowania funkcji ESET Anti-Theft. Podczas konfiguracji funkcji Anti-Theft kod PIN jest ustawiany jako domyślny sposób odblokowania. Można zmienić kod PIN na odblokowywanie za pomocą wzoru.

Użyj odcisku palca

Gdy ta opcja jest włączona, możesz użyć odcisku palca zapisanego w urządzeniu, aby odblokować funkcję Anti-Theft.

Optymalizacja

Optymalizacja przeprowadzana przez funkcję ESET Anti-Theft polega na wymiernej ocenie technicznej stanu bezpieczeństwa urządzenia. Ochrona Anti-Theft sprawdzi system pod kątem problemów wymienionych poniżej.

W przypadku każdego problemu z zabezpieczeniami można nacisnąć pozycję **Zmień ustawienia**, aby przejść na ekran umożliwiający rozwiązanie tego problemu. Jeśli nie chcesz, aby program ESET Mobile Security zgłaszał problem, kliknij **Ignoruj ten problem**.

• **Wyłączone usługi lokalizacji** — aby je włączyć, należy wybrać kolejno pozycje Ustawienia systemu Android > **Usługi lokalizacji** i wybrać pozycję **Używaj sieci bezprzewodowych**.

• **Niekorzystanie z satelitów GPS** — dostęp do odpowiedniego ustawienia jest możliwy po wybraniu kolejno pozycji Ustawienia systemu Android > **Lokalizacja** > **Tryb** > **Wysoka dokładność**.

• **Niezabezpieczona blokada ekranu** — aby zabezpieczyć urządzenie przy użyciu kodu blokady ekranu, hasła, kodu PIN lub wzoru, należy wybrać kolejno pozycje Ustawienia systemu Android > **Zabezpieczenie ekranu ; Blokada ekranu** i wybrać jedną z dostępnych opcji. Większość urządzeń z Androidem oferuje przeciągnięcie, ruch, odblokowywanie twarzą, twarz i głos, wzór, kod PIN lub hasło. Gdy ktoś próbuje odblokować urządzenie z użyciem nieprawidłowego kodu, funkcja ESET Anti-Theft wysyła do użytkownika powiadomienie o podejrzanym działaniu za pośrednictwem portalu ESET HOME.

• **Niewłączona obsługa danych mobilnych** — dostęp do odpowiedniego ustawienia jest możliwy po wybraniu kolejno pozycji Ustawienia systemu Android > **Połączenia bezprzewodowe i sieci** > **Sieci komórkowe** > **Dane**.

• **Brak usług Google Play** — funkcja ESET Anti-Theft używa usług Google Play do dostarczania poleceń na urządzenie w czasie rzeczywistym i wyświetlania powiadomień wypychanych. Jeśli te usługi są wyłączone lub brakuje ich na urządzeniu, zakres funkcji ESET Anti-Theft, którymi można zarządzać w portalu ESET HOME, jest ograniczony.

Portal internetowy

ESET Mobile Security całkowicie integruje się z ochroną ESET Anti-Theft za pośrednictwem nowego portalu ESET HOME. Portal ESET Anti-Theft ten umożliwia monitorowanie aktywności urządzenia, blokowanie urządzenia, wysyłanie niestandardowych wiadomości do znalazcy urządzenia, uruchamianie bardzo głośnego alarmu oraz zdalne usuwanie danych.

Aby utworzyć konto w portalu ESET HOME, naciśnij pozycję **Utwórz nowe konto** i wypełnij formularz rejestracyjny. Sprawdź w skrzynce odbiorczej, czy nadeszła wiadomość e-mail z potwierdzeniem, a następnie kliknij łącze, by aktywować konto. Po aktywacji konta możesz zdalnie zarządzać funkcją bezpieczeństwa ESET Anti-Theft podłączonych urządzeń poprzez portal ESET HOME. Jeśli masz już konto w portalu ESET HOME, naciśnij pozycję **Zaloguj się** i wpisz swój adres e-mail oraz hasło. Po wykonaniu tych czynności będzie można powiązać urządzenie z kontem w portalu ESET HOME.

Dalsze informacje na temat korzystania z funkcji ESET Anti-Theft znajdziesz w podręczniku użytkownika funkcji Anti-Theft. Możesz też nacisnąć pozycję **Pomoc** w prawym górnym rogu portalu ESET HOME.

ESET HOME hasło

Aby zmienić zapomniane hasło:

1.Otwórz witrynę https://login.eset.com/LostPassword.

2.Wpisz adres e-mail użyty do rejestracji w portal ESET HOME i kliknij przycisk **Wyślij**.

3.Zaloguj się na swoje konto e-mail, otwórz wiadomość e-mail o tytule **Resetowanie hasła do konta ESET HOME** i kliknij link znajdujący się w tej wiadomości.

4.Wprowadź i potwierdź nowe hasło, a następnie kliknij przycisk **Potwierdź zmianę**.

5.Wprowadź nowe hasło na urządzeniu i naciśnij przycisk **Odblokuj,** aby odblokować urządzenie.

Zmień hasło do konta ESET HOME:

1.Przejdź do witryny ESET HOME.

2.Zaloguj się, podając swój adres e-mail i bieżące hasło.
3.Kliknij swój adres e-mail obok strzałki skierowanej w dół znajdującej się w prawym górnym rogu.
4.Kliknij pozycję **Zmień hasło**.

5.Wpisz bieżące hasło.

6.Wpisz nowe hasło i potwierdź je.

7.Kliknij pozycję **Zapisz zmiany**.

Anti-Phishing

Termin phishing określa przestępczą działalność polegającą na skłanianiu użytkowników do podania informacji poufnych w witrynie internetowej, która udaje prawdziwą, ale taka nie jest. Ten rodzaj manipulacji jest znany jako pod pojęciem inżynierii społecznej. Phishingu często używa się, aby uzyskać dostęp do poufnych danych, na przykład numerów kont bankowych, numerów kart płatniczych, numerów PIN oraz nazw użytkowników i haseł.

Funkcja Anti-Phishing w programie ESET Mobile Security chroni przed witrynami uznanymi za szkodliwe lub niebezpieczne.

Zalecamy pozostawienie włączonej funkcji **Ochrona przed atakami typu „phishing”**. Po jej włączeniu wszystkie potencjalne ataki typu „phishing” pochodzące z witryn internetowych lub domen wyszczególnionych w prowadzonej przez firmę ESET bazie szkodliwego oprogramowania zostaną zablokowane, a użytkownik zostanie powiadomiony o próbie ataku przez wyświetlenie powiadomienia z ostrzeżeniem.

Ochrona przed atakami typu „phishing” integruje się z najpopularniejszymi przeglądarkami oraz aplikacjami społecznościowymi dla systemu operacyjnego Android, Chrome oraz przeglądarkami zainstalowanymi fabrycznie na urządzeniach z systemem Android (zwykle mają one nazwę *Internet* lub *Przeglądarka*). Inne przeglądarki mogą być wymienione jako niechronione, ponieważ nie zapewniają wystarczającej integracji dla funkcji Anti-Phishing. Aby w pełni wykorzystać funkcję Anti-Phishing, nie zalecamy korzystania z nieobsługiwanych przeglądarek internetowych.

W celu zapewnienia prawidłowej integracji ochrony Anti-Phishing z przeglądarkami internetowymi zalecamy korzystanie z systemu Android 6 (Marshmallow) lub nowszego.

Popraw funkcjonalność — ESET Mobile Security ostrzega, jeśli ochrona przed atakami typu „phishing” wymaga dodatkowych uprawnień w systemie operacyjnym Android. Naciśnij pozycję **Zezwól**, aby otworzyć ustawienia dostępu systemu i uwzględnij dostępne opcje w celu zapewnienia obsługi większej liczby przeglądarek i włączenia ochrony podczas przeglądania w trybie prywatnym (incognito). Jeśli ta sytuacja ma nie zostać zgłoszona jako problem, naciśnij **Ignoruj ten problem (nie jest to zalecane)**.

Aby wyłączyć funkcję Anti-Phishing, dotknij trzech kropek ⋮ w sekcji Anti-Phishing, a następnie dotknij opcji **Wyłącz**.

Zezwól na uprawnienie dostępu w przypadku ESET Mobile Security zainstalowanego z pliku .APK w systemie Android 13

Uwaga

Ze względów bezpieczeństwa system Android 13 ogranicza użycie uprawnienia dostępu do aplikacji zainstalowanych z plików .apk, aby zapobiec jednorodnemu dostępowi do tych uprawnień.

W jaki sposób ESET Mobile Security wykorzystuje to uprawnienie

Używamy tego pozwolenia, aby uzyskać dostęp do adresów URL odwiedzanych witryn. Analizujemy te strony internetowe pod kątem złośliwych intencji, takich jak phishing, szkodliwe oprogramowanie lub inne niebezpieczne działania.

Strona internetowa jest blokowana w przypadku wykrycia zagrożenia, aby chronić Ciebie oraz Twoje dane wrażliwe.

Dane, do których dostęp uzyskano za pośrednictwem uprawnienia dostępności, nie są udostępniane osobom trzecim.

Aby rozwiązać problem z uprawnieniem dostępu:

Przyznaj uprawnienia dostępu

Aby zapoznać się z ilustrowanymi instrukcjami, przeczytaj nasz artykuł w bazie wiedzy (może być dostępny tylko w języku angielskim).

1. Otwórz **Ustawienia** > **Uprawnienia dostępu** > **Pobrane aplikacje**, aplikacja ESET Mobile Security jest niedostępna.

2. Naciśnij aplikację ESET Mobile Security, a otworzy się okno dialogowe **Ograniczone ustawienie**.

3. Naciśnij opcję **„OK”**.

4. Przejdź do opcji **Ustawienia** > **Aplikacje** > ESET Mobile Security i otwórz **Informacje o aplikacji**.

5. Dotknij ikony menu z trzema kropkami w prawym górnym rogu, a następnie opcji > **Zezwól na ustawienia ograniczone**.

Ustawienia ograniczone są teraz włączone, możesz rozpocząć bezpieczne korzystanie z aplikacji.

Ochrona przed atakami typu „phishing” na Samsung DeX

Ochrona przed atakami typu "phishing" nie jest obsługiwana na urządzeniach podłączonych do stacji Samsung DeX.

Chronione przeglądarki

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera

- Opera Beta
- Opera Mini
- Opera Mini Beta
- Przeglądarka Opera TV
- Samsung Internet
- Mint
- Przeglądarka Yandex
- DuckDuckGo (w ESET Mobile Security wersji 6.1 i nowszej)
- Przeglądarka Kiwi
- Granica
- Przeglądarka Silk w urządzeniach Amazon
- Przeglądarka Mi
- Przeglądarka Xiaomi Mi
- Vewd w Android TV

Chronione aplikacje sieci społecznościowych

- Facebook
- Facebook Lite
- Messenger
- Messenger Lite
- Instagram
- Chronione są również aplikacje sieci społecznościowych używające chronionych składników przeglądarki do przeglądania stron internetowych.

Ochrona SMS i Ochrona powiadomień

Ochrona SMS i Ochrona powiadomień chronią Cię przed smishingiem.

Smishing pochodzi z połączenia słów phishing i SMS (Short Message Service). Dlatego zagrożenie to może być czasem określane jako phishing SMS. Atakujący używają wiadomości SMS, ponieważ ludzie bardziej ufają SMS-om niż e-mailom.

Ochrona SMS chroni przed smishingiem pochodzącym z wiadomości SMS. Jednak zagrożenie może rozprzestrzeniać się również z dowolnej platformy komunikacyjnej. W tym miejscu wkracza Ochrona

powiadomień. Po otrzymaniu wiadomości SMS lub powiadomienia (na przykład po otrzymaniu wiadomości w aplikacji Whatsapp),ESET Mobile Security analizuje link. Analiza może zakończyć się trzema wynikami:

- Nie znaleziono zagrożeń.
- Znalezienie Potencjalnie niepożądanej zawartości. Treść wiadomości lub powiadomienia może nie stwarzać bezpośredniego zagrożenia. Intencja nie jest tak jednoznacznie szkodliwa jak inne rodzaje szkodliwego oprogramowania, np. wirusy lub konie trojańskie. Może jednak instalować niechciane oprogramowanie, zmieniać sposób działania urządzenia cyfrowego, a także wykonywać działania niezatwierdzone lub nieoczekiwane przez użytkownika.
- Znaleziono niebezpieczne treści. Ta wiadomość lub powiadomienie zawiera niebezpieczne lub phishingowe linki. Zalecamy, aby nie otwierać zawartości i usunąć wiadomość lub powiadomienie.

Usuwanie wiadomości i powiadomień
Ze względów bezpieczeństwa ESET Mobile Security nie może usuwać wiadomości i powiadomień za Ciebie. Niebezpieczne treści należy usunąć ręcznie.

Jak działa smishing

1. Osoba atakująca wysyła wiadomość zawierającą łącze do strony internetowej.

2. Zwykle prowadzi ono do witryny phishingowej, która może próbować nakłonić Cię do podania danych osobowych. Można je wykorzystać np. do kradzieży pieniędzy lub popełnienia kolejnych oszustw. Łącze może również prowadzić do złośliwej witryny zawierającej złośliwe oprogramowanie lub próbować nakłonić Cię do jego pobrania.

Oznaki smishingu

- Podejrzany numer telefonu, na przykład numer zagraniczny lub o niestandardowej długości.
- Wiadomość zawiera nieznane pliki lub łącza.
- Wiadomości smishingowe zwykle mają pilny ton.
- Wiadomości smishingowe często udają informację o nagrodzie lub zwycięstwie.

Blokada aplikacji

Funkcja Blokada aplikacji umożliwia zabezpieczanie dostępu do wybranych aplikacji (do obsługi poczty e-mail, wiadomości, kalendarza itd.) przy użyciu kodu PIN lub odcisku palca. Blokada aplikacji zapobiega dostępowi osób nieupoważnionych do wybranych aplikacji nawet wtedy, gdy urządzenie jest odblokowane.

Zalecenie
Funkcja włączeniu uprawnienia **Nakładka ekranowa** (**umożliwia wyświetlanie aplikacji na wierzchu**) dla ESET Mobile Security.

Aby skonfigurować funkcję Blokada aplikacji na urządzeniu, należy wykonać poniższe czynności:

1. Włącz **Blokadę aplikacji** na ekranie głównym aplikacji ESET Mobile Security.

2. Naciśnij **Włącz**.

3. Zezwól na uprawnienia dostępu do informacji o użyciu i kliknij **Kontynuuj**.

4. Wprowadź kod PIN do odblokowywania aplikacji.

5. Potwierdź kod PIN, wpisując go ponownie.

6. Naciśnij aplikację, aby ją zablokować lub odblokować.

Skonfiguruj ustawienia blokady aplikacji

Aby uzyskać dostęp do ustawień blokady aplikacji, otwórz menu ⋮ w prawym górnym rogu i kliknij **Ustawienia**:

- **Zablokuj nowe aplikacje** — kiedy opcja blokady aplikacji jest włączona, po instalacji nowej aplikacji na urządzeniu jest wyświetlane pytanie, czy chcesz zablokować nową aplikację.

- **Zablokuj ponownie aplikację** — możesz ustawić Blokadę aplikacji tak, by blokowała aplikacje bezpośrednio po zamknięciu, po wyłączeniu ekranu lub po upływie minuty.

- **Typ blokady** — aplikację można zablokować przy użyciu PIN lub wzoru.

- **Odblokuj odciskiem palca** — ta opcja jest dostępna tylko po zapisaniu zweryfikowanego odcisku palca na urządzeniu. Po jej włączeniu można odblokowywać aplikacje przy użyciu odcisku palca zapisanego na urządzeniu. Nadal będzie można odblokowywać aplikacje przy użyciu PIN. Aby to zrobić, wybierz pozycję **Użyj kodu PIN** podczas otwierania zablokowanej aplikacji.

- **Alert o włamaniu** — po serii nieudanych prób odblokowania urządzenia ESET Mobile Security robi zdjęcie włamywaczowi. Zdjęcie to jest wyświetlane po kolejnym udanym odblokowaniu aplikacji.

Wyłącz blokadę aplikacji

1. Przejdź do blokady aplikacji w ESET Mobile Security.

2. Wpisz kod PIN blokady aplikacji.

3. Naciśnij menu ⋮ w prawym górnym rogu.

4. Naciśnij pozycję **Wyłącz**.

Włączanie trybu nocnego

Tryb nocny na ekranie blokady aplikacji jest łagodniejszy dla oczu i można go włączyć, wybierając ikonę trybu nocnego w prawym górnym rogu.

Nie pamiętam PIN blokady aplikacji

Jeśli zapomnisz kodu PIN blokady aplikacji, a na urządzeniu nie masz zapisanego odcisku palca, zablokowaną aplikację możesz odblokować na dwa sposoby zgodnie z ustawieniami funkcji Anti-Theft:

- Jeśli funkcja Anti-Theft została aktywowana w ESET Mobile Security:

1.Otwórz ESET Mobile Security.

2.Przejdź do blokady aplikacji.

3.Wprowadź swój kod PIN. **Naciśnij Nie pamiętasz kodu PIN?** na środku ekranu.

4.Jeśli funkcja Anti-Theft jest aktywna, zostanie wyświetlony monit o wpisanie hasła do konta ESET HOME. Wpisz hasło w polu **Hasło** i naciśnij **Enter**.

5.Wprowadź nowy kod PIN i naciśnij , aby go potwierdzić.

6.Ponownie wprowadź ten sam kod PIN, aby go potwierdzić. Następnie naciśnij .

- Jeśli funkcja Anti-Theft nie została aktywowana, odinstaluj ESET Mobile Security, a następnie zainstaluj ponownie.

Ochrona płatności

Ochrona płatności to dodatkowa warstwa przeznaczona do ochrony danych finansowych na urządzeniach z Androidem przed zaawansowanym phishingiem i innymi zagrożeniami. Ochrona płatności uniemożliwia innym aplikacjom zauważenie uruchomienia chronionych aplikacji, a także zastępowanie lub odczytywanie informacji na ekranie z chronionej aplikacji. Ochrona płatności uniemożliwia innym aplikacjom zauważenie uruchomienia chronionych aplikacji. Przy aktywacji tej funkcji na tę listę automatycznie trafiają wybrane aplikacje banków i operatorów płatności.

Dodawanie nowej aplikacji do listy chronionych aplikacji

1. Otwórz okno Ochrona płatności w menu Aplikacje lub w menu ESET Mobile Security.

2. Naciśnij opcję **Zarządzaj**.

3. Wybierz aplikacje, które chcesz chronić za pomocą Ochrony płatności.

4. Naciśnij przycisk **OK**, aby potwierdzić wybór.

Otwieranie aplikacji bankowej lub płatniczej przy użyciu funkcji Ochrona płatności

Aby zapewnić najwyższą ochronę aplikacji bankowych i płatniczych, otwieraj te aplikacje za pomocą Bezpiecznego uruchamiania. Rozwiązanie to zapewnia dodatkową warstwę ochrony w porównaniu ze standardową ochroną funkcji Ochrona płatności podczas otwierania aplikacji poza mechanizmem Bezpiecznego uruchamiania. Bezpieczne uruchamianie jest udostępniane automatycznie po włączeniu Ochrony płatności. Zawiera wszystkie aplikacje chronione przez Ochronę płatności.

Co to jest Bezpieczne uruchamianie i jak mogę uzyskać do niego dostęp?

Bezpieczne uruchamianie można znaleźć na liście aplikacji lub przechodząc do pozycji ESET Mobile Security >

Ochrona płatności .

> **Dostęp do Bezpiecznego uruchamiania**
> Aby uzyskać szybszy i łatwiejszy dostęp do aplikacji bankowych i płatniczych, możesz dodać Bezpieczne uruchamianie do ekranu głównego. W tym celu naciśnij ikonę Bezpiecznego uruchamiania i przeciągnij ją na ekran główny.

Filtr połączeń

Filtr połączeń blokuje połączenia przychodzące i wychodzące na podstawie ustawionych reguł.

Zablokowaniu połączenia przychodzącego nie towarzyszy wyświetlenie żadnego powiadomienia. Aby sprawdzić, czy istnieją połączenia, które mogły zostać zablokowane przypadkowo, przejrzyj **Dziennik połączeń**.

Zablokuj ostatnią osobę dzwoniącą — naciśnięcie tej opcji blokuje połączenia przychodzące od ostatniego numeru telefonu. Spowoduje to utworzenie nowej reguły.

Reguły

Aby utworzyć nową regułę, wybierz ikonę +. Więcej informacji zawiera następny rozdział.

Aby zmodyfikować istniejącą regułę, wybierz ją na liście reguł. Aby usunąć wpis z listy **Reguły**, wybierz go i naciśnij ikonę **usuwania** .

Dziennik połączeń

Sekcja **Dziennik połączeń** zawiera dziennik wszystkich połączeń zablokowanych przez Filtr połączeń. Każdy dziennik zawiera nazwę połączenia, związany z nim numer telefonu oraz datę i godzinę zdarzenia.

> **Urządzenia bez karty SIM**
> **Filtr połączeń** nie działa na urządzeniach, które nie obsługują funkcji połączeń i wiadomości.

> **Połączenia wychodzące**
> Filtr połączeń nie blokuje połączeń wychodzących w wersji aplikacji ESET Mobile Security pobranej ze sklepu Google Play.

> **Obsługa systemu Android**
> Filtr połączeń jest dostępny tylko na urządzeniach z systemem Android 6 lub nowszym.

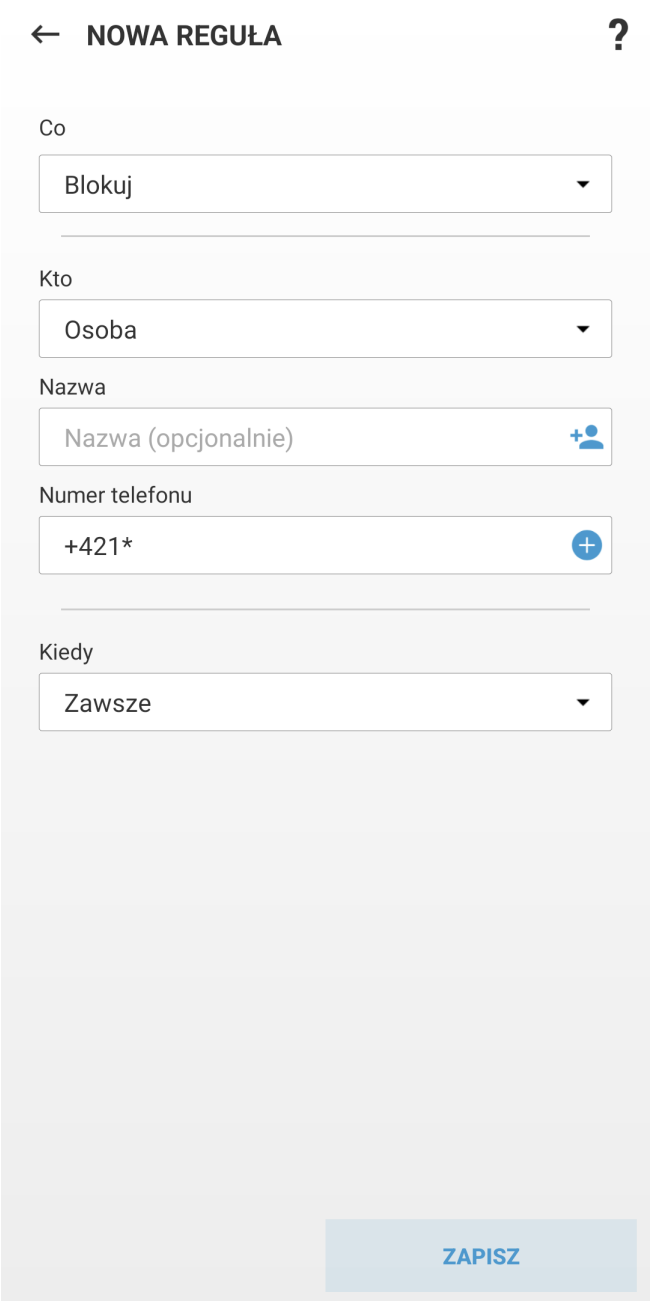
Blokowanie numerów telefonów przy użyciu symboli wieloznaczności

Przy użyciu symboli wieloznaczności opisanych w poniżej tabeli można blokować szereg numerów:

Symbol wieloznaczności	Opis
*	reprezentuje wiele znaków
?	reprezentuje pojedynczy znak

Przykład

Jeśli nie chcesz odbierać połączeń z określonego kraju, wpisz kod kraju oraz symbol wieloznaczności * w polu **Numer telefonu komórkowego**, a wszystkie połączenia przychodzące z tego kraju zaczynające się od tego wzorca numerycznego zostaną zablokowane. Jeśli postanowisz wykluczyć numer z tego kraju, dodaj nową regułę z działaniem **Zezwól**. Na poniższym rysunku pokazano, jak zablokować wszystkie połączenia ze Słowacji.



Dodawanie nowej reguły

Aby utworzyć nową regułę, wybierz ikonę **+**.

1. W sekcji **Co** wybierz pozycję **Blokuj** lub **Zezwól**, aby określić typ reguły dotyczącej połączeń i wiadomości. Wybierz kierunek połączeń do blokowania (domyślnie jest wybrana opcja Przychodzące).

2. W sekcji **Kto** wybierz opcję, aby określić numery telefonów, które będzie obejmować reguła.

• **Osoba** — wybierz osobę z listy kontaktów lub dodaj imię i nazwisko i numer ręcznie. Do jednego imienia i nazwiska możesz przypisać więcej numerów telefonów, klikając przycisk **+** w sekcji **Numer telefonu**.
• **Grupa** — program ESET Mobile Security rozpoznaje grupy kontaktów zapisane w obszarze Kontakty (np. Rodzina, Znajomi lub Praca).
• Opcja **Wszystkie nieznane numery** obejmuje wszystkie numery telefonów niezapisane na liście kontaktów. Ta opcja umożliwia zablokowanie niepożądanych połączeń (np. nieoczekiwanych ofert handlowych) lub dzwonienia pod nieznane numery przez dzieci.
• Opcja **Wszystkie znane numery** obejmuje wszystkie numery telefonów zapisane na liście kontaktów.
• Opcja **Wszystkie numery** blokuje wszystkie połączenia przychodzące.
• Opcja **Ukryte numery** dotyczy wszystkich rozmówców, którzy ukrywają swój numer telefonu za pomocą usługi Calling Line Identification Restriction (CLIR).

3.W sekcji **Kiedy** wybierz pozycję **Zawsze** lub **Niestandardowy**, aby określić przedział czasu i dni tygodnia, podczas których będzie obowiązywać ta reguła. Domyślnie wybrana jest sobota i niedziela.

Instrukcję z ilustracjami zawiera ten artykuł bazy wiedzy.

> **Filtr połączeń za granicą**
> w przypadku pobytu za granicą wszystkie numery telefonów na liście muszą być poprzedzone międzynarodowym numerem kierunkowym (np. +1610100100).

Inspekcja sieci

Funkcja Inspekcja sieci umożliwia wyszukiwanie w sieci urządzeń podłączonych do routera oraz sprawdzanie ich luk w zabezpieczeniach. Funkcja Inspekcja sieci skanuje sieć dwuetapowo.

Najpierw funkcja Inspekcja sieci wyszukuje w sieci podłączone urządzenia. Jeżeli wykryje nowe urządzenie, wyświetli powiadomienie, a urządzenie zostanie oznaczone gwiazdką. Urządzenia w sieci możesz wykrywać ręcznie, wybierając pozycję **Skanuj sieć**. Urządzenia można także wykrywać automatycznie. W tym celu dotknij ikony menu > **Ustawienia** i wybierz opcję **Automatycznie wykrywaj urządzenia**.

Na drugim etapie skanowania funkcja Inspekcja sieci sprawdza luki w zabezpieczeniach podłączonych urządzeń, takie jak otwarte porty, słabe nazwy użytkownika i hasła użytkowników routera, problemy z oprogramowaniem firmware routera itp. Atakujący mogą wykorzystywać takie luki do przejęcia kontroli nad routerem oraz innymi podłączonymi do niego urządzeniami. Routery i urządzenia kontrolowane przez włamywaczy mogą służyć do gromadzenia informacji o użytkowniku, udziału w atakach rozproszonej odmowy usługi (DDoS) itp.

Funkcja Inspekcja sieci zapewnia także wyczerpującą listę urządzeń podłączonych do sieci, dzięki której można sprawdzić, kto nawiązuje połączenia z siecią użytkownika. Na tej podstawie można zarządzać dostępem urządzeń do sieci z interfejsu routera w przeglądarce, w tym także tego dostępu odmówić. Do interfejsu routera można przejść bezpośrednio z funkcji Sieć domowa, wybierając router i opcję **Otwórz interfejs sieciowy**.

Podłączone urządzenia można wyświetlać na liście lub w formacie wizualnym:

• Widok listy — podłączone urządzenia są wyświetlane w standardowym widoku listy z routerem u góry, po którym następują urządzenia będące online, a w dalszej kolejności — historia uprzednio podłączonych urządzeń.

-  Widok sonaru — urządzenia są wyświetlane w formacie półkola, w którego środku znajduje się router. W drugiej warstwie od środka są wyświetlane urządzenia aktualnie online. W trzeciej warstwie jest wyświetlana historia uprzednio podłączonych urządzeń. Między urządzeniami można przechodzić, dotykając przycisków ze strzałkami lub przewijając w kierunku kółka.

Aby ułatwić sobie zarządzanie urządzeniami, można przypisać im kategorie (np. Smartfon, Telewizor, Konsola, Komputer) i zamienić standardowe nazwy producenta lub adresy IP na bardziej zrozumiałe nazwy (np. SM-G955F na telefon Pawła, 192.168.1.52 na komputer Kasi itp.).

Aby zmienić nazwy urządzeń w funkcji Inspekcja sieci, wybierz ikonę urządzenia, a następnie wybierz ikonę ołówka w prawym górnym rogu ekranu, wybierz kategorię, wpisz nazwę urządzenia i wybierz przycisk **OK**.

Audyt zabezpieczeń

Audyt zabezpieczeń ułatwia monitorowanie i zmienianie ważnych ustawień urządzenia. Przejrzyj uprawnienia aplikacji zainstalowanych na urządzeniu, aby zapobiec zagrożeniom.

Aby włączyć lub wyłączyć funkcję Audyt zabezpieczeń oraz jej komponenty, wybierz przycisk menu , a następnie wybierz pozycję **Wyłącz monitorowanie urządzenia** lub **Wyłącz audyt aplikacji**.

- Monitorowanie urządzenia
- Audyt aplikacji

Monitorowanie urządzenia

W sekcji **Monitorowanie urządzenia** należy określić elementy urządzenia monitorowane przez program ESET Mobile Security.

Aby wyświetlić szczegółowy opis każdej opcji oraz jej bieżący status, należy ją nacisnąć. W przypadku opcji **Nieznane źródła** i **Tryb debugowania** należy nacisnąć pozycję **Otwórz ustawienia**, aby zmienić ustawienia w **ustawieniach systemu operacyjnego Android**.

Każdy komponent można wyłączyć.

1. Naciśnij komponent, który chcesz wyłączyć.
2. Naciśnij ikonę menu .
3. Naciśnij pozycję **Wyłącz**.

Audyt aplikacji

Funkcja Audyt aplikacji wykonuje audyt zainstalowanych na urządzeniu aplikacji, które mogą uzyskiwać dostęp do usług płatnych, śledzić lokalizację użytkownika oraz odczytywać jego dane osobowe, kontakty lub wiadomości tekstowe. ESET Mobile Security zawiera listę tych aplikacji posortowanych według kategorii. Naciskając poszczególne kategorie, można wyświetlić ich szczegółowe opisy. Aby wyświetlić szczegóły uprawnień aplikacji,

należy nacisnąć aplikację.

Ustawienia

Aby uzyskać dostęp do ustawień programu, naciśnij pozycję Menu  na ekranie głównym programu ESET Mobile Security (lub naciśnij przycisk Menu na urządzeniu) i naciśnij pozycję **Ustawienia**.

Kopia zapasowa i przywracanie

ESET Mobile Security umożliwia utworzenie pliku kopii zapasowej zawierającego ustawienia ESET Mobile Security. Plik ten możesz pobrać do urządzenia zewnętrznego i użyć go do przywrócenia ustawień aplikacji ESET Mobile Security.

Język

Domyślnie program ESET Mobile Security jest instalowany w języku ustawionym jako domyślny na urządzeniu (Ustawienia Język i klawiatura w systemie operacyjnym Android). Aby zmienić wersję językową interfejsu użytkownika aplikacji, należy nacisnąć pozycję **Język** i wybrać preferowany język.

Stałe powiadamianie

(Ta opcja jest dostępna tylko w systemie Android 7 i starszych wersjach)

Program ESET Mobile Security wyświetla powiadomienie w dolnej części paska powiadomień systemu Android. Jeśli nie chcesz, aby powiadomienie było wyświetlane, odznacz opcję Stałe powiadamianie i dotknij pozycji Wyłącz.

Zgoda użytkownika

- **Zezwól ESET LiveGrid©** — aby dowiedzieć się więcej na temat **ESET LiveGrid©**, odwiedź sekcję Ustawienia zaawansowane.
- **Zezwól analitykom na ulepszanie naszych produktów**—ESET Mobile Security będzie przesyłać anonimowe informacje o aplikacji (dane dotyczące wydajności, statystyki działania), które pomogą nam w doskonaleniu aplikacji i usług. Aby dowiedzieć się więcej o gromadzonych przez nas informacjach, odwiedź rozdział Polityka prywatności.
- **Zezwalaj na wykorzystanie danych do celów marketingowych**

Aktualizuj

Aby zapewnić maksymalną ochronę, należy używać najnowszej wersji programu ESET Mobile Security. Opcja **Aktualizuj** umożliwia sprawdzanie, czy na stronie internetowej firmy ESET dostępna jest nowsza wersja. Ta opcja nie jest dostępna, jeśli pobrano program ESET Mobile Security ze sklepu Google Play. W takim przypadku program ten jest aktualizowany przy użyciu sklepu Google Play.

Odinstaluj

Uruchomienie kreatora odinstalowywania spowoduje trwałe usunięcie ESET Mobile Security z urządzenia. Jeśli ochrona Anti-Theft jest włączona, zostanie wyświetlona prośba, aby wprowadzić numer PIN lub zeskanować odcisk palca zabezpieczający program ESET Mobile Security. Aby ręcznie odinstalować produkt, wykonaj kroki opisane w tej sekcji.

> **Ochrona przed odinstalowaniem**
> Ochrona przed odinstalowaniem nie jest aktywna w systemie Android w wersjach 7.0 i nowszych.

Dział obsługi klienta

Specjaliści z działu obsługi klienta firmy ESET służą pomocą w sprawach administracyjnych i technicznych dotyczących programu ESET Mobile Security lub innych produktów firmy ESET.

Skontaktuj się z działem obsługi klienta ESET

Aby wysłać zgłoszenie do działu pomocy technicznej bezpośrednio z urządzenia:

1. Naciśnij pozycję Menu na ekranie głównym programu ESET Mobile Security (lub naciśnij przycisk Menu na urządzeniu).

2. Naciśnij pozycję **Dział obsługi klienta**.

3. Naciśnij pozycję **Dział obsługi klienta**, aby wysłać żądanie udzielenia pomocy technicznej.

4. Wypełnij wszystkie wymagane pola. Program ESET Mobile Security udostępnia zaawansowane funkcje zapisywania w dzienniku, które pomagają w diagnozowaniu potencjalnych problemów technicznych.

5. Aby przekazać firmie ESET szczegółowy dziennik aplikacji, sprawdź, czy opcja **Prześlij dziennik aplikacji** jest wybrana (domyślnie jest włączona).

6. Naciśnij pozycję **Prześlij**, aby wysłać żądanie.

7. Specjalista z działu obsługi klienta firmy ESET skontaktuje się z Tobą przy użyciu podanego adresu e-mail.

Dzienniki diagnostyczne zostały usunięte po odinstalowaniu i ponownym zainstalowaniu ESET Mobile Security w ramach rozwiązywania problemów. Zalecamy ponowne wygenerowanie problemu, a następnie wysłanie dzienników.

> **Nie można otworzyć aplikacji lub aplikacja nie odpowiada**
> Aby przesłać zgłoszenie do działu obsługi klienta ESET w przypadku, gdy program ESET Mobile Security nie odpowiada lub nie można go otworzyć, wybierz kolejno **Ustawienia** > **Aplikacje** > **ESET Mobile Security** > **Pamięć masowa** > **Zarządzaj pamięcią**. Zarządzaj pamięcią. Kliknij pozycję **Dział obsługi klienta** i wypełnij wszystkie wymagane pola.

Umowa licencyjna użytkownika końcowego

Obowiązuje od 19 października 2021 r..

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

Umowę Licencyjną Użytkownika Końcowego

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

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

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

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

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

2. **Instalacja, komputer i klucz licencyjny**. Oprogramowanie dostarczone na nośniku danych, otrzymane za pośrednictwem poczty elektronicznej, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł musi zostać zainstalowane. Oprogramowanie należy zainstalować na prawidłowo skonfigurowanym komputerze, który spełnia minimalne wymagania określone w Dokumentacji. Procedurę instalacji również opisano w Dokumentacji. Na komputerze, na którym zostanie zainstalowane Oprogramowanie, nie można instalować sprzętu komputerowego ani programów komputerowych, które mogłyby niekorzystnie wpłynąć na Oprogramowanie. Komputer oznacza sprzęt, w tym między innymi komputery osobiste, laptopy, stacje robocze, palmtopy, smartfony, przenośne urządzenia elektroniczne lub inne urządzenia elektroniczne, dla których przeznaczone jest Oprogramowanie, na których zostanie zainstalowane i/lub będzie używane. Klucz licencyjny oznacza niepowtarzalny ciąg symboli, liter, cyfr i znaków specjalnych, dostarczony Użytkownikowi końcowemu w celu umożliwienia mu legalnego korzystania z Oprogramowania, jego określonych wersji lub rozszerzenia warunków Licencji zgodnie z niniejszą Umową.

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

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

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

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

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

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

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

g) **Wygaśnięcie Licencji.** Licencja wygasa automatycznie po upływie okresu jej obowiązywania. Jeśli Licencjobiorca naruszył którekolwiek z postanowień niniejszej Umowy, Dostawca jest uprawniony do rozwiązania niniejszej Umowy oraz do wykonania wszelkich innych praw i zastosowania wszelkich innych środków prawnych przysługujących mu w takiej sytuacji. W razie anulowania Licencji Licencjobiorca musi natychmiast usunąć lub zniszczyć Oprogramowanie i wszystkie jego kopie zapasowe lub zwrócić je na własny koszt do firmy ESET bądź w miejscu zakupu Oprogramowania. Po wygaśnięciu Licencji Dostawca jest też uprawniony do anulowania prawa Użytkownika końcowego do używania funkcji Oprogramowania, które wymagają połączenia z serwerami Dostawcy lub serwerami innych firm.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

e) Licencjobiorca zobowiązuje się używać Oprogramowania w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Oprogramowania ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze

stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

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

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

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

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

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

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

11. **OŚWIADCZENIA UŻYTKOWNIKA KOŃCOWEGO**. LICENCJOBIORCA (WYSTĘPUJĄCY W CHARAKTERZE UŻYTKOWNIKA KOŃCOWEGO) PRZYJMUJE OPROGRAMOWANIE W STANIE TAKIM, W JAKIM ZOSTAŁO MU ONO DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA. ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE OPROGRAMOWANIE NIE BĘDZIE NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA OSOBA NIE GWARANTUJE, ŻE FUNKCJE OPROGRAMOWANIA SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE OPROGRAMOWANIA BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. LICENCJOBIORCA BIERZE NA SIEBIE WSZELKĄ ODPOWIEDZIALNOŚĆ I RYZYKO ZA DOBÓR OPROGRAMOWANIA ODPOWIEDNIEGO DO OSIĄGNIĘCIA CELÓW LICENCJOBIORCY ORAZ ZA PRZEPROWADZENIE INSTALACJI OPROGRAMOWANIA, ZA JEGO UŻYCIE I ZA WYNIKI TEGO UŻYCIA.

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

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

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

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

16. **Przeniesienie Licencji**. Jeśli odpowiednie postanowienia niniejszej Umowy tego nie zabraniają,

Oprogramowanie można przenosić między poszczególnymi systemami komputerowymi. O ile nie jest to sprzeczne z warunkami określonymi w niniejszej Umowie, za zgodą Dostawcy Użytkownik końcowy może trwale przenieść Licencję i wszelkie prawa przysługujące mu na podstawie niniejszej Umowy na innego Użytkownika końcowego, pod warunkiem że (i) nie zachowa dla siebie żadnych kopii Oprogramowania; (ii) przeniesienie praw będzie bezpośrednie, tj. prawa zostaną przeniesione bezpośrednio na nowego Użytkownika końcowego; (iii) nowy Użytkownik końcowy przejmie na siebie wszystkie prawa i obowiązki wynikające z niniejszej Umowy, które miały dotąd zastosowanie do Użytkownika końcowego przenoszącego Licencję; (iv) nowy Użytkownik końcowy otrzyma od Użytkownika końcowego przenoszącego Licencję dokumentację, która umożliwi mu stwierdzenie zgodnie z zapisami w punkcie 17, czy Oprogramowanie jest oryginalne.

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

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

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

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

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

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

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

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

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

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

c) Żadne z postanowień Umowy nie ma na celu ani nie powinno być interpretowane lub odczytywane jako nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

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

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

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

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

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

ANEKS DO UMOWY

Ocena zabezpieczeń urządzeń podłączonych do sieci. Dodatkowe zapisy dotyczące oceny zabezpieczeń urządzeń podłączonych do sieci brzmią następująco:

Oprogramowanie zawiera funkcję służącą do sprawdzania zabezpieczeń sieci lokalnej Użytkownika końcowego oraz zabezpieczeń urządzeń w sieci lokalnej. Funkcja ta wymaga podania nazwy sieci lokalnej i informacji na temat urządzeń w tej sieci, takich jak obecność, typ, nazwa, adres IP i adres MAC urządzenia w sieci lokalnej w połączeniu z informacjami o licencji. Informacje te obejmują także typ zabezpieczeń i typ szyfrowania sieci bezprzewodowej w przypadku routerów. Wspomniana funkcja może również przekazywać informacje dotyczące dostępności programowego rozwiązania zabezpieczającego na potrzeby ochrony urządzeń w sieci lokalnej.

Ochrona przed niewłaściwym wykorzystaniem danych. Dodatkowe zapisy dotyczące ochrony przed niewłaściwym wykorzystaniem danych brzmią następująco:

Oprogramowanie zawiera funkcję zapobiegającą utracie i niewłaściwemu wykorzystywaniu kluczowych danych wskutek kradzieży Komputera. Funkcja jest domyślnie wyłączona w ustawieniach Oprogramowania. W celu jej aktywacji należy utworzyć Konto ESET HOME, za pośrednictwem którego uruchamiany jest mechanizm gromadzenia danych, gdy komputer zostanie skradziony. W przypadku aktywacji tej funkcji Oprogramowania dane dotyczące ukradzionego komputera zostaną zebrane i wysłane Dostawcy. Mogą zawierać dane dotyczące lokalizacji sieci komputera, dane na temat treści wyświetlanych na ekranie komputera, dane na temat konfiguracji komputera i/lub dane zarejestrowane przez kamerę podłączoną do komputera (odtąd określane „Danymi"). Użytkownik końcowy ma prawo wykorzystywać Dane pozyskane przez tę funkcję i dostarczone za pośrednictwem Konta ESET HOME wyłącznie w celu usunięcia skutków kryzysowej sytuacji spowodowanej kradzieżą komputera. Wyłącznie na potrzeby tej funkcji Dostawca przetwarza Dane zgodnie z Polityką prywatności i obowiązującymi przepisami prawa. Dostawca zezwoli Użytkownikowi końcowemu na dostęp do Danych przez okres niezbędny do realizacji celu, dla którego Dane zostały pozyskane, jednak nie dłuższy niż okres przechowywania określony w Polityce prywatności. Użytkownik końcowy może stosować funkcję ochrony przed niewłaściwym wykorzystaniem danych wyłącznie na Komputerach i kontach, do których ma uprawniony dostęp. Każde zdarzenie nielegalnego użycia będzie zgłaszane właściwym władzom. Dostawca będzie przestrzegał obowiązujących przepisów prawa, a w przypadku niewłaściwego wykorzystania danych będzie wspierał działania uprawnionych organów. Użytkownik przyjmuje do wiadomości i potwierdza, że odpowiada za utrzymanie poufności hasła dostępu do swojego Konta ESET HOME i nie ujawni go żadnym osobom trzecim. Użytkownik końcowy odpowiada za wszelkie przypadki użycia funkcji ochrony przed niewłaściwym wykorzystaniem danych oraz Konta ESET HOME, bez względu na fakt, czy odbyło się to za jego zgodą czy nie. W razie naruszenia zabezpieczeń Konta ESET HOME należy natychmiast powiadomić Dostawcę.

Kody. Dodatkowe zapisy dotyczące Kodu brzmią następująco:

Firma ESET może według własnego uznania utworzyć i udostępnić kod polecającego i/lub inny kod w celach promocyjnych lub marketingowych (zwany dalej „Kodem"). Licencjobiorca może zrealizować Kod, aby przedłużyć okres licencji zgodnie z niniejszą Umową. Firma ESET zastrzega sobie prawo do wyłączenia Kodu w dowolnej chwili, gdy Kod został uzyskany lub jest używany w sposób, który nie jest zgodny z niniejszą Umową, i/lub w przypadku uzasadnionego podejrzenia, że Kod został uzyskany w wyniku błędu, oszustwa lub nielegalnej działalności. Licencjobiorca musi przestrzegać następujących ograniczeń:

i. Licencjobiorca nie może zrealizować Kodu więcej niż raz.

ii. Licencjobiorca nie może sprzedać, wydzierżawić, wypożyczyć Kodu ani używać go w celach świadczenia usług o charakterze komercyjnym.

iii. Licencjobiorca akceptuje, że firma ESET może wyłączyć udostępnianie i/lub używanie Kodu w dowolnym czasie bez ponoszenia przez nią odpowiedzialności.

iv. Licencjobiorca akceptuje, że Kod nie uprawnia do uzyskania gotówki ani innego wynagrodzenia.

v. Licencjobiorca akceptuje, że Kod i/lub użycie Kodu może podlegać warunkom szczególnym udostępnionym przez firmę ESET na potrzeby konkretnej kampanii poleceń, promocyjnej lub marketingowej.

EULAID: EULA-PRODUCT-LG-EMS; 3537.0

Zasady ochrony prywatności

Jako administrator danych, firma ESET, spol. s r. o., z siedzibą pod adresem Einsteinova 24, 851 01 Bratislava, Slovak Republic, zarejestrowana w Rejestrze Handlowym prowadzonym przez Sąd Rejonowy dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 („ESET" lub „My"), przykłada szczególną wagę do kwestii ochrony danych osobowych. Chcemy spełnić wymóg przejrzystości znormalizowany prawnie zgodnie z Ogólnym rozporządzeniem o ochronie danych UE („RODO"). W związku z tym publikujemy niniejszą Politykę prywatności wyłącznie w celu przekazania klientowi jako osobie, której dane dotyczą (dalej „Użytkownik końcowy" lub „Ty"), informacji na następujące tematy z obszaru ochrony danych osobowych:

- Podstawa prawna przetwarzania danych osobowych,
- Udostępnianie danych i poufność,
- Bezpieczeństwo danych,
- Prawa osoby, której dane dotyczą,
- Przetwarzanie danych osobowych
- Informacje kontaktowe.

Podstawa prawna przetwarzania danych osobowych

Firma ESET przetwarza dane wyłącznie w oparciu o kilka podstaw prawnych przewidzianych przepisami prawa dotyczącymi ochrony prywatności danych osobowych. Przetwarzanie danych osobowych przez firmę ESET jest niezbędne głównie do realizacji Umowę Licencyjną Użytkownika Końcowego („EULA") z Użytkownikiem końcowym (art. 6 ust. 1 lit. b ustawy RODO), która obejmuje dostarczanie produktów lub usług firmy ESET, chyba że wyraźnie zaznaczono inaczej, np.:

- Podstawa prawna dotycząca uzasadnionego interesu (art. 6 ust. 1 lit. f ustawy RODO), która umożliwia firmie ESET przetwarzanie danych oraz monitorowanie sposobu korzystania i zadowolenia z Usług przez użytkowników w celu zapewnienia najlepszej możliwej ochrony, wsparcia i doświadczenia. W świetle obowiązujących przepisów prawa działania marketingowe są uznawane za uzasadniony interes, dlatego firma ESET polega na nich w komunikacji marketingowej z klientami.
- Firma ESET może wymagać od Użytkownika zgody w określonych sytuacjach (art. 6 ust. 1 lit. a ustawy RODO), gdy taka podstawa prawna zostanie uznana za najodpowiedniejszą lub jeśli wymaga tego prawo.
- Przestrzeganie obowiązków prawnych (art. 6 ust. 1 lit. c ustawy RODO), np. określenie wymagań dotyczących komunikacji elektronicznej, fakturowania lub dokumentów rozliczeniowych.

Udostępnianie danych i poufność

Nie udostępniamy Twoich danych stronom trzecim. Jednakże ESET jest firmą działającą na całym świecie za pośrednictwem swoich spółek stowarzyszonych oraz partnerów będących częścią sieci sprzedaży, usług i pomocy technicznej. Przetwarzane przez firmę ESET informacje dotyczące licencji, rozliczeń i pomocy technicznej mogą być przesyłane między nami a naszymi partnerami oraz spółkami stowarzyszonymi z tytułu realizacji Umowy Licencyjnej Użytkownika Końcowego, na przykład świadczenia usług lub udzielania pomocy technicznej.

Firma ESET woli przetwarzać swoje dane w Unii Europejskiej (UE). Jednak w zależności od Twojej lokalizacji (w razie korzystania z naszych produktów i/lub usług poza UE) i/lub wybranej usługi może być konieczne przekazanie Twoich danych do kraju spoza UE. Na przykład korzystamy z usług stron trzecich w związku z przetwarzaniem w

chmurze. W takich przypadkach starannie dobieramy naszych usługodawców i zapewniamy odpowiedni poziom ochrony danych za pomocą wymogów umownych oraz środków technicznych i organizacyjnych. Z reguły zawieramy standardowe klauzule umowne UE, w razie potrzeby uzupełniając je dodatkowymi przepisami umownymi.

W przypadku niektórych krajów spoza UE, takich jak Wielka Brytania i Szwajcaria, UE określiła już porównywalny poziom ochrony danych. Ze względu na ten porównywalny poziom ochrony danych przekazywanie danych do tych krajów nie wymaga żadnego specjalnego upoważnienia ani zgody.

Bezpieczeństwo danych

Firma ESET stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu zabezpieczeń odpowiedniego do zagrożeń. Dokładamy wszelkich starań, aby zapewnić nieprzerwaną poufność, integralność, dostępność i odporność systemów oraz usług związanych z przetwarzaniem danych. W przypadku naruszenia ochrony danych zagrażającego prawom i wolnościom Użytkownika końcowego jesteśmy jednak gotowi do powiadomienia o tym fakcie odpowiednich organów nadzorczych oraz osoby, których dane dotyczą.

Prawa osób, których dane dotyczą

Prawa każdego Użytkownika końcowego są ważne i chcemy poinformować, że wszyscy Użytkownicy końcowi (z dowolnego kraju UE oraz spoza UE) mają następujące prawa zagwarantowane przez firmę ESET. Aby skorzystać z praw osoby, której dane dotyczą, możesz skontaktować się z nami za pośrednictwem formularza pomocy technicznej lub poczty elektronicznej, wysyłając wiadomość na adres dpo@eset.sk. W celach identyfikacyjnych prosimy o podanie następujących informacji: Imię i nazwisko, adres e-mail oraz – jeśli jest dostępny – klucz licencyjny lub numer klienta oraz przynależność do firmy. Prosimy o powstrzymanie się od przesyłania nam jakichkolwiek innych danych osobowych, takich jak data urodzenia. Zwracamy uwagę, że aby móc przetworzyć Twoje zapytanie, a także w celach identyfikacyjnych, będziemy przetwarzać Twoje dane osobowe.

Prawo do wycofania zgody. Prawo do wycofania zgody obowiązuje wyłącznie w przypadku przetwarzania na podstawie udzielonej zgody. Jeśli przetwarzamy Twoje dane osobowe na podstawie Twojej zgody, masz prawo wycofać tę zgodę w dowolnym momencie bez podania przyczyn. Wycofanie zgody jest skuteczne tylko na przyszłość i nie wpływa na zgodność z prawem danych przetwarzanych przed jej wycofaniem.

Prawo do wyrażenia sprzeciwu. Prawo do wyrażenia sprzeciwu wobec przetwarzania danych obowiązuje wyłącznie w przypadku przetwarzania na podstawie uzasadnionego interesu firmy ESET lub strony trzeciej. Jeśli przetwarzamy Twoje dane osobowe w celu ochrony uzasadnionego interesu, będąc osobą, której dane dotyczą, masz prawo w dowolnym momencie sprzeciwić się uzasadnionemu interesowi wskazanemu przez nas i przetwarzaniu Twoich danych osobowych. Sprzeciw jest skuteczny tylko na przyszłość i nie wpływa na zgodność z prawem danych przetwarzanych przed jego wyrażeniem. Jeśli przetwarzamy Twoje dane osobowe w celach marketingu bezpośredniego, nie jest konieczne podawanie powodów Twojego sprzeciwu. Dotyczy to również profilowania, o ile jest ono związane z marketingiem bezpośrednim. We wszystkich innych przypadkach prosimy o krótkie poinformowanie nas o powodzie sprzeciwu wobec przetwarzania Twoich danych osobowych zgodnie z uzasadnionym interesem firmy ESET.

Należy pamiętać, że w niektórych przypadkach, pomimo wycofania zgody, jesteśmy uprawnieni do dalszego przetwarzania Danych osobowych na podstawie innej podstawy prawnej, na przykład w celu realizacji umowy.

Prawo do uzyskania dostępu. Jako osoba, której dane dotyczą, masz prawo do bezpłatnego uzyskania w dowolnym momencie informacji o Twoich danych przechowywanych przez firmę ESET.

Prawo do sprostowania. Jeśli nieumyślnie przetwarzamy Twoje nieprawidłowe dane osobowe, masz prawo do ich poprawienia.

Prawo do usunięcia danych i prawo do ograniczenia przetwarzania. Jako osoba, której dane dotyczą, masz prawo do zażądania usunięcia lub ograniczenia przetwarzania swoich danych osobowych. Jeśli przetwarzamy Twoje dane osobowe, na przykład na mocy wyrażonej przez Ciebie zgody, którą następnie wycofujesz, a nie istnieje żadna inna podstawa prawna, taka jak umowa, natychmiast usuwamy Twoje dane osobowe. Twoje dane osobowe zostaną również usunięte z końcem naszego okresu przechowywania, gdy tylko nie będą już potrzebne do określonych dla nich celów.

Jeśli wykorzystujemy Twoje dane osobowe wyłącznie do celów marketingu bezpośredniego i zdecydujesz się odwołać swoją zgodę lub sprzeciwisz się leżącemu u podstaw przetwarzania uzasadnionemu interesowi firmy ESET, ograniczymy przetwarzanie Twoich danych osobowych, umieszczając Twoje dane kontaktowe na naszej wewnętrznej czarnej liście, aby uniknąć niechcianego kontaktu. W innych przypadkach Twoje dane osobowe zostaną usunięte.

Należy pamiętać, że możemy być zobowiązani do przechowywania Twoich danych do czasu wygaśnięcia obowiązków przechowywania i okresów wymaganych przez ustawodawcę lub organy nadzorcze. Obowiązki i okresy przechowywania mogą również wynikać z ustawodawstwa słowackiego. Po ich upłynięciu właściwe dane zostaną rutynowo usunięte.

Prawo do przeniesienia danych. Z przyjemnością przekazujemy Użytkownikowi będącemu osobą, której dane dotyczą, jego dane osobowe przetwarzane przez firmę ESET w formacie xls.

Prawo do wniesienia skargi. Jako osoba, której dane dotyczą, masz prawo do wniesienia w dowolnym momencie skargi do organu nadzorczego. Firma ESET podlega prawu słowackiemu i obowiązują ją przepisy Unii Europejskiej o ochronie danych. Właściwym organem nadzorczym ds. danych jest Urząd Ochrony Danych Osobowych Republiki Słowackiej z siedzibą pod adresem Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Przetwarzanie danych osobowych

Usługi zaimplementowane w produkcie firmy ESET są przez nas świadczone zgodnie z postanowieniami Umowy EULA, ale niektóre z nich mogą wymagać szczególnej uwagi. Chcemy przekazać szczegółowe informacje na temat gromadzenia danych związanych ze świadczonymi przez nas usługami. Świadczymy różne usługi opisane w Umowie Licencyjnej Użytkownika Końcowego oraz w dokumentacja. Abyśmy mogli dostarczać nasze usługi, musimy gromadzić następujące informacje:

Dane licencyjne i rozliczeniowe. Imię i nazwisko, adres e-mail, klucz licencyjny i (w stosownych przypadkach) adres, przynależność do firmy i dane dotyczące płatności są gromadzone i przetwarzane przez firmę ESET w celu ułatwienia aktywacji licencji, dostarczenia klucza licencyjnego, przypomnień o wygaśnięciu, realizacji wniosków o pomoc techniczną, weryfikacji autentyczności licencji, świadczenia naszych usług oraz dostarczania innych powiadomień, w tym wiadomości marketingowych, zgodnie z obowiązującymi przepisami lub zgodą użytkownika. Firma ESET jest prawnie zobowiązana do przechowywania informacji rozliczeniowych przez okres 10 lat, jednak informacje licencyjne zostaną zanonimizowane nie później niż 12 miesięcy po wygaśnięciu licencji.

Aktualizacja i inne statystyki. Przetwarzane informacje obejmują 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 informacje o systemie operacyjnym, dane dotyczące sprzętu, identyfikatory instalacji, identyfikatory licencji, adres IP, adres MAC oraz ustawienia konfiguracji produktu. Są one przetwarzane do celów dostarczania aktualizacji usług oraz konserwacji, zapewniania bezpieczeństwa i ulepszania naszej infrastruktury.

Informacje te są przechowywane oddzielnie od informacji identyfikacyjnych wymaganych do celów licencjonowania i fakturowania, ponieważ nie wymagają identyfikacji Użytkownika końcowego. Okres przechowywania wynosi do 4 lat.

System reputacji ESET LiveGrid®. Skróty jednokierunkowe związane z infekcjami są przetwarzane na potrzeby systemu reputacji ESET LiveGrid®, który poprawia wydajność naszych rozwiązań do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze. Użytkownik końcowy nie jest identyfikowany podczas tego procesu.

System informacji zwrotnych ESET LiveGrid®. Próbki podejrzanego kodu i metadanych używane przez system reputacji ESET LiveGrid®, które pozwalają produktom ESET reagować natychmiast na potrzeby użytkowników końcowych i zapewnić ochronę przed najnowszymi zagrożeniami. Korzystamy następujących danych otrzymanych od użytkowników końcowych

- Dane dotyczące infekcji, takie jak próbki potencjalnych wirusów i innych szkodliwych programów, a także podejrzane, potencjalnie niepożądane i potencjalnie niebezpieczne obiekty (np. pliki wykonywalne i wiadomości e-mail zgłoszone jako spam lub oznaczone przez nasz produkt);
- Informacje dotyczące korzystania z Internetu, takie jak adres IP, informacje geograficzne, pakiety IP, adresy URL i ramki sieci Ethernet;
- Pliki zrzutu awaryjnego i informacje w nich zawarte.

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

Wszystkie informacje uzyskane i przetwarzane za pośrednictwem systemu informacji zwrotnych ESET LiveGrid® są przeznaczone do użycia bez identyfikowania Użytkownika końcowego.

Ocena zabezpieczeń urządzeń podłączonych do sieci. Na potrzeby dostarczania funkcji oceny zabezpieczeń urządzeń podłączonych do sieci przetwarzamy nazwy sieci lokalnej i informacje na temat urządzeń w tej sieci, takie jak dane dotyczące obecności, typ, nazwa, adres IP i adres MAC urządzenia w sieci lokalnej w połączeniu z informacjami o licencji. Informacje te obejmują także typ zabezpieczeń i typ szyfrowania sieci bezprzewodowej w przypadku routerów. Informacje dotyczące licencji pozwalające na identyfikację Użytkownika końcowego będą anonimizowane nie później niż 12 miesięcy po wygaśnięciu licencji.

Pomoc techniczna. Aby zapewnić możliwość świadczenia pomocy technicznej lub pomocy innego rodzaju, mogą być wymagane dane kontaktowe i informacje dotyczące licencji przesyłane 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. W celu podniesienia jakości udzielanej pomocy technicznej możemy poprosić Użytkownika końcowego o dodatkowe informacje. Dane przetwarzane w celu świadczenia pomocy technicznej są przechowywane przez 4 lata.

Ochrona przed niewłaściwym wykorzystaniem danych. Jeśli utworzysz konto ESET HOME na stronie https://home.eset.com i oznaczysz urządzenie jako zaginione za pomocą funkcji Anti-Theft, będą zbierane i przetwarzane następujące informacje: dane o lokalizacji, zrzuty ekranu, dane o konfiguracji komputera i dane zarejestrowane przez kamerę komputera. Zebrane dane są przechowywane na naszych serwerach lub serwerach naszych usługodawców przez 3 miesiące.

Analiza użycia i awarii urządzenia. Na podstawie Twojej zgody będziemy gromadzić i analizować dane dotyczące korzystania z naszych produktów w celu przetestowania ich wydajności i ulepszenia ich dla naszych użytkowników. Zebrane dane mogą obejmować różne działania użytkownika i zdarzenia mające miejsce w produkcie (na przykład uruchomienie aplikacji, aktualizacja aplikacji, czas trwania sesji, zakup w aplikacji), informacje o używanym urządzeniu, platformie lub systemie operacyjnym, a także dane związane z wiekiem, płcią, lokalizacją i zainteresowaniami, które mogą być powiązane z różnymi identyfikatorami (na przykład identyfikatorami instalacji). Co więcej, będziemy przetwarzać dane techniczne związane z awariami aplikacji (takie

jak informacje o urządzeniu, identyfikator instalacji, ślady oraz pliki minidump awarii), aby uzyskać wgląd w awarie, dowiedzieć się o ich przyczynach i upewnić się, że nasz produkt jest w pełni sprawny. Do zbierania i analizy tych danych korzystamy z Programu poprawy jakości doświadczeń użytkowników (w którym przetwarzane są tylko anonimowe dane telemetryczne) oraz usług Google w celu uzyskania bardziej szczegółowych informacji. Aby dowiedzieć się więcej o przetwarzaniu Twoich danych przez Google, zapoznaj się z odpowiednią Polityką prywatności Google.

Przetwarzanie danych w celach marketingowych. Jeśli zdecydujesz się udzielić nam zgody na przetwarzanie danych w celach marketingowych, wraz z naszymi partnerami marketingowymi wykorzystamy dane dotyczące korzystania z naszego produktu, aby ocenić skuteczność naszych działań marketingowych online, lepiej zrozumieć Twoje zainteresowania i pokazać Ci reklamy online, które powinny być dla Ciebie bardziej odpowiednie. Zebrane dane mogą obejmować różne działania użytkownika i zdarzenia mające miejsce w produkcie (na przykład uruchomienie aplikacji, aktualizacja aplikacji, czas trwania sesji, zakup w aplikacji), informacje o używanym urządzeniu, platformie lub systemie operacyjnym, a także dane związane z wiekiem, płcią, lokalizacją i zainteresowaniami, które mogą być powiązane z różnymi identyfikatorami (identyfikator instalacji, identyfikator reklamy na urządzeniach mobilnych). Te dane gromadzi i analizuje dla nas Google. Aby dowiedzieć się więcej o przetwarzaniu Twoich danych przez Google, zapoznaj się z odpowiednią Polityką prywatności Google.

Należy pamiętać, że jeśli osoba korzystająca z naszych produktów i usług nie jest Użytkownikiem końcowym, który zakupił produkt lub usługę i zawarł z nami Umowę Licencyjną Użytkownika Końcowego (np. pracownik Użytkownika końcowego, członek rodziny lub osoba w inny sposób upoważniona przez Użytkownika końcowego do korzystania z produktu lub usługi zgodnie z umową EULA), przetwarzanie danych odbywa się w uzasadnionym interesie firmy ESET w rozumieniu art. 6 ust. 1 lit. f ustawy RODO, aby umożliwić użytkownikowi upoważnionemu przez Użytkownika końcowego korzystanie z produktów i usług świadczonych przez nas zgodnie z Umową EULA.

Informacje kontaktowe

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