ESET Cyber Security Pro

Gebruikershandleiding

Klik hier om de Help-versie van dit document weer te geven

Digital Security
Progress. Protected.

Copyright ©2023 door ESET, spol. s r.o.

ESET Cyber Security Pro is ontwikkeld door ESET, spol. s r.o.

Ga voor meer informatie naar https://www.eset.com.

Alle rechten voorbehouden. Niets uit deze documentatie mag worden verveelvoudigd, opgeslagen in een geautomatiseerd systeem, of openbaar worden gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, scannen of enige andere manier, zonder schriftelijke toestemming van de auteur.

ESET, spol. s r.o. behoudt zich het recht voor om de beschreven toepassingssoftware zonder voorafgaande kennisgeving te wijzigen.

Technische ondersteuning: https://support.eset.com

REV. 19-3-2023

1 ESET Cyber Security Pro 1
1.1 Wat is er nieuw in versie 6 1
1.2 Systeemvereisten 1
2 Installatie 2
2.1 Standaardinstallatie 2
2.2 Aangepaste installatie 4
2.3 Systeemextensies toestaan 5
2.4 Volledige schijftoegang toestaan 6
3 Productactivering 6
4 Verwijderen 7
5 Basisoverzicht 7
5.1 Sneltoetsen 7
5.2 Beveiligingsstatus controleren 8
5.3 Te volgen procedure als het programma niet correct werkt 8
6 Computerbeveiliging 8
6.1 Antivirus- en antispywarebeveiliging 9
6.1 Algemeen 9
6.1 Uitsluitingen 9
6.1 Beveiliging bij het opstarten 10
6.1 Real-timebeveiliging van bestandssysteem 10
6.1 Geavanceerde opties 11
6.1 Wanneer moet de configuratie voor Real-timebeveiliging worden gewijzigd? 11
6.1 Real-timebeveiliging controleren 11
6.1 Te volgen procedure als Real-timebeveiliging niet werkt 11
6.1 On-demand computerscan 12
6.1 Type scan 13
6.1 Smart scan 13
6.1 Aangepaste scan 13
6.1 Scandoelen 14
6.1 Scanprofielen 14
6.1 Parameters voor ThreatSense-engine instellen 15
6.1 Objecten 15
6.1 Opties 16
6.1 Opschonen 16
6.1 Uitsluitingen 17
6.1 Limiet 17
6.1 Overige 18
6.1 Er is een infiltratie gedetecteerd 18
6.2 Scannen en blokkeren van verwisselbare media 19
7 Antiphishing 20
8 Firewall 20
8.1 Filtermodi 20
8.2 Firewallregels 21
8.2 Nieuwe regels maken 22
8.3 Firewallzones 22
8.4 Firewallprofielen 22
8.5 Firewalllogboeken 22
9 Web- en e-mailbeveiliging 23
9.1 Webbeveiliging 23
9.1 Poorten 23

9.1 URL-lijsten ... 24
9.2 E-mailbeveiliging ... 24
9.2 POP3-protocolcontrole ... 25
9.2 IMAP-protocolcontrole ... 25
10 Ouderlijk toezicht ... 25
11 Bijwerken ... 26
11.1 Instellingen voor bijwerken ... 26
11.1 Geavanceerde opties ... 27
11.2 Updatetaken maken ... 27
11.3 ESET Cyber Security Pro bijwerken naar een nieuwe versie ... 27
11.4 Systeemupdates ... 28
12 Hulpmiddelen ... 29
12.1 Logbestanden ... 29
12.1 Logbestanden onderhouden ... 29
12.1 Logbestanden filteren ... 30
12.2 Planner ... 30
12.2 Nieuwe taken maken ... 31
12.2 Scannen als mapeigenaar ... 32
12.2 Door gebruiker gedefinieerde taken maken ... 33
12.3 Quarantaine ... 33
12.3 Bestanden in quarantaine plaatsen ... 34
12.3 Herstellen vanuit quarantaine ... 34
12.3 Bestand verzenden vanuit quarantaine ... 34
12.4 Actieve processen ... 34
12.5 Netwerkverbindingen ... 35
12.6 Live Grid ... 35
12.6 Live Grid installeren ... 36
12.7 Verzenden van voorbeeld voor analyse ... 37
13 Gebruikersinterface ... 37
13.1 Waarschuwingen en meldingen ... 38
13.1 Waarschuwingen weergeven ... 38
13.1 Beveiligingsstatussen ... 38
13.2 Machtigingen ... 39
13.3 Contextmenu ... 39
13.4 Instellingen importeren en exporteren ... 40
13.5 Proxyserver instellen ... 41
14 Licentieovereenkomst voor eindgebruikers ... 41
15 Privacybeleid ... 48

ESET Cyber Security Pro

ESET Cyber Security Pro vertegenwoordigt een nieuwe benadering van echt geïntegreerde computerbeveiliging. De meest recente versie van de ThreatSense®-scanengine, in combinatie met Beveiliging van e-mailclient, Firewall en Ouderlijk toezicht, houdt uw computer met snelheid en precisie veilig. Het resultaat is een intelligent systeem dat continu alert is en uw computer verdedigt tegen aanvallen en schadelijke software.

ESET Cyber Security Pro is een complete beveiligingsoplossing die voortkomt uit onze jarenlange inspanningen om een maximale beveiliging te combineren met een minimale systeembelasting. De geavanceerde technologieën, gebaseerd op kunstmatige intelligentie, kunnen proactief infiltraties door virussen, wormen, trojaanse paarden, spyware, adware, rootkits en andere aanvallen vanaf internet tegen ESET Cyber Security Pro voorkomen, zonder dat de prestaties van uw systeem daardoor achteruitgaan.

Wat is er nieuw in versie 6

Met ESET Cyber Security Pro versie 6 worden de volgende updates en verbeteringen geïntroduceerd:

- **Ondersteuning voor 64-bits architectuur**
- **Antiphishing**: verhindert dat nepsites zich als betrouwbare websites vermommen en uw persoonlijke informatie proberen te stelen.
- **Systeemupdates**: ESET Cyber Security Pro versie 6 biedt diverse oplossingen en verbeteringen, waaronder meldingen over besturingssysteemupdates. Zie de sectie Systeemupdates voor meer informatie.
- **Beveiligingsstatussen**: verbergt meldingen van het scherm Beveiligingsstatus (bijvoorbeeld *Beveiliging van e-mail uitgeschakeld* of *Computer moet opnieuw worden opgestart*)
- **Te scannen media**: bepaalde mediatypen kunnen worden uitgesloten van de real-timescanner (lokale stations, verwisselbare media, netwerkmedia)
- **Netwerkverbindingen**: geeft netwerkverbindingen op uw computer weer en maakt het mogelijk om regels te maken voor deze verbindingen.

Lees voor meer informatie over de nieuwe functies van ESET Cyber Security Pro het volgende artikel in de ESET-kennisbank:

Systeemvereisten

Voor optimale prestaties van ESET Cyber Security Pro moet uw systeem voldoen aan de volgende hardware- en softwarevereisten:

	Systeemvereisten:
Processorarchitectuur	Intel 64-bit, M1, M2
Besturingssysteem	macOS 10.12 en later
Geheugen	300 MB
Vrije schijfruimte	200 MB

ESET Cyber Security Pro versie 6.10.900.0 en hoger bieden ondersteuning voor Intel, maar nu ook voor de Apple M1- en M2-chip via Rosetta 2

Installatie

Sluit alle programma's op de computer voordat u het installatieproces start. ESET Cyber Security Pro bevat onderdelen die tot conflicten kunnen leiden met andere antivirusprogramma's die op de computer zijn geïnstalleerd. ESET raadt u aan dergelijke antivirusprogramma's te verwijderen om potentiële problemen te voorkomen.

Ga op een van de volgende manieren te werk om de installatiewizard te starten:

- Als u installeert met een bestand dat u hebt gedownload van de ESET-website, opent u het bestand en dubbelklikt u op het pictogram **Installeren**
- Als u het programma installeert vanaf de installatie-cd/dvd, plaatst u deze in de computer, opent u deze vanaf het bureaublad of het **Finder**-venster en dubbelklikt u op het pictogram **Installeren**.



De installatiewizard begeleidt u tijdens de installatie. Tijdens de eerste fase van de installatie zoekt het installatieprogramma automatisch online naar de meest recente productversie. Als er een nieuwere versie wordt gevonden, hebt u de mogelijkheid de nieuwste versie te downloaden alvorens het installatieproces voor te zetten.

Nadat u akkoord bent gegaan met de eindgebruikersovereenkomst wordt u gevraagd een van de volgende installatiemodi te selecteren:

- Standaardinstallatie
- Aangepaste installatie

Standaardinstallatie

Een standaardinstallatiemodus omvat de configuratie-opties die geschikt zijn voor de meeste gebruikers. Deze instellingen bieden maximale veiligheid in combinatie met uitstekende systeemprestaties. De standaardinstallatie

is de standaardoptie en wordt aanbevolen voor degenen zonder speciale vereisten voor bepaalde instellingen.

1.Selecteer de optie van uw voorkeur in het venster **ESET LiveGrid** en klik op **Doorgaan**. Als u later besluit dat u deze instelling wilt wijzigen, kunt u dit doen met behulp van de **LiveGrid-instelling**. Ga voor meer informatie over ESET Live Grid, naar onze woordenlijst.
2.Selecteer in het venster **Potentieel ongewenste toepassingen** de optie van uw voorkeur (zie Wat is een potentieel ongewenste toepassing?) en klik op **Doorgaan**. Als u later besluit dat u deze instelling wilt wijzigen, gebruikt u **Geavanceerde instellingen**.
3.Klik op **Installeren**. Als u wordt gevraagd uw macOS-wachtwoord in te voeren, voert u dit in en klikt u op **Software installeren**.

Na de installatie van ESET Cyber Security Pro:

macOS Big Sur (11)

1.Systeemextensies toestaan.

2.Volledige schijftoegang toestaan

3.ESET toestaan om proxyconfiguraties toe te voegen. U ontvangt de volgende melding: **"**ESET Cyber Security Pro**" wil graag proxyconfiguraties toevoegen**. Wanneer u deze melding ontvangt, klikt u op **Toestaan**. Als u op **Niet toestaan** klikt, werkt Beveiliging van webtoegang niet.

macOS 10.15 en ouder

1.Op macOS 10.13 en later ontvangt u de melding **Systeemuitbreiding geblokkeerd** van uw systeem en de melding **Uw computer is niet beveiligd** van ESET Cyber Security Pro. Als u toegang wilt tot alle functies van ESET Cyber Security Pro, moet u kerneluitbreidingen toestaan op uw apparaat. Om kerneluitbreidingen toe te staan op uw apparaat, navigeert u naar **Systeemvoorkeuren** > **Beveiliging en privacy** en klikt u op **Toestaan** om systeemsoftware toe te staan van de ontwikkelaar **ESET, spol. s.r.o.** Ga voor uitvoerige informatie naar ons kennisbankartikel.

2.Op macOS 10.14 en later ontvangt u de melding **Uw computer is gedeeltelijk beveiligd** van ESET Cyber Security Pro. Als u toegang wilt tot alle functies van ESET Cyber Security Pro, moet u **Toegang tot volledige schijf** toestaan voor ESET Cyber Security Pro. Klik op **Systeemvoorkeuren openen** > **Beveiliging en privacy**. Ga naar het tabblad **Privacy** en selecteer de optie **Toegang tot volledige schijf**. Klik op het hangslotpictogram om bewerken in te schakelen. Klik op het pluspictogram en selecteer de toepassing ESET Cyber Security Pro. Op uw computer wordt een melding weergegeven om uw computer opnieuw op te starten. Klik op **Later**. Start de computer niet opnieuw op nu. Klik op **Opnieuw starten** in het meldingsvenster van ESET Cyber Security Pro of start uw computer opnieuw op. Ga voor uitvoerige informatie naar ons kennisbankartikel.

Na installatie van ESET Cyber Security Pro moet u de computer scannen om op schadelijke code te controleren. Klik in het hoofdvenster van het programma op **Computerscan** > **Smart scan**. Zie het gedeelte Computerscan op aanvraag voor meer informatie over computerscans op aanvraag.

Aangepaste installatie

De modus Aangepaste installatie is bedoeld voor ervaren gebruikers die geavanceerde instellingen willen wijzigen tijdens de installatie.

- **Proxyserver**

Als u een proxyserver gebruikt, geeft u de parameters daarvan op door de optie **Ik gebruik een proxyserver** te selecteren. Typ in het volgende venster het IP-adres of de URL van uw proxyserver in het veld **Adres**. Geef in het veld **Poort** de poort op waarop de proxyserver verbindingen accepteert (standaard is dit 3128). Als de proxyserver verificatie vereist, typt u een geldige **gebruikersnaam** en een geldig **wachtwoord** om toegang te krijgen tot de proxyserver. Als u geen proxyserver gebruikt, selecteert u **Ik gebruik geen proxyserver**. Als u niet zeker weet of u een proxyserver gebruikt, selecteer dan **Systeeminstellingen gebruiken (aanbevolen)** om uw huidige systeeminstellingen te gebruiken.

- **Machtigingen**

Kunt u gemachtigde gebruikers of groepen definiëren die u machtigt om de programmaconfiguratie te bewerken. Selecteer de gebruikers in de lijst aan de linkerkant en klik op **Toevoegen** om hen toe te voegen aan de lijst **Gemachtigde gebruikers**. Als u alle systeemgebruikers wilt weergeven, selecteert u **Alle gebruikers weergeven**. Als u de lijst Gemachtigde gebruikers leeg laat, worden alle gebruikers beschouwd als gemachtigd.

- **ESET LiveGrid®**

Ga voor meer informatie over ESET Live Grid naar onze woordenlijst.

- **Potentieel ongewenste toepassingen**

Ga voor meer informatie over potentieel ongewenste toepassingen naar onze woordenlijst.

- **Firewall**

Kunt u een filtermodus voor de firewall selecteren. Zie het onderwerp Filtermodi voor meer informatie.Na de installatie van ESET Cyber Security Pro:

macOS Big Sur (11)

1.Systeemextensies toestaan.

2.Volledige schijftoegang toestaan

3.ESET toestaan om proxyconfiguraties toe te voegen. U ontvangt de volgende melding: **"**ESET Cyber Security Pro**" wil graag proxyconfiguraties toevoegen**. Wanneer u deze melding ontvangt, klikt u op **Toestaan**. Als u op **Niet toestaan** klikt, werkt Beveiliging van webtoegang niet.

macOS 10.15 en ouder

1.Op macOS 10.13 en later ontvangt u de melding **Systeemuitbreiding geblokkeerd** van uw systeem en de melding **Uw computer is niet beveiligd** van ESET Cyber Security Pro. Als u toegang wilt tot alle functies van ESET Cyber Security Pro, moet u kerneluitbreidingen toestaan op uw apparaat. Om kerneluitbreidingen toe te staan op uw apparaat, navigeert u naar **Systeemvoorkeuren** > **Beveiliging en privacy** en klikt u op **Toestaan** om systeemsoftware toe te staan van de ontwikkelaar **ESET, spol. s.r.o.** Ga voor uitvoerige informatie naar ons kennisbankartikel.

2.Op macOS 10.14 en later ontvangt u de melding **Uw computer is gedeeltelijk beveiligd** van ESET Cyber Security Pro. Als u toegang wilt tot alle functies van ESET Cyber Security Pro, moet u **Toegang tot volledige**

schijf toestaan voor ESET Cyber Security Pro. Klik op **Systeemvoorkeuren openen** > **Beveiliging en privacy**. Ga naar het tabblad **Privacy** en selecteer de optie **Toegang tot volledige schijf**. Klik op het hangslotpictogram om bewerken in te schakelen. Klik op het pluspictogram en selecteer de toepassing ESET Cyber Security Pro. Op uw computer wordt een melding weergegeven om uw computer opnieuw op te starten. Klik op **Later**. Start de computer niet opnieuw op nu. Klik op **Opnieuw starten** in het meldingsvenster van ESET Cyber Security Pro of start uw computer opnieuw op. Ga voor uitvoerige informatie naar ons kennisbankartikel.

Na installatie van ESET Cyber Security Pro moet u de computer scannen om op schadelijke code te controleren. Klik in het hoofdvenster van het programma op **Computerscan** > **Smart scan**. Zie het gedeelte Computerscan op aanvraag voor meer informatie over computerscans op aanvraag.

Systeemextensies toestaan

In macOS 11 (Big Sur) zijn kernelextensies vervangen door systeemextensies. Hiervoor is goedkeuring van de gebruiker nodig voordat nieuwe systeemextensies van derden worden geladen.

Na installatie van ESET Cyber Security Pro op macOS Big Sur (11) en later ontvangt u de melding Systeemextensie geblokkeerd van uw systeem en de melding Uw computer is niet beveiligd van ESET Cyber Security Pro. Als u toegang tot alle functies van ESET Cyber Security Pro wilt hebben, moet u systeemextensies toestaan op uw apparaat.



Upgrade van vorige macOS naar Big Sur.
Als u ESET Cyber Security Pro al hebt geïnstalleerd en gaat upgraden naar macOS Big Sur, moet u de ESET-kernelextensies handmatig toestaan na de upgrade. Fysieke toegang tot de clientcomputer is vereist: wanneer u op afstand toegang hebt, is de knop Toestaan uitgeschakeld.

Wanneer u het ESET-product installeert op macOS Big Sur of hoger, moet u de ESET-systeemextensies handmatig toestaan. Fysieke toegang tot de clientcomputer is vereist: wanneer u op afstand toegang hebt, is deze optie uitgeschakeld.

Systeemextensies handmatig toestaan

1. Klik op **Systeemvoorkeuren** openen of **Beveiligingsvoorkeuren openen** in een van de waarschuwingsdialoogvensters.
2. Klik linksonder op het vergrendelingspictogram om wijzigingen in het instellingenvenster toe te staan.
3. Gebruik uw Touch ID of klik op **Wachtwoord gebruiken** en typ uw gebruikersnaam en wachtwoord, en klik vervolgens op **Ontgrendelen**.
4. Klik op **Details**.
5. Selecteer beide ESET Cyber Security Pro**.app**-opties.
6. Klik op **OK**.

Ga voor een uitvoerige stap-voor-stap gids naar ons kennisbankartikel. (Kennisbankartikelen zijn niet in alle talen beschikbaar.)

Volledige schijftoegang toestaan

Bij macOS 10.14 ontvangt u de melding **Uw computer is gedeeltelijk beveiligd** van ESET Cyber Security Pro. Als u toegang wilt krijgen tot alle ESET Cyber Security Pro-functies, moet u **Volledige schijftoegang** tot ESET Cyber Security Pro toestaan.

1. Klik op **Systeemvoorkeuren openen** in het waarschuwingsdialoogvenster.
2. Klik linksonder op het vergrendelingspictogram om wijzigingen in het instellingenvenster toe te staan.
3. Gebruik uw Touch ID of klik op **Wachtwoord gebruiken** en typ uw gebruikersnaam en wachtwoord, en klik vervolgens op **Ontgrendelen**.
4. Selecteer ESET Cyber Security Pro**.app** in de lijst.
5. Er wordt een melding over het opnieuw starten van ESET Cyber Security Pro weergegeven. Klik op Later.
6. Selecteer ESET **Real-timebeveiliging van bestandssysteem** in de lijst.



ESET Real-timebeveiliging van bestandssysteem niet aanwezig

Als de optie **Real-timebeveiliging van bestandssysteem** niet in de lijst aanwezig is, moet u systeemextensies toestaan voor uw ESET-product.

7. Klik op Opnieuw starten in het ESET Cyber Security Pro-waarschuwingsdialoogvenster of start de computer opnieuw op. Ga voor meer informatie naar ons kennisbankartikel.

Productactivering

Na installatie wordt automatisch het venster Productactivering weergegeven. U kunt het dialoogvenster Productactivering op elk moment oproepen door op het ESET Cyber Security Pro-pictogram te klikken op de macOS-menubalk (boven aan het scherm) en vervolgens op **Productactivering...** te klikken.

- **Licentiecode**: een unieke tekenreeks in de notatie XXXX-XXXX-XXXX-XXXX-XXXX of XXXX-XXXXXXXX die wordt gebruikt om de licentie-eigenaar te identificeren en de licentie te activeren. Als u een versie in de detailhandel hebt aangeschaft, activeert u uw product met een Licentiecode. Deze bevindt zich doorgaans binnen in of op de achterkant van de productverpakking.
- **Gebruikersnaam en wachtwoord**: als u een gebruikersnaam en wachtwoord hebt en niet weet hoe u ESET Cyber Security Pro activeert, klik dan op **Ik heb een gebruikersnaam en wachtwoord. Wat moet ik doen?**. U wordt dan doorverwezen naar my.eset.com, waar u uw referenties kunt omzetten in een Licentiecode.
- **Gratis proeflicentie**: selecteer deze optie als u ESET Cyber Security Pro wilt evalueren voordat u tot aanschaf overgaat. Vul uw e-mailadres in om ESET Cyber Security Pro voor een beperkte tijd te activeren. U ontvangt de testlicentie in een e-mail. Proeflicenties kunnen slechts eenmaal per klant worden geactiveerd.
- **Licentie kopen**: als u geen licentie hebt en er een wilt kopen, klikt u op Licentie kopen. U wordt dan doorgestuurd naar de website van de ESET-distributeur in uw regio.
- **Later activeren**: klik op deze optie als u op dit moment niet wilt activeren.

Verwijderen

Als u ESET Cyber Security Pro wilt verwijderen, kan dit op de volgende manieren:

- plaats de installatie-cd/dvd van ESET Cyber Security Pro in de computer, open deze vanaf het bureaublad of het **Finder**-venster en dubbelklik op **Verwijderen**;
- open het installatiebestand van ESET Cyber Security Pro (*.dmg*) en dubbelklik op **Verwijderen**;
- start **Finder**, open de map **Programma's** op de vaste schijf, druk op CTRL en klik op het pictogram **ESET Cyber Security Pro** , en selecteer **Toon pakketinhoud**. Open de map **Contents** > **Helpers** en dubbelklik op het pictogram **Uninstaller**.

Basisoverzicht

Het hoofdvenster van ESET Cyber Security Pro is onderverdeeld in twee hoofdgedeelten. In het hoofdvenster aan de rechterkant wordt informatie weergegeven over de optie die is geselecteerd in het hoofdmenu aan de linkerkant.

De volgende onderdelen zijn toegankelijk vanuit het hoofdmenu:

- **Start**: biedt informatie over de beveiligingsstatus van uw Computer, Firewall, Web- en e-mailbeveiliging en Ouderlijk toezicht.
- **Computerscan**: in dit gedeelte kunt u de Computerscan op aanvraag configureren en starten.
- **Bijwerken**: hier wordt informatie weergegeven over updates van de detectiemodules.
- **Instellingen**: selecteer deze sectie om het beveiligingsniveau van uw computer aan te passen.
- **Hulpmiddelen**: hier hebt u toegang tot Logbestanden, Planner, Quarantaine, Actieve processen en andere functies van het programma.
- **Help**: hier hebt u toegang tot Help-bestanden, de kennisbank op internet, het aanvraagformulier voor ondersteuning en aanvullende informatie over het programma.

Sneltoetsen

U kunt de volgende sneltoetsen gebruiken wanneer u met ESET Cyber Security Pro werkt:

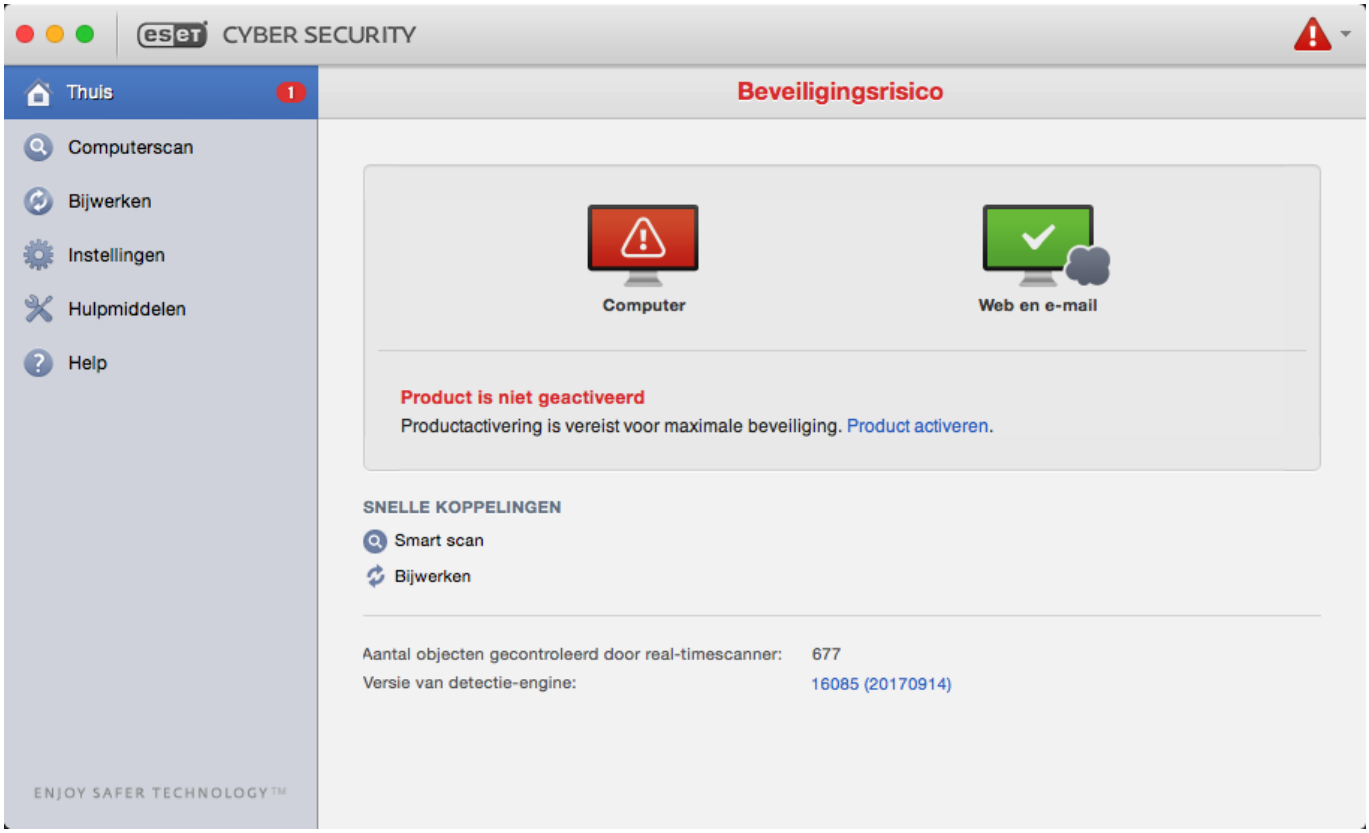
- cmd+,: hiermee geeft u ESET Cyber Security Pro-voorkeuren weer,
- cmd+O: hiermee wijzigt u het formaat van het hoofdvenster van de gebruikersinterface van ESET Cyber Security Pro in het standaardformaat en verplaatst u dit naar het midden van het scherm,
- cmd+Q: hiermee verbergt u het hoofdvenster van de gebruikersinterface van ESET Cyber Security Pro. U opent dit door te klikken op het ESET Cyber Security Pro-pictogram op de macOS-menubalk (boven in het scherm),
- cmd+W: hiermee sluit u het hoofdvenster van de gebruikersinterface van ESET Cyber Security Pro.

De volgende sneltoetsen werken alleen als de optie **Standaardmenu gebruiken** is ingeschakeld onder **Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Interface**:

- cmd+alt+L: hiermee opent u het gedeelte Logbestanden,
- cmd+alt+S: hiermee opent u het gedeelte Planner,
- cmd+alt+Q: hiermee opent u het gedeelte Quarantaine.

Beveiligingsstatus controleren

Klik op **Thuis** in het hoofdmenu als u uw beveiligingsstatus wilt controleren. Er wordt een statusoverzicht over de werking van ESET Cyber Security Pro-modules weergegeven in het hoofdvenster.



Te volgen procedure als het programma niet correct werkt

Wanneer een module correct werkt, wordt er een groen pictogram weergegeven. Wanneer een module niet correct werkt, wordt er een rood uitroepteken of een oranje meldingspictogram weergegeven. Er wordt aanvullende informatie over de module en een voorgestelde oplossing voor het probleem weergegeven. U kunt de status van afzonderlijke modules wijzigen door op de blauwe koppeling onder elk waarschuwingsbericht te klikken.

Als u een probleem niet kunt oplossen met de voorgestelde oplossingen, kunt u zoeken in de ESET-kennisbank zoeken naar een oplossing of contact opnemen met de klantenservice van ESET. De klantenservice zal uw vragen zo spoedig mogelijk beantwoorden en eventuele problemen met ESET Cyber Security Pro oplossen.

Computerbeveiliging

De computerconfiguratie is te vinden in **Instellingen** > **Computer**. Hier wordt de status weergegeven van **Real-timebeveiliging van bestandssysteem** en **Blokkering van verwisselbare media**. U kunt afzonderlijke modules uitschakelen door de knop van de betreffende module om te schakelen naar **UITGESCHAKELD**. Het beveiligingsniveau van de computer kan hierdoor verslechteren. Voor toegang tot gedetailleerde instellingen voor elke module klikt u op **Instellingen...**.

Antivirus- en antispywarebeveiliging

Antivirusbeveiliging beschermt tegen schadelijke aanvallen op het systeem door mogelijk gevaarlijke bestanden te wijzigen. Als een bedreiging via schadelijke code wordt gedetecteerd, kan de antivirusmodule deze onschadelijk maken door de code eerst te blokkeren en deze vervolgens op te schonen, te verwijderen of in quarantaine te plaatsen.

Algemeen

In het gedeelte **Algemeen** (**Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Algemeen**) kunt u detectie van de volgende soorten toepassingen inschakelen:

- **Potentieel ongewenste toepassingen**: grayware of potentieel ongewenste toepassingen (PUA's) is een brede categorie software die niet ontegenzeggelijk schadelijk is als andere typen malware, zoals virussen en Trojaanse paarden. Grayware kan echter aanvullende ongewenste software installeren, het gedrag van het digitale apparaat wijzigen of activiteiten uitvoeren die de gebruiker niet heeft goedgekeurd of had verwacht. Meer informatie over deze typen toepassingen vindt u in de Woordenlijst.
- **Potentieel onveilige toepassingen** - deze toepassingen verwijzen naar commerciële, legitieme software die kan worden misbruikt door aanvallers, als deze wordt geïnstalleerd zonder toestemming van de gebruiker. Deze categorie omvat programma's zoals hulpmiddelen voor externe toegang. Dat is de reden waarom deze optie standaard is uitgeschakeld.
- **Verdachte toepassingen** - deze toepassingen omvatten programma's die zijn gecomprimeerd met packers of protectors. Deze soorten protectors worden vaak door malwareauteurs gebruikt om detectie te omzeilen. Een packer is een zelfuitpakkend uitvoerbaar bestand waarin verschillende soorten malware in één pakket zijn verzameld. De meest gebruikte packers zijn UPX, PE_Compact, PKLite en ASPack. Dezelfde malware kan anders worden gedetecteerd wanneer deze met een andere packer is gecomprimeerd. Packers kunnen hun 'handtekeningen' in de loop van de tijd doen veranderen, waardoor het moeilijker is malware te detecteren en te verwijderen.

Voor het instellen van Uitsluitingen van het bestandssysteem of internet en e-mail klikt u op de knop **Instellen...**.

Uitsluitingen

In het gedeelte **Uitsluitingen** kunt u bepaalde bestanden en mappen, toepassingen of IP/IPv6-adressen opgeven die u wilt uitsluiten van het scannen.

Bestanden en mappen die worden vermeld op het tabblad **Bestandssysteem** worden van alle scanners uitgesloten: Opstarten, Real-time en On-demand (Computerscan).

- **Pad**: het pad naar uitgesloten bestanden en mappen.
- **Bedreiging**: als er naast een uitgesloten bestand de naam van een bedreiging wordt weergegeven, betekent dit dat het bestand alleen wordt uitgesloten voor de betreffende bedreiging, maar niet volledig. Als het bestand later wordt geïnfecteerd door andere malware, wordt het bestand gedetecteerd door de antivirusmodule.
- : hiermee wordt een nieuwe uitsluiting gemaakt. Voer het pad in naar een object (u kunt ook de jokertekens * en ? gebruiken) of selecteer de map of het bestand in de boomstructuur.

- : hiermee worden geselecteerde vermeldingen verwijderd
- **Standaard**: hiermee worden alle uitsluitingen geannuleerd

Op het tabblad **Web en e-mail** kunt u bepaalde **Toepassingen** of **IP/IPv6-adressen** uitsluiten van protocolscannen.

Beveiliging bij het opstarten

Met Opstartbestanden controleren worden bestanden automatisch gescand bij het opstarten van het systeem. Deze scan wordt standaard regelmatig als een geplande taak uitgevoerd nadat de gebruiker zich heeft aangemeld of na een update van de detectiemodules. Voor het wijzigen van de parameterinstellingen voor de ThreatSense-engine die van toepassing zijn op het scannen bij het opstarten, klikt u op de knop **Instellen**. Meer informatie over het instellen van de ThreatSense-engine vindt u in deze sectie.

Real-timebeveiliging van bestandssysteem

De real-timebeveiliging van het bestandssysteem controleert alle typen media en de scan wordt geactiveerd door verschillende gebeurtenissen. Real-timebeveiliging van het bestandssysteem door ThreatSense-technologie (beschreven in Parameters voor ThreatSense-engine instellen) kan voor nieuw gemaakte bestanden anders zijn dan voor reeds bestaande bestanden. Nieuwe bestanden kunnen nauwkeuriger worden beheerd.

Standaard worden alle bestanden gescand op het moment dat ze worden **geopend**, **gemaakt** of **uitgevoerd**. Wij adviseren u deze standaardinstellingen te handhaven aangezien deze uw computer het hoogste niveau van Real-timebeveiliging bieden. Real-timebeveiliging wordt gestart bij het opstarten van het systeem en scant ononderbroken. In speciale gevallen (zoals bij een conflict met een andere real-timescanner) kan de real-timebeveiliging worden beëindigd door op de menubalk (boven aan het scherm) op het pictogram ESET Cyber Security Pro te klikken (boven aan het scherm. Selecteer daarna **Real-timebeveiliging van bestandssysteem uitschakelen**. U kunt de real-timebeveiliging van bestanden ook in het hoofdvenster van het programma uitschakelen (klik op **Instellen** > **Computer** en zet **Real-timebeveiliging van bestandsysteem** op **UITGESCHAKELD**).

De volgende mediatypen kunnen worden uitgesloten bij de scanner voor Real-time:

- **Lokale stations**: systeemschijven
- **Verwisselbare media**: cd's/dvd's, USB-media, Bluetooth-apparaten, enz.
- **Netwerkmedia**: alle gekoppelde stations

Het wordt aangeraden de standaardinstellingen te gebruiken en scanuitsluitingen alleen in specifieke gevallen te wijzigen, bijvoorbeeld wanneer het scannen van bepaalde media tot aanzienlijke vertragingen in de gegevensoverdracht leidt.

Als u geavanceerde instellingen voor Real-timebeveiliging van bestandssysteem wilt wijzigen, gaat u naar **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,* > **Real-timebeveiliging** en klik op **Instellen...** naast **Geavanceerde opties** (beschreven in Geavanceerde scanopties).

Geavanceerde opties

In dit venster kunt u definiëren welke objecttypen door de ThreatSense-engine worden gescand. Voor meer informatie over **Zelfuitpakkende archieven**, **Software voor runtime-compressie** en **Geavanceerde heuristiek**, verwijzen wij u naar Parameters voor ThreatSense-engine instellen.

We raden niet aan wijzigingen aan te brengen in het gedeelte **Standaardarchiefinstellingen**, tenzij u een specifiek probleem wilt oplossen, aangezien hogere nestingsniveaus voor archieven de systeemprestaties negatief kunnen beïnvloeden.

ThreatSense-parameters voor uitgevoerde bestanden: standaard wordt **Geavanceerde heuristiek** gebruikt wanneer bestanden worden uitgevoerd. Wij raden ten zeerste aan Smart-optimalisatie en ESET Live Grid ingeschakeld te laten om negatieve gevolgen voor de systeemprestaties te beperken.

Compatibiliteit van netwerkvolumes vergroten: met deze optie verbetert u de prestaties wanneer bestanden via het netwerk worden geopend. Deze optie moet worden ingeschakeld als u met vertragingen te maken krijgt wanneer bestanden op netwerkstations worden geopend. Deze functie maakt op macOS 10.10 en later gebruik van de systeembestandcoördinator. Niet alle toepassingen ondersteunen de systeembestandcoördinator. Microsoft Word 2011 bijvoorbeeld ondersteunt deze functie niet en Word 2016 wel.

Wanneer moet de configuratie voor Real-timebeveiliging worden gewijzigd?

Real-timebeveiliging is het meest essentiële onderdeel om een systeem veilig te houden met ESET Cyber Security Pro. Wees voorzichtig bij het aanpassen van de parameters voor Real-timebeveiliging. Wij adviseren u deze parameters alleen te wijzigen in specifieke situaties. Bijvoorbeeld een situatie waarin er een conflict is met een bepaalde toepassing.

Na installatie van ESET Cyber Security Pro zijn alle instellingen geoptimaliseerd om gebruikers een zo hoog mogelijk niveau van systeembeveiliging te bieden. U kunt de standaardinstellingen herstellen door te klikken op **Standaard** linksonder in het venster **Real-timebeveiliging** (**Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Real-timebeveiliging**).

Real-timebeveiliging controleren

Download het eicar.com-testbestand en controleer of ESET Cyber Security Pro dit als bedreiging detecteert zodat u zeker weet dat Real-timebeveiliging werkt en virussen detecteert. Dit testbestand is een speciaal, onschadelijk bestand dat door alle virusprogramma's kan worden gedetecteerd. Het bestand is gemaakt door EICAR (European Institute for Computer Antivirus Research) om de werking van antivirusprogramma's te testen.

Te volgen procedure als real-timebeveiliging niet werkt

In dit hoofdstuk worden probleemsituaties beschreven die zich kunnen voordoen bij het gebruik van Real-timebeveiliging, en oplossingen hiervoor.

Real-timebeveiliging is uitgeschakeld

Als Real-timebeveiliging per ongeluk is uitgeschakeld door de gebruiker, moet Real-timebeveiliging opnieuw worden geactiveerd. U kunt Real-timebeveiliging opnieuw activeren door in het hoofdmenu te klikken op **Instellingen** > **Computer** en **Real-timebeveiliging van bestandssystemen** op **INGESCHAKELD** te zetten. U kunt Real-timebeveiliging van bestandssysteem ook inschakelen in het venster met voorkeuren voor de toepassing onder **Real-timebeveiliging** door **Real-timebeveiliging van bestandssysteem inschakelen** te selecteren.

Real-time beveiliging voert geen detecties uit en schoont geen infiltraties op

Controleer of er geen andere antivirusprogramma's zijn geïnstalleerd op de computer. Als twee programma's voor real-timebeveiliging tegelijk zijn geactiveerd, conflicteren deze mogelijk. Wij adviseren u alle eventuele andere antivirusprogramma's van uw systeem te verwijderen.

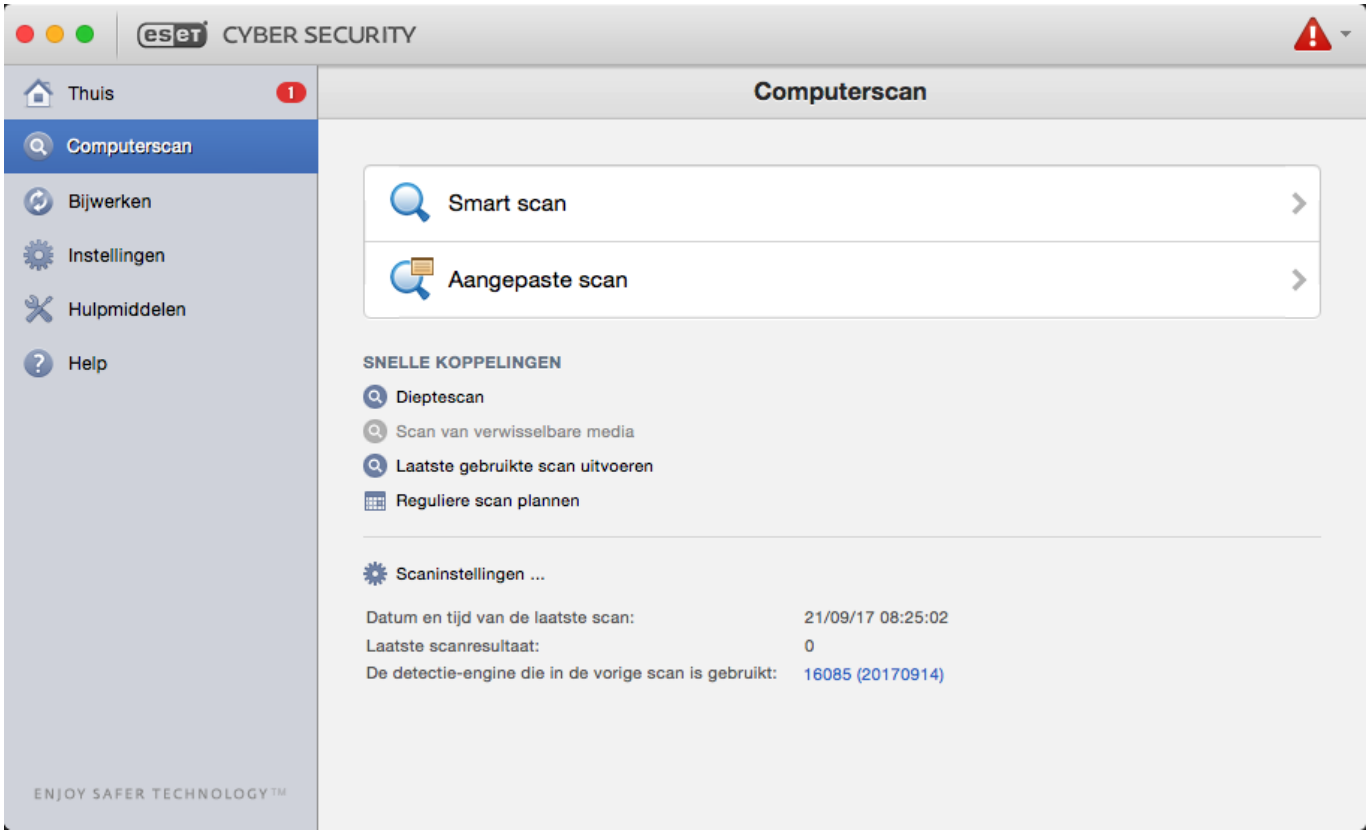
Real-timebeveiliging wordt niet gestart

Als real-timebeveiliging niet wordt geactiveerd wanneer u het systeem opstart, zijn er mogelijk conflicten met andere programma's. Als dat het geval is, neem dan contact op met ESET Klantenservice.

On-demand computerscan

Als u vermoedt dat de computer is geïnfecteerd (deze gedraagt zich abnormaal), voert u **Smart scan** uit om uw computer te onderzoeken op infiltraties. Voor een optimale beveiliging is het van belang regelmatig een computerscan uit te voeren als onderdeel van routinematige beveiligingsmaatregelen, niet alleen wanneer u vermoedt dat de computer is geïnfecteerd. Door regelmatig te scannen kunnen infiltraties worden gedetecteerd die niet door de real-timescanner zijn gedetecteerd op het moment van opslag op de schijf. Dit kan gebeuren als de real-timescanner was uitgeschakeld op het moment van infectie of de detectiemodules verouderd waren.

Wij adviseren u minimaal eenmaal per maand een on-demand scan uit te voeren. Scannen kan worden geconfigureerd als een geplande taak in **Hulpmiddelen** > **Planner**.



Type scan

Er zijn twee typen on-demand computerscan beschikbaar. Gebruik een **Smart scan** om het systeem snel zonder verdere configuratie van de scanparameters te scannen. Met een **Aangepaste scan** kunt u elk van de vooraf gedefinieerde scanprofielen selecteren en specifieke scandoelen opgeven.

Smart scan

Met Smart scan kunt u snel een computerscan starten en geïnfecteerde bestanden opschonen zonder dat er gebruikersinterventie is vereist. Het belangrijkste voordeel is de eenvoudige werking zonder gedetailleerde scanconfiguratie. Smart scan controleert alle bestanden in alle mappen en schoont automatisch gedetecteerde infiltraties op of verwijdert deze. Het opschoonniveau wordt automatisch ingesteld op de standaardwaarde. Zie het gedeelte over Opschonen voor meer informatie over typen opschoonbewerkingen.

Aangepaste scan

Aangepaste scan is een optimale oplossing als u scanparameters wilt opgeven, zoals scandoelen en scanmethoden. Het voordeel van het uitvoeren van een aangepaste scan is de mogelijkheid om de parameters in detail te configureren. Verschillende configuraties kunnen worden opgeslagen in door de gebruiker gedefinieerde scanprofielen. Deze profielen zijn met name handig als het scannen herhaaldelijk plaatsvindt met dezelfde parameters.

Als u scandoelen wilt selecteren, selecteert u **Computerscan** > **Aangepaste scan** en selecteert u vervolgens specifieke **Scandoelen** in de boomstructuur. Een scandoel kan tevens nader worden gespecificeerd door het pad naar de map met het bestand of de bestanden die u wilt opnemen in te voeren. Als u alleen het systeem wilt

scannen zonder aanvullende opschoonacties, selecteer dan **Scannen zonder opschonen**. Bovendien kunt u een keuze maken uit drie opschoonniveaus door op **Instellingen** > **Opschonen** te klikken.

> **Aangepaste scan**
> Het uitvoeren van computerscans met Aangepaste scan wordt aanbevolen voor ervaren gebruikers die eerder antivirusprogramma's hebben gebruikt.

Scandoelen

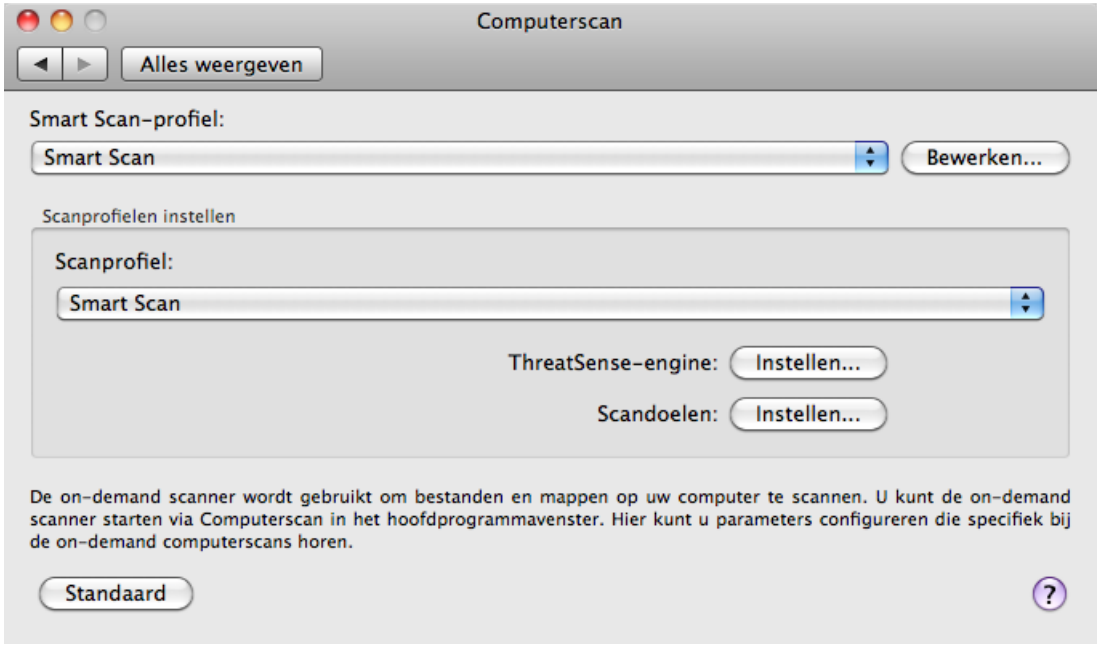
In de boomstructuur met scandoelen kunt u bestanden en mappen selecteren de u op virussen wilt scannen. Mappen kunnen ook worden geselecteerd aan de hand van de instellingen van een profiel.

Een scandoel kan nader worden gespecificeerd door het pad naar de map met het bestand of de bestanden die u wilt opnemen in de scan in te voeren. Selecteer doelen in de boomstructuur met alle mappen die beschikbaar zijn op de computer door het selectievakje bij de bijbehorende bestanden of mappen in te schakelen.

Scanprofielen

U kunt uw voorkeursinstellingen voor scannen opslaan voor toekomstige scans. Wij adviseren u voor elke regelmatig gebruikte scan een ander profiel te maken (met verschillende scandoelen, scanmethoden en andere parameters).

Als u een nieuw profiel wilt maken, klik dan in het hoofdmenu op **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Computerscan** en klik op **Bewerken...** naast de lijst met huidige profielen.



Raadpleeg het gedeelte Parameters voor ThreatSense-engine instellen voor een beschrijving van elke parameter van de scaninstellingen, zodat u een scanprofiel kunt maken dat aan uw behoeften voldoet.

Voorbeeld: Stel, u wilt een eigen scanprofiel maken en de Smart scan-configuratie is deels geschikt, maar u wilt geen programma's voor runtime-compressie of potentieel onveilige toepassingen scannen en u wilt ook Volledig opschonen toepassen. Voer de profielnaam in het venster **Profielenlijst voor on-demand scanner** in, klik op de

knop **Toevoegen** en bevestig uw keuze met **OK**. Pas vervolgens de parameters aan uw vereisten aan door de **ThreatSense-engine** en **Scandoelen** in te stellen.

Als u het besturingssysteem wilt uitschakelen en de computer wilt afsluiten nadat de on-demand scan is voltooid, gebruikt u de optie **Computer afsluiten na scan**.

Parameters voor ThreatSense-engine instellen

ThreatSense is een exclusieve technologie van ESET die bestaat uit een combinatie van complexe methoden voor de detectie van dreigingen. Deze technologie is proactief. Dit betekent dat tevens beveiliging wordt geboden tijdens de eerste uren van de verspreiding van een nieuwe bedreiging. Er wordt gebruik gemaakt van een combinatie van verschillende methoden (codeanalyse, code-emulatie, generieke kenmerken enz.) die samenwerken om de systeembeveiliging aanzienlijk te verbeteren. De scanengine is in staat verschillende gegevensstromen tegelijk te besturen voor een maximale efficiëntie en een zo hoog mogelijk detectiepercentage. De ThreatSense-technologie zorgt tevens voor de verwijdering van rootkits.

Via de instellingsopties voor de ThreatSense-technologie kunt u verschillende scanparameters opgeven:

- Bestandstypen en extensies die moeten worden gescand
- De combinatie van verschillende detectiemethoden
- Opschoonniveaus, enz.

U opent het instellingenvenster door te klikken op **Instellen > Voorkeuren voor toepassing opgeven** (of druk op *cmd+,*) en klik op de knop ThreatSense-engine **instellen** in de module **Beveiliging bij het opstarten**, **Real-timebeveiliging** en **Computerscan**, die allemaal gebruikmaken van ThreatSense-technologie (zie hieronder). Verschillende beveiligingsscenario's vereisen mogelijk verschillende configuraties. ThreatSense is individueel configureerbaar voor de volgende beveiligingsmodules:

- **Beveiliging bij het opstarten**: automatisch bestanden controleren bij het opstarten
- **Real-timebeveiliging**: Real-timebeveiliging van bestandssysteem
- **Computerscan**: on-demand computerscan.
- **Beveiliging van webtoegang**
- **E-mailbeveiliging**

De ThreatSense-parameters zijn speciaal geoptimaliseerd voor elke module en wijziging hiervan kan een aanzienlijke invloed hebben op de werking van het systeem. Als bijvoorbeeld instellingen voor het altijd scannen van programma's voor runtime-compressie worden gewijzigd of als geavanceerde heuristiek wordt ingeschakeld in de module Real-timebeveiliging van bestandssysteem, zou dit kunnen resulteren in een vertraging van het systeem. Daarom adviseren wij de standaard ThreatSense-parameters ongewijzigd te laten voor alle modules met uitzondering van Computerscan.

Objecten

In het gedeelte **Objecten** kunt u definiëren welke bestanden worden gescand op infiltraties.

- **Symbolische koppelingen** - (alleen computerscan) scant bestandstypen die een tekenreeks bevatten die door

het besturingssysteem wordt geïnterpreteerd en gevolgd als een pad naar een ander bestand of een andere map.

• **E-mailbestanden** - (niet beschikbaar in real-timebeveiliging) scant e-mailbestanden.

• **Postvakken** - (niet beschikbaar in real-timebeveiliging) scant postvakken van gebruikers in het systeem. Onjuist gebruik van deze optie kan leiden tot een conflict met uw e-mailclient. Meer informatie over de voor- en nadelen van deze optie vindt u in dit knowledgebase-artikel.

• **Archieven** - (niet beschikbaar in real-timebeveiliging) scant bestanden die zijn gecomprimeerd in archieven (RAR, ZIP, ARJ, TAR, enz.).

• **Zelfuitpakkende archieven** - (niet beschikbaar in real-timebeveiliging) scant bestanden die deel uitmaken van zelfuitpakkende archiefbestanden.

• **Software voor runtime-compressie** - programma's voor runtime-compressie decomprimeren in het geheugen (in tegenstelling tot standaardarchieftypen). Als dit is geselecteerd, worden standaardprogramma's voor statische compressie (zoals UPX, yoda, ASPack, FGS) ook gescand.

Opties

In het gedeelte **Opties** kunt u de methoden selecteren die moeten worden gebruikt tijdens het scannen van het systeem. De volgende opties zijn beschikbaar:

• **Heuristiek**: heuristiek maakt gebruik van een algoritme dat de (schadelijke) activiteit van programma's analyseert. Het voornaamste voordeel van heuristieke detectie is de mogelijkheid om nieuwe schadelijke software te detecteren die eerder nog niet bestond.

• **Geavanceerde heuristiek**: geavanceerde heuristiek bestaat uit een uniek heuristisch algoritme dat door ESET is ontwikkeld en dat is geoptimaliseerd voor het detecteren van computerwormen en trojaanse paarden. Dit algoritme is geschreven in programmeertalen van hoog niveau. De geavanceerde heuristiek breidt de detectiemogelijkheden van het programma aanzienlijk uit.

Opschonen

De instellingen voor het opschonen bepalen op welke manier de scanner geïnfecteerde bestanden opschoont. Er zijn 3 opschoonniveaus:

• **Niet opschonen**: geïnfecteerde bestanden worden niet automatisch opgeschoond. Er wordt een waarschuwingsvenster weergegeven en u kunt een actie kiezen.

• **Standaard opschonen**: er wordt automatisch geprobeerd een geïnfecteerd bestand op te schonen of te verwijderen. Als het niet mogelijk is de juiste actie automatisch te selecteren, wordt een selectie van vervolgacties aangeboden. De beschikbare vervolgacties worden tevens weergegeven als een vooraf gedefinieerde actie niet kon worden voltooid.

• **Volledig opschonen**: alle geïnfecteerde bestanden (inclusief archieven) worden opgeschoond of verwijderd. Dit geldt niet voor systeembestanden. Als het niet mogelijk is een bestand op te schonen, ontvangt u een melding en wordt u gevraagd een type actie te selecteren.

Bestanden archiveren

in de modus Standaard opschonen worden hele archiefbestanden alleen verwijderd als alle bestanden in het archief zijn geïnfecteerd. Als een archief legitieme bestanden bevat evenals geïnfecteerde bestanden, wordt het niet verwijderd. Als een geïnfecteerd archiefbestand wordt gedetecteerd in de modus Volledig opschonen, wordt het gehele archief verwijderd, zelfs als er schone bestanden aanwezig zijn.

Archieven scannen

In de modus Standaard opschonen worden gehele archiefbestanden alleen verwijderd als alle bestanden in het archief zijn geïnfecteerd. Als een archief legitieme bestanden bevat evenals geïnfecteerde bestanden, wordt het niet verwijderd. Als een geïnfecteerd archiefbestand wordt gedetecteerd in de modus Volledig opschonen, wordt het gehele archief verwijderd, zelfs als er schone bestanden aanwezig zijn.

Uitsluitingen

Een extensie maakt deel uit van een bestandsnaam en wordt afgebakend door een punt. De extensie definieert het type en de inhoud van een bestand. In dit gedeelte van de instellingen voor ThreatSense-parameters kunt u de typen bestanden definiëren die u wilt uitsluiten van scannen.

Standaard worden alle bestanden gescand, ongeacht hun extensie. Elke extensie kan worden toegevoegd aan de lijst met bestanden die zijn uitgesloten van scannen. Met de knoppen + en − kunt u het scannen van specifieke extensies inschakelen of verbieden.

Het uitsluiten van bestanden van scannen is soms nodig als het scannen van bepaalde bestandstypen een onjuiste werking veroorzaakt van het programma. Het kan bijvoorbeeld raadzaam zijn om *log*-, *cfg*- en *tmp*-bestanden uit te sluiten. De juiste notatie voor het invoeren van bestandextensies is:

log

cfg

tmp

Limiet

Gebruik het gedeelte **Limiet** om de maximale grootte op te geven van objecten die moeten worden gescand, evenals het maximale niveau voor het scannen van geneste archieven:

- **Maximumgrootte:** de maximale grootte van objecten die moeten worden gescand. Wanneer de maximale grootte is gedefinieerd, scant de antivirusmodule uitsluitend objecten die kleiner zijn dan de opgegeven grootte. De waarde mag alleen worden gewijzigd door gevorderde gebruikers die een specifieke reden hebben om grotere objecten niet te scannen.
- **Maximumscantijd:** de maximale tijd voor het scannen van een object. Als hier een door de gebruiker gedefinieerde waarde is ingevoerd, wordt het scannen van een object beëindigd wanneer die tijd is verstreken, ongeacht of de scan is voltooid.
- **Maximumnestingsniveau:** het maximum aantal niveaus waarop archieven moeten worden gescand. Het is in

de meeste gevallen niet nodig de standaardwaarde van 10 te wijzigen. Als het scannen voortijdig wordt afgebroken omdat archieven dieper dan 10 niveaus zijn genest, blijft het archief ongecontroleerd.

- **Maximumbestandsgrootte:** gebruik deze optie om de maximale bestandsgrootte op te geven voor bestanden in archieven (als deze worden uitgepakt) die moeten worden gescand. Als het scannen van een archief vanwege deze limiet voortijdig wordt afgebroken, blijft het archief ongecontroleerd.

Overige

Smart-optimalisatie inschakelen

Wanneer Smart-optimalisatie is ingeschakeld, worden de instellingen geoptimaliseerd om het meest efficiënte scanniveau te garanderen, zonder dat dit ten koste gaat van de scansnelheid. De diverse beveiligingsmodules scannen op intelligente wijze, waarbij gebruik wordt gemaakt van verschillende scanmethoden. De Smart-optimalisatie is niet strikt gedefinieerd in het product. Het ontwikkelingsteam van ESET implementeert continu nieuwe wijzigingen, die vervolgens via de regelmatige updates worden geïntegreerd in ESET Cyber Security Pro. Als de Smart-optimalisatie is uitgeschakeld, worden alleen de door de gebruiker gedefinieerde instellingen in de ThreatSense-technologie van de betreffende module toegepast bij het uitvoeren van een scan.

Alternatieve gegevensstromen scannen (alleen on-demand scanner)

Alternatieve gegevensstromen die worden gebruikt door het bestandssysteem zijn bestands- en mapkoppelingen die onzichtbaar zijn voor normale scantechnieken. Veel infiltraties proberen detectie te vermijden door zichzelf te vermommen als alternatieve gegevensstromen.

Er is een infiltratie gedetecteerd

Infiltraties kunnen het systeem via verschillende toegangspunten bereiken: webpagina's, gedeelde mappen, e-mail of verwisselbare computermedia (USB, externe schijven, cd's, dvd's enz.).

Als de computer tekenen van infectie door malware vertoont, bijvoorbeeld als deze trager is, vaak vastloopt, enz., adviseren wij u het volgende te doen:

1. Klik op **Computerscan**.
2. Klik op **Smart scan** (zie het gedeelte Smart scan voor meer informatie).
3. Nadat de scan is voltooid, controleert u in het logbestand het aantal gescande, geïnfecteerde en opgeschoonde bestanden.

Als u alleen een bepaald gedeelte van uw schijf wilt scannen, klikt u op **Aangepaste scan** en selecteert u doelen die u wilt scannen op virussen.

Als algemeen voorbeeld van hoe infiltraties worden afgehandeld door ESET Cyber Security Pro, gaan we ervan uit dat een infiltratie is gedetecteerd door de real-timebewaking van het bestandssysteem, welke gebruikmaakt van het standaardopschoonniveau. De real-timebewaking probeert het bestand op te schonen of te verwijderen. Als er geen vooraf gedefinieerde actie beschikbaar is voor de module voor real-timebeveiliging, wordt u via een waarschuwingsvenster gevraagd om een optie te selecteren. Gewoonlijk zijn de opties **Opschonen**, **Verwijderen** en **Geen actie** beschikbaar. Het wordt niet aanbevolen **Geen actie** te selecteren, aangezien de geïnfecteerde bestanden dan geïnfecteerd zouden blijven. Deze optie is bedoeld voor situaties waarin u zeker weet dat het bestand onschadelijk is en per ongeluk is gedetecteerd.

Opschonen en verwijderen

Pas opschonen toe als een bestand is aangevallen door een virus dat schadelijke code aan het bestand heeft toegevoegd. Als dit het geval is, probeert u eerst het geïnfecteerde bestand op te schonen zodat het in de oorspronkelijke staat kan worden hersteld. Als het bestand uitsluitend uit schadelijke code bestaat, wordt het verwijderd.



Bestanden in archieven verwijderen

In de modus Standaard opschonen wordt het volledige archief alleen verwijderd als dit uitsluitend geïnfecteerde en geen schone bestanden bevat. Met andere woorden, archieven worden niet verwijderd als zij ook onschadelijke, schone bestanden bevatten. Wees echter voorzichtig bij het gebruik van een scan in de modus **Volledig opschonen**: met Volledig opschonen wordt het archief verwijderd als het minimaal één geïnfecteerd bestand bevat, ongeacht de status van andere bestanden in het archief.

Scannen en blokkeren van verwisselbare media

ESET Cyber Security Pro kan een on-demand scan uitvoeren van geplaatste verwisselbare geheugenapparaten (cd, dvd, USB, enz.). Op macOS 10.15 kan ESET Cyber Security Pro ook andere externe media-apparaten scannen.

Scannen van verwisselbare media op macOS 11 en hoger

ESET Cyber Security Pro geïnstalleerd op macOS 11 en hoger scant alleen geheugenapparaten.



Verwisselbare media kunnen schadelijke code bevatten en uw computer in gevaar brengen. Als u verwisselbare media wilt blokkeren, klikt u op de knop **Mediablokkering instellen** (zie de bovenstaande afbeelding) of **Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Media** in het hoofdvenster van het programma en selecteert u de optie **Blokkering van verwijderbare media inschakelen**. Als u toegang tot bepaalde typen media wilt toestaan, heft u de selectie van de gewenste mediavolumes op.

Toegang tot cd-rom

Als u toegang wilt geven tot een extern cd-romstation dat via een USB-kabel op uw computer is aangesloten, schakelt u de optie **Cd-rom** uit.

Antiphishing

De term phishing verwijst naar een criminele activiteit waarbij gebruik wordt gemaakt van 'sociale engineering'. Hierbij worden gebruikers gemanipuleerd met als doel het verkrijgen van vertrouwelijke informatie. Met phishing wordt vaak geprobeerd toegang te krijgen tot gevoelige gegevens zoals bankrekeningnummers, creditcardnummers, pincodes of gebruikersnamen en wachtwoorden.

Wij raden u aan om Antiphishing ingeschakeld te laten (**Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Antiphishing-beveiliging**). Alle potentiële phishingaanvallen die afkomstig zijn van gevaarlijke websites of domeinen, worden geblokkeerd en er wordt een waarschuwing weergegeven die u op de hoogte stelt van de aanval.

Firewall

De firewall beheert alle netwerkwerkverkeer naar en van het systeem door afzonderlijke netwerkverbindingen toe te staan of te weigeren op basis van opgegeven filterregels. De firewall biedt bescherming tegen aanvallen van externe computers en maakt het blokkeren van bepaalde services mogelijk. Hij biedt ook antivirusbeveiliging voor de protocollen HTTP, POP3 en IMAP.

Scanuitzonderingen

ESET Cyber Security Pro scant niet de versleutelde protocollen HTTPS, POP3S en IMAPS.

De firewallconfiguratie is te vinden in **Instellingen** > **Firewall**. Hier kunt u de filtermodus, regels en gedetailleerde instellingen aanpassen. Daarnaast kunt u van hieruit toegang krijgen tot meer gedetailleerde instellingen van het programma.

Als u **Alle netwerkverkeer blokkeren: verbinding met netwerk verbreken** op **INGESCHAKELD** zet, wordt alle binnenkomende en uitgaande communicatie door de firewall geblokkeerd. Gebruik deze optie alleen als u vermoedt dat het systeem vanwege kritieke beveiligingsrisico's moet worden afgesloten van het netwerk.

Filtermodi

Er zijn drie filtermodi beschikbaar voor de firewall van ESET Cyber Security Pro. Instellingen voor filtermodi zijn te vinden bij de voorkeuren van ESET Cyber Security Pro (druk op *cmd+,*) > **Firewall**. Het gedrag van de firewall verandert op basis van de geselecteerde modus. Filtermodi zijn ook van invloed op de benodigde mate van gebruikersinteractie.

Al het verkeer geblokkeerd: alle binnenkomende en uitgaande verbindingen worden geblokkeerd.

Automatisch met uitzonderingen: de standaardmodus. Deze modus is geschikt voor gebruikers die de voorkeur geven aan eenvoudig en handig gebruik van de firewall, zonder regels te hoeven definiëren. De automatische modus staat al het standaard uitgaande verkeer voor het opgegeven systeem toe en blokkeert alle niet-geïnitieerde verbindingen die van de netwerkkant tot stand worden gebracht. U kunt ook aangepaste, door de gebruiker gedefinieerde regels toevoegen.

Interactieve modus: hiermee kunt u een aangepaste configuratie instellen voor uw firewall. Wanneer er communicatie wordt gedetecteerd waarop geen bestaande regels van toepassing zijn, wordt er een dialoogvenster weergegeven waarin een onbekende verbinding wordt gemeld. Het dialoogvenster biedt de optie de communicatie toe te staan of te weigeren. De beslissing om toe te staan of te weigeren kan worden onthouden als een nieuwe regel voor de firewall. Als u er nu voor kiest een nieuwe regel te maken, worden alle toekomstige verbindingen van dit type toegestaan of geblokkeerd aan de hand van de regel.



Als u gedetailleerde informatie over alle geblokkeerde verbindingen wilt vastleggen in een logbestand, selecteer dan **Alle geblokkeerde verbindingen vastleggen in logboek**. Als u de logboeken van de firewall wilt controleren, klik dan in het hoofdmenu op **Hulpmiddelen** > **Logboeken** en selecteer **Firewall** in het vervolgkeuzemenu **Logboek**.

Firewallregels

Firewallregels zijn een reeks condities die worden gebruikt om alle netwerkverbindingen te testen en alle acties voor deze condities te bepalen. Met de firewallregels kunt u definiëren welke actie moet worden ondernomen als een door de regel gedefinieerde verbinding tot stand wordt gebracht.

Binnenkomende verbindingen zijn afkomstig van een externe computer die een verbinding tot stand probeert te brengen met het lokale systeem. Uitgaande verbindingen werken andersom. Het lokale systeem maakt contact met een externe computer.

Als er nieuwe, onbekende communicatie wordt gedetecteerd, moet u zorgvuldig overwegen of u deze toestaat of weigert. Ongevraagde, niet beveiligde of onbekende verbindingen vormen een beveiligingsrisico voor het systeem. Als een dergelijke verbinding tot stand wordt gebracht, raden we u aan speciale aandacht te besteden aan de externe computer en de toepassing die probeert verbinding te maken met uw computer. Veel infiltraties proberen persoonlijke gegevens te verkrijgen en verzenden, of downloaden andere schadelijke toepassingen naar hostwerkstations. De firewall stelt u in staat dergelijke verbindingen te detecteren en te beëindigen.

Standaard kunnen toepassingen die zijn ondertekend door Apple automatisch toegang krijgen tot het netwerk.

Als u deze mogelijkheid wilt uitschakelen, schakel **Software die is ondertekend door Apple automatisch netwerktoegang geven** dan uit.

Nieuwe regels maken

Op het tabblad **Regels** staat een lijst met alle regels die worden toegepast op het verkeer dat door afzonderlijke toepassingen wordt gegenereerd. Regels worden automatisch toegevoegd aan de hand van reacties van de gebruiker op elke nieuwe communicatie.

1. Als u een nieuwe regel wilt maken, klikt u op **Toevoegen**, typt u een naam voor de regel en sleept u het pictogram van de toepassing naar het lege veld en zet u het daar neer, of klikt u op **Bladeren** om het programma te zoeken in de map */Applications*. Als u de regel wilt toepassen op alle toepassingen die op de computer zijn geïnstalleerd, selecteert u de optie **Alle toepassingen**.

2. Geef in het volgende venster de **Actie** op (de communicatie tussen de geselecteerde toepassing en het netwerk toestaan of weigeren) en de **Richting** van de communicatie (binnenkomend, uitgaand of beide). U kunt alle communicatie met betrekking tot deze regel vastleggen in een logboekbestand. Schakel hiervoor de optie **Logboekregel** in. Als u de logboeken wilt controleren, klikt u in het hoofdmenu van ESET Cyber Security Pro op **Hulpmiddelen** > **Logboeken** en selecteert u **Firewall** in het vervolgkeuzemenu **Logboek**.

3. Selecteer in het gedeelte **Protocol/poorten** het protocol via welke de toepassing communiceert en poortnummers (als het TCP- of UDP-protocol is geselecteerd). De transportprotocollaag zorgt voor veilige en efficiënte gegevensoverdracht.

4. Geef tot slot de criteria voor het **Doel** op (IP-adres, bereik, subnet, ethernet of internet) voor de regel.

Firewallzones

Een zone is een verzameling netwerkadressen die één logische groep vormen. Aan elk adres in de desbetreffende groep worden regels toegewezen die centraal zijn gedefinieerd voor de hele groep.

U kunt deze zones maken door op **Toevoegen...** te klikken. Geef een **Naam** en een **Beschrijving** (optioneel) voor de zone op, selecteer een profiel waartoe de zone behoort en voeg een IPv4-/IPv6-adres, adresbereik, subnet, Wi-Fi-netwerk of een interface toe.

Firewallprofielen

Met **Profielen** kunt u het gedrag van de firewall van ESET Cyber Security Pro bepalen. Wanneer u een regel voor de firewall maakt of bewerkt, kunt u deze toewijzen aan een bepaald profiel. Wanneer u een profiel selecteert, worden alleen de algemene regels (waarvoor geen profiel is opgegeven) en de regels die zijn toegewezen aan dat profiel toegepast. U kunt het gedrag van de firewall eenvoudig wijzigen door meerdere profielen te maken waaraan verschillende regels zijn toegewezen.

Firewalllogboeken

De firewall van ESET Cyber Security Pro slaat alle belangrijke gebeurtenissen op in een logbestand. Als u de firewalllogboeken wilt openen vanuit het hoofdmenu, klikt u op **Hulpmiddelen** > **Logboeken** en selecteer **Firewall** in het vervolgkeuzemenu **Logboek**.

Logbestanden zijn een waardevol hulpmiddel bij het detecteren van fouten en het aan het licht brengen van inbreuken in het systeem. De logboeken van de ESET-firewall bevatten de volgende gegevens:

- Datum en tijd van de gebeurtenis
- Naam van de gebeurtenis
- Bron
- Doelnetwerkadres
- Netwerkcommunicatieprotocol
- Regel toegepast
- Betrokken toepassing
- Gebruiker

Een grondige analyse van deze gegevens kan helpen bij het detecteren van pogingen de systeembeveiliging in gevaar te brengen. Er zijn veel andere factoren die kunnen wijzen op potentiële risico's en waartegen u zich kunt beveiligen met de firewall, zoals: frequente verbindingen vanaf onbekende locaties, meerdere pogingen om verbindingen tot stand te brengen, communicatie via onbekende toepassingen of gebruik van ongebruikelijke poortnummers.

Web- en e-mailbeveiliging

Klik op **Instellingen** > **Web en e-mail** om toegang te krijgen tot Web- en e-mailbeveiliging in het hoofdvenster. Van hieruit hebt u ook toegang tot de gedetailleerde instellingen voor elke module door te klikken op **Instellen...**.

- **Beveiliging van webtoegang**: bewaakt HTTP-communicatie tussen webbrowsers en externe servers.
- **Beveiliging van e-mailclient**: biedt controle van e-mailcommunicatie die wordt ontvangen via het POP3- en IMAP-protocol.
- **Antiphishing-beveiliging**: blokkeert potentiële phishing-aanvallen afkomstig van websites of uit domeinen.



Scanuitzonderingen
ESET Cyber Security Pro scant niet de versleutelde protocollen HTTPS, POP3S en IMAPS.

Webbeveiliging

Beveiliging van webtoegang controleert communicatie tussen webbrowsers en externe servers op naleving van HTTP-regels (Hypertext Transfer Protocol).

Webfiltering kan worden gerealiseerd door de poortnummers voor HTTP-communicatie en/of URL-adressen te definiëren.

Poorten

Op het tabblad **Poorten** kunt u de poortnummers definiëren die worden gebruikt voor HTTP-communicatie. Standaard zijn de poortnummers 80, 8080 en 3128 vooraf gedefinieerd.

URL-lijsten

In het gedeelte **URL-lijsten** kunt u HTTP-adressen opgeven die u wilt blokkeren, toestaan of uitsluiten van controle. Websites in de lijst met geblokkeerde adressen zijn niet toegankelijk. Websites in de lijst met uitgesloten adressen zijn toegankelijk zonder te worden gescand op schadelijke code.

Als u alleen toegang wilt toestaan tot de URL-adressen die worden vermeld in de lijst **Toegestane URL**, selecteert u de optie **Niet-toegankelijke URL-adressen**.

Als u een lijst wilt activeren, selecteert u **Ingeschakeld** naast de lijstnaam. Als u een melding wilt krijgen wanneer u een adres invoert van de huidige lijst, selecteert u de optie **Op de hoogte gesteld**.

In alle lijsten kunnen de speciale tekens *(sterretje) en ?(vraagteken) worden gebruikt. Het sterretje vervangt een willekeurige tekenreeks en het vraagteken een willekeurig teken. Wees voorzichtig met het opgeven van uitgesloten adressen. De lijst mag alleen vertrouwde en veilige adressen bevatten. Evenzo is het noodzakelijk ervoor te zorgen dat de tekens * en ? op de juiste wijze worden gebruikt in de lijst.

E-mailbeveiliging

E-mailbeveiliging biedt controle over e-mailcommunicatie die wordt ontvangen via de protocollen POP3 en IMAP. Bij het onderzoeken van binnenkomende berichten maakt ESET Cyber Security Pro gebruik van alle geavanceerde scanmethoden van de ThreatSense-scanengine. Het scannen van de communicatie via het POP3- of IMAP-protocol gebeurt onafhankelijk van de gebruikte e-mailclient.

ThreatSense-engine: Instellingen: via de geavanceerde instellingen van de scanner kunt u scandoelen, detectiemethoden enz. configureren. Klik op **Instellingen** om het venster met gedetailleerde scaninstellingen weer te geven.

Bericht toevoegen aan e-mailvoetnoot: nadat een e-mail is gescand, kan er een melding met de scanresultaten aan het bericht worden toegevoegd. Tagberichten zijn handig maar moeten niet worden gebruikt om uiteindelijk te bepalen of een bericht veilig is of niet, aangezien ze kunnen worden overgeslagen in problematische HTML-berichten en door bepaalde bedreigingen kunnen worden vervalst. De volgende opties zijn beschikbaar:

- **Nooit**: er wordt aan geen enkele e-mail een tagbericht toegevoegd
- **Alleen geïnfecteerde e-mail**: alleen e-mail met malware wordt gemarkeerd als gecontroleerd
- **Alle gescande e-mail**: aan alle gescande e-mail worden tagberichten toegevoegd

Opmerking toevoegen aan het onderwerp van ontvangen en gelezen geïnfecteerde e-mail: schakel dit selectievakje in als u een bedreigingswaarschuwing aan het onderwerp van geïnfecteerde e-mail wilt toevoegen. Met deze functie kunt u eenvoudig filteren op geïnfecteerde e-mail. Het schept ook meer vertrouwen bij de ontvanger, en als een infiltratie wordt gedetecteerd beschikt u hiermee over waardevolle informatie over het risiconiveau van een bepaalde e-mail of afzender.

Sjabloon toegevoegd aan het onderwerp van geïnfecteerde e-mail: u kunt deze sjabloon bewerken als u de indeling van het onderwerpvoorvoegsel van een geïnfecteerde e-mail wilt wijzigen.

- %avstatus%: voegt de e-mailinfectiestatus toe (bijvoorbeeld: schoon, geïnfecteerd...)
- %virus%: voegt de naam van de bedreiging toe
- %aspmstatus%: wijzigt het onderwerp op basis van het resultaat van de antispamscan
- %product%: voegt de naam van uw ESET-product toe (in dit geval - ESET Cyber Security Pro)

- %product_url%: voegt de koppeling naar de ESET-website toe (www.eset.com)

In het onderste gedeelte van dit venster kunt u ook de controle van e-mailcommunicatie in/uitschakelen die wordt ontvangen via het POP3- en IMAP-protocol. Zie de volgende onderwerpen voor meer informatie hierover:

- POP3-protocolcontrole
- IMAP-protocolcontrole

POP3-protocolcontrole

Het POP3-protocol is het meest gebruikte protocol voor het ontvangen van e-mailcommunicatie in een e-mailclienttoepassing. ESET Cyber Security Pro biedt beveiliging voor dit protocol, ongeacht welke e-mailclient wordt gebruikt.

De beveiligingsmodule die deze controle biedt wordt automatisch gestart wanneer het systeem wordt opgestart en is vervolgens actief in het geheugen. Zorg ervoor dat de module is ingeschakeld anders werkt protocolfiltering niet goed; POP3-protocolcontrole wordt automatisch uitgevoerd zonder dat u uw e-mailclient daarvoor opnieuw hoeft te configureren. Standaard wordt alle communicatie via poort 110 gescand, maar u kunt indien nodig andere communicatiepoorten toevoegen. Poortnummers moeten worden gescheiden door een komma.

Als de optie **POP3-protocolcontrole inschakelen** is geselecteerd, wordt alle POP3-verkeer gecontroleerd op schadelijke software.

IMAP-protocolcontrole

Het Internet Message Access Protocol (IMAP) is een ander e-mailprotocol voor het ophalen van e-mail. IMAP heeft bepaalde voordelen boven POP3. Meerdere clients kunnen bijvoorbeeld gelijktijdig verbinding maken met hetzelfde postvak en de statusinformatie van berichten bijhouden, zoals of een bericht al dat niet is gelezen, beantwoord of verwijderd. ESET Cyber Security Pro biedt beveiliging voor dit protocol, ongeacht welke e-mailclient u gebruikt.

De beveiligingsmodule die deze controle biedt wordt automatisch gestart wanneer het systeem wordt opgestart en is vervolgens actief in het geheugen. Zorg ervoor dat IMAP-protocolcontrole is ingeschakeld anders werkt de module niet goed; IMAP-protocolcontrole wordt automatisch uitgevoerd zonder dat u uw e-mailclient daarvoor opnieuw hoeft te configureren. Standaard wordt alle communicatie via poort 143 gescand, maar u kunt indien nodig andere communicatiepoorten toevoegen. Poortnummers moeten worden gescheiden door een komma.

Als **IMAP-protocolcontrole inschakelen** is geselecteerd, wordt al het verkeer via IMAP gecontroleerd op schadelijke software.

Ouderlijk toezicht

In het gedeelte **Ouderlijk toezicht** kunt u de instellingen voor Ouderlijk toezicht configureren. Ouders beschikken hiermee over geautomatiseerde hulpmiddelen om hun kinderen te helpen beschermen. Het doel is te voorkomen dat kinderen en jongeren toegang kunnen krijgen tot pagina's met ongeschikte of schadelijke inhoud. Met Ouderlijk toezicht kunt u webpagina's blokkeren die mogelijk schadelijk materiaal bevatten. Daarnaast kunnen ouders de toegang tot maximaal 27 vooraf gedefinieerde categorieën websites verbieden.

Uw gebruikersaccounts worden vermeld in het venster **Ouderlijk toezicht** (**Instellingen** > **Voorkeuren voor**

toepassing opgeven... > **Ouderlijk toezicht**). Selecteer het account dat u wilt gebruiken voor Ouderlijk toezicht. U kunt een beveiligingsniveau opgeven voor het geselecteerde account door op **Instellingen... te klikken.** . Als u een nieuw account wilt maken, klikt u op **Toevoegen...** . Hiermee wordt u omgeleid naar het venster met macOS-systeemaccounts.

Selecteer in het venster **Ouderlijk toezicht instellen** een van de vooraf gedefinieerde profielen in het vervolgkeuzemenu **Profiel instellen**, of kopieer instellingen voor Ouderlijk toezicht van een ander gebruikersaccount. Elk profiel bevat een aangepaste lijst met toegestane categorieën. Als het selectievakje van een categorie is ingeschakeld, is deze toegestaan. Als u de muisaanwijzer boven een categorie houdt, wordt een lijst weergegeven met webpagina's die in die categorie vallen.

Als u de lijst met **Toegestane en geblokkeerde webpagina's** wilt aanpassen, klikt u op **Instellingen...** onder in een venster en voegt u een domeinnaam toe aan de gewenste lijst. U hoeft *http://* niet te typen. Het gebruik van jokertekens (*) is niet nodig. Als u alleen een domeinnaam invoert, zijn alle subdomeinen daarbij inbegrepen. Als u bijvoorbeeld *google.com* toevoegt aan **Lijst met toegestane webpagina's**, zijn alle subdomeinen (*mail.google.com*, *news.google.com*, *maps.google.com* enz.) toegestaan.



Regels
Het blokkeren of toestaan van een specifieke webpagina kan nauwkeuriger zijn dan het blokkeren of toestaan van een hele categorie webpagina's.

Bijwerken

ESET Cyber Security Pro moet regelmatig worden bijgewerkt om het maximale beveiligingsniveau te kunnen blijven bieden. De updatemodule waarborgt dat het programma altijd is bijgewerkt door steeds de meest recente detectiemodules te downloaden.

Klik in het hoofdmenu op **Bijwerken** voor het weergeven van de actuele updatestatus van ESET Cyber Security Pro, inclusief de datum en tijd van de laatste update en of er een update nodig is. U begint het updateproces handmatig door te klikken op **Modules bijwerken**.

Onder normale omstandigheden, dus wanneer updates zonder problemen worden gedownload, wordt het bericht **Bijwerken is niet nodig. De geïnstalleerde modules zijn up-to-date** in het venster Bijwerken weergegeven. Als de modules niet kunnen worden bijgewerkt, wordt aangeraden de update-instellingen te controleren. De meest voorkomende reden voor deze fout is onjuist ingevoerde verificatiegegevens (gebruikersnaam en wachtwoord) of onjuist geconfigureerde verbindingsinstellingen.

Het updatevenster bevat ook het versienummer van de detectie-engine. Het versienummer is gekoppeld aan de webpagina van ESET waar de updategegevens over de detectie-engine staan.

Instellingen voor bijwerken

Als u alle tijdelijk opgeslagen updategegevens wilt verwijderen, klikt u op **Opschonen** naast **Updatecache wissen**. Gebruik deze optie als er problemen optreden tijdens de update.

Geavanceerde opties

Als u meldingen na elke geslaagde update wilt uitschakelen, selecteert u **Geen meldingen over geslaagde updates weergeven**.

Als u ontwikkelmodules wilt downloaden die de testfase bijna hebben voltooid, moet u **Bèta-updates** inschakelen. In veel bèta-updates zijn oplossingen voor productproblemen opgenomen. Met **Vertraagde updates** downloadt u updates enkele uren nadat ze zijn vrijgegeven. Zo zorgt u ervoor dat clients geen updates ontvangen tot is bevestigd dat deze vrij zijn van praktische problemen.

In ESET Cyber Security Pro worden momentopnames van de detectie-engine en programmamodules vastgelegd voor gebruik met de functie **Ongedaan maken van updates**. Laat **Momentopnamen maken van updatebestanden** ingeschakeld, zodat ESET Cyber Security Pro deze momentopnamen automatisch maakt. Als u vermoedt dat een nieuwe update van de detectiemodule en/of programmamodule instabiel of beschadigd is, kunt u terugkeren naar de vorige versie en alle updates voor een bepaalde periode uitschakelen. Of u kunt eerder uitgeschakelde updates inschakelen als u deze voor onbepaalde tijd hebt uitgesteld. Als u updates ongedaan wilt maken en wilt terugkeren naar de oudste versie in de geschiedenis, klikt u op **Terugdraaien**. Wanneer u de functie Ongedaan maken van updates gebruikt om terug te keren naar een eerdere update, gebruikt u het vervolgkeuzemenu **Periode van opschorting instellen op** om de tijdperiode op te geven gedurende welke u updates wilt opschorten. Als u **tot ingetrokken** selecteert, worden normale updates pas weer hervat als u deze handmatig herstelt. Wees voorzichtig met het instellen van de tijdperiode om updates op te schorten.

Maximumleeftijd voor detectie-engine automatisch instellen: hier kunt u de maximale tijd (in dagen) instellen waarna de detectiemodules als verouderd worden aangemerkt. De standaardwaarde is 7 dagen.

Updatetaken maken

Updates kunnen handmatig worden geactiveerd door in het hoofdmenu te klikken op **Bijwerken** en vervolgens te klikken op **Modules bijwerken**.

Updates kunnen ook worden uitgevoerd als geplande taken. Als u een geplande taak wilt configureren, klikt u op **Hulpmiddelen** > **Planner**. Standaard zijn in ESET Cyber Security Pro de volgende taken geactiveerd:

- **Regelmatig automatisch bijwerken**
- **Automatisch bijwerken na aanmelding van gebruiker**

Elk van de updatetaken kan worden gewijzigd om te voldoen aan uw behoeften. Behalve de standaardupdatetaken kunt u ook nieuwe updatetaken maken met een door de gebruiker gedefinieerde configuratie. Zie het gedeelte Planner voor meer informatie over het maken en configureren van updatetaken.

ESET Cyber Security Pro bijwerken naar een nieuwe versie

Voor maximale beveiliging is het belangrijk dat u de nieuwste build van ESET Cyber Security Pro gebruikt. U controleert of er een nieuwe versie beschikbaar is door in het hoofdmenu op **Thuis** te klikken. Als er een nieuwe build beschikbaar is, wordt een bericht weergegeven. Klik op **Meer informatie...** om een nieuw venster te openen

met het versienummer van de nieuwe build en het wijzigingslogboek.

Klik op **Ja** om de nieuwste build te downloaden of klik op **Niet nu** om het venster te sluiten en de upgrade later te downloaden.

Als u op **Ja** hebt geklikt, wordt het bestand gedownload naar uw downloadmap (of naar de standaardmap die door de browser is ingesteld). Nadat het downloaden van het bestand is voltooid, kunt u het bestand starten en de installatie-instructies uitvoeren. Uw gebruikersnaam en wachtwoord worden automatisch overgezet naar de nieuwe installatie. We raden aan dat u regelmatig controleert of er upgrades beschikbaar zijn, vooral als u ESET Cyber Security Pro via een cd/dvd installeert.

Systeemupdates

De macOS-systeemupdatefunctie is een belangrijk onderdeel dat is gemaakt om gebruikers te kunnen beschermen tegen schadelijke software. Voor een maximale beveiliging raden wij aan om deze updates zo snel mogelijk te installeren nadat deze beschikbaar zijn gekomen. ESET Cyber Security Pro brengt u op de hoogte van eventueel ontbrekende updates volgens het niveau dat u zelf opgeeft. U kunt de mate van updatemeldingen die u ontvangt aanpassen in **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Waarschuwingen en meldingen > Instellen...** en wijzig de opties van **Weergavevoorwaarden** naast **Updates van het besturingssysteem**.

- **Alle updates weergeven** - er wordt een melding weergegeven als er een systeemupdate ontbreekt
- **Alleen aanbevolen weergeven** - u ontvangt alleen meldingen over aanbevolen updates

Als u geen meldingen over ontbrekende updates wilt ontvangen, schakel het selectievakje naast **Updates van het besturingssysteem** dan uit.

Het meldingenvenster geeft een overzicht van de updates die beschikbaar zijn voor het macOS-besturingssysteem en de toepassingen die met het hulpprogramma van macOS zelf (Software-updates) zijn en kunnen worden bijgewerkt. U kunt de update rechtstreeks vanuit het meldingenvenster installeren of vanuit de sectie **Thuis** van ESET Cyber Security Pro door te klikken op **De ontbrekende update installeren**.

In het meldingenvenster staan de toepassingsnaam, versie, grootte, eigenschappen (vlaggen) en aanvullende informatie over beschikbare updates. In de kolom Vlaggen staat de volgende informatie:

- **[aanbevolen]** - de fabrikant van het besturingssysteem raadt aan dat u deze update installeert om de beveiliging en stabiliteit van het systeem te vergroten
- **[opnieuw opstarten]** - het opnieuw opstarten van de computer is vereist na de installatie
- **[afsluiten]** - de computer moet worden afgesloten en daarna opnieuw opgestart na de installatie

In het meldingsvenster staat welke updates door het opdrachtregelhulpprogramma genaamd 'softwareupdate' worden opgehaald. Updates die door dit hulpprogramma worden opgehaald, kunnen anders zijn dan de updates die worden weergegeven door de toepassing 'Software-updates'. Als u alle beschikbare updates wilt installeren die in het venster 'Ontbrekende systeemupdates' worden weergegeven en ook de updates die niet door de toepassing 'Software-updates' worden weergegeven, moet u het opdrachtregelhulpprogramma 'softwareupdate' gebruiken. Lees voor meer informatie over dit hulpprogramma de handleiding voor software-updates door man softwareupdate te typen in een Terminal-venster. Dit wordt alleen aangeraden voor ervaren gebruikers.

Hulpmiddelen

Het menu **Hulpmiddelen** omvat modules die het programmabeheer helpen vereenvoudigen en aanvullende opties voor geavanceerde gebruikers.

Logbestanden

De logbestanden bevatten informatie over belangrijke programmagebeurtenissen die zich hebben voorgedaan en bieden een overzicht van gedetecteerde bedreigingen. Logboekregistratie vormt een essentieel hulpmiddel bij systeemanalyse, bedreigingsdetectie en probleemoplossing. Logboekregistratie wordt zonder gebruikersinteractie op de achtergrond uitgevoerd. Informatie wordt vastgelegd op basis van huidige detailinstellingen voor logboekregistratie. U kunt tekstberichten en logboeken rechtstreeks vanuit de ESET Cyber Security Pro-omgeving weergeven. U kunt de logboeken ook archiveren.

Logbestanden zijn toegankelijk vanuit het hoofdmenu van ESET Cyber Security Pro door op **Hulpmiddelen** > **Logboeken** te klikken. Selecteer het gewenste logboektype in de vervolgkeuzelijst **Logboek** boven in het venster. De volgende logboeken zijn beschikbaar:

1. **Gedetecteerde bedreigingen** - met deze optie geeft u alle informatie weer over gebeurtenissen die verband houden met de detectie van infiltraties.
2. **Gebeurtenissen** - met deze optie kunnen systeembeheerders en gebruikers problemen oplossen. Alle belangrijke acties die worden uitgevoerd door ESET Cyber Security Pro, worden opgenomen in de gebeurtenislogboeken.
3. **Computerscan** - in dit logboek worden de resultaten van alle voltooide scans weergegeven. Dubbelklik op een vermelding om de details voor de desbetreffende on-demand computerscan weer te geven.
4. **Ouderlijk** - een lijst met alle webpagina's die zijn geblokkeerd door Ouderlijk toezicht.
5. **Firewall** - dit log bevat de resultaten van alle gebeurtenissen met betrekking tot het netwerk.
6. **Gefilterde websites**: deze lijst is nuttig als u een lijst met websites wilt bekijken die door Beveiliging van webtoegang zijn geblokkeerd. In deze logboeken ziet u de tijd, URL, status, het IP-adres, de gebruiker en toepassing die een verbinding met deze website heeft geopend.

U kunt de informatie in elke sectie rechtstreeks naar het klembord kopiëren door de gewenste vermelding te selecteren en op de knop **Kopiëren** te klikken.

Logbestanden onderhouden

De configuratie van logbestanden voor ESET Cyber Security Pro is toegankelijk vanuit het hoofdvenster van het programma. Klik op **Instellen** > **Voorkeuren voor toepassing opgeven** (of druk op *cmd+,*) > **Logboekbestanden**. U kunt de volgende opties opgeven voor logbestanden:

- **Oude logboekrecords automatisch verwijderen**: logboekvermeldingen die ouder zijn dan het opgegeven aantal dagen, worden automatisch verwijderd (standaard 90 dagen).
- **Logbestanden automatisch optimaliseren**: logbestanden worden automatisch gedefragmenteerd als het opgegeven percentage ongebruikte records is overschreden (standaard 25%).

Alle relevante informatie die wordt weergegeven in de grafische gebruikersinterface en berichten over bedreigingen en gebeurtenissen kunnen worden opgeslagen in een voor mensen leesbare tekstindeling, zoals tekst zonder opmaak of CSV-bestanden (Comma-separated values). Als u deze bestanden beschikbaar wilt maken voor verwerking met programma's van derden, schakelt u het selectievakje naast **Registratie naar tekstbestanden inschakelen in**.

Klik op **Instellingen** naast **Geavanceerde opties** om de doelmap te definiëren waarin de logbestanden moeten worden opgeslagen.

Afhankelijk van de opties die u hebt geselecteerd onder **Tekstlogbestanden: Bewerken**, kunt u logbestanden opslaan waarin de volgende informatie wordt geschreven:

- Gebeurtenissen zoals *Gebruikersnaam en wachtwoord ongeldig*, *Modules kunnen niet worden bijgewerkt* enz., worden naar het bestand eventslog.txt geschreven.
- Bedreigingen die zijn gedetecteerd door de Opstartscanner, Real-timebeveiliging of Computerscan worden opgeslagen in het bestand met de naam threatslog.txt.
- De resultaten van alle voltooide scans worden opgeslagen in de indeling scanlog.NUMMER.txt
- Alle gebeurtenissen die gerelateerd zijn aan communicatie die door de firewall loopt, worden naar firewalllog.txt geschreven,

Als u filters wilt configureren voor **Standaardlogboekrecords voor computerscans**, klikt u op **Bewerken** en selecteert u de benodigde typen logbestanden of heft u de selectie ervan op. Meer informatie over deze logtypen vindt u Logbestanden filteren.

Logbestanden filteren

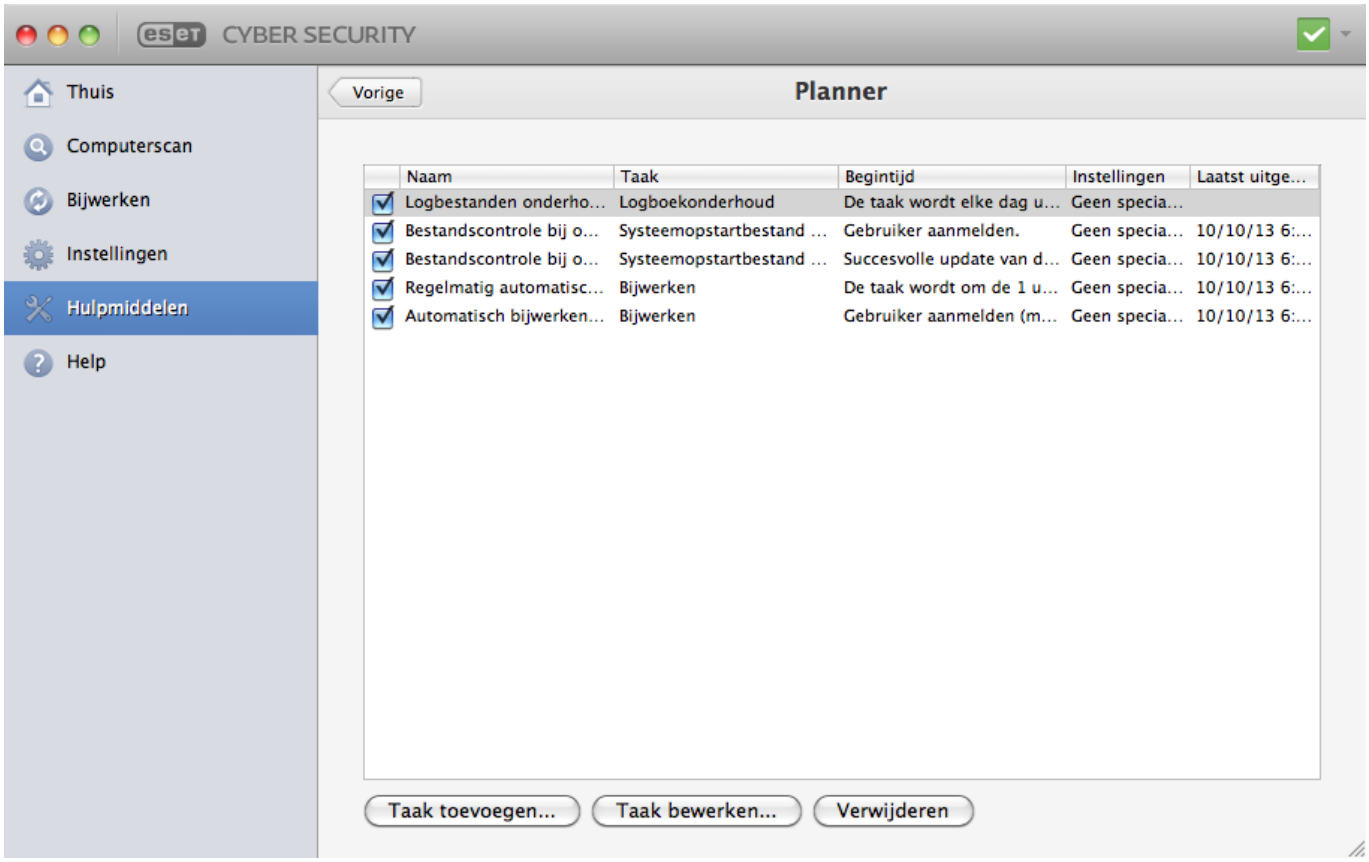
In logbestanden (ook wel logboeken genoemd) wordt informatie over belangrijke systeemgebeurtenissen opgeslagen. U kunt logbestanden filteren om alleen records voor een bepaald type gebeurtenis weer te geven.

Hieronder worden de meest gebruikte typen logbestanden beschreven:

- **Kritieke waarschuwingen** - kritieke systeemfouten (bijvoorbeeld het niet starten van de antivirusbeveiliging)
- **Fouten** - foutmeldingen zoals '*Fout bij downloaden van bestand*' en kritieke fouten.
- **Waarschuwingen** - waarschuwingsberichten
- **Informatieve records**- informatieve berichten, met betrekking tot onder andere geslaagde updates, waarschuwingen enz.
- **Diagnostische records** - informatie die nodig is voor het instellen van het programma, plus alle hierboven beschreven records.

Planner

De **Planner** is te vinden in het hoofdmenu van ESET Cyber Security Pro onder **Hulpmiddelen**. De **Planner** bevat een lijst met alle geplande taken en hun configuratie-eigenschappen, zoals de vooraf gedefinieerde datum en tijd en het gebruikte scanprofiel.



De Planner beheert en start geplande taken met vooraf gedefinieerde configuraties en eigenschappen. De configuratie en eigenschappen bevatten informatie zoals de datum en tijd alsmede opgegeven profielen die moeten worden gebruikt tijdens de uitvoering van de taak.

Standaard worden de volgende geplande taken in de Planner weergegeven:

- Logbestanden onderhouden (nadat de optie **Systeemtaken weergeven** is ingeschakeld in de instellingen voor de Planner)
- Opstartbestand controleren na aanmelding gebruiker
- pstartbestand controleren na succesvolle update van de detectiemodules
- Regelmatig automatisch bijwerken
- Automatisch bijwerken na aanmelding van gebruiker

U kunt de configuratie van een bestaande geplande taak (zowel standaard als door de gebruiker gedefinieerd) bewerken door Ctrl ingedrukt te houden, op de taak te klikken die u wilt wijzigen en op **Bewerken** te klikken, of door de taak te selecteren en op **Taak bewerken** te klikken.

Nieuwe taken maken

U kunt een nieuwe taak maken in de Planner door op **Taak toevoegen...** te klikken of door op CTRL te drukken en te klikken in het lege veld en **Toevoegen...** te selecteren in het contextmenu. Er zijn vijf typen geplande taken beschikbaar:

- **Toepassing uitvoeren**
- **Bijwerken**

- **Logbestanden onderhouden**
- **On-demand computerscan**
- **Controle van systeemopstartbestanden**

Toepassing uitvoeren

Door **Toepassing uitvoeren** te selecteren, kunt u programma's uitvoeren als systeemgebruiker genaamd "nobody". Machtigingen voor het uitvoeren van toepassingen via de Planner worden door macOS gedefinieerd. Als u een andere gebruiker dan de standaard ingestelde gebruiker wilt instellen, typt u de gebruikersnaam, gevolgd door een dubbele punt (:) voorafgaand aan de opdracht. Ook kunt u de **hoofdgebruiker** in deze functie gebruiken.

Voorbeeld: Taak uitvoeren als gebruiker

In dit voorbeeld plannen wij dat de app Rekenmachine op een bepaald tijdstip wordt gestart uit naam van een gebruiker met de naam **UserOne**:
1.Ga naar **Planner** en selecteer **Taak toevoegen**.
2.Typ de taaknaam. Selecteer **Toepassing uitvoeren** als **Geplande taak**. Selecteer in het venster **Taak uitvoeren** de optie **Eenmaal** om deze taak één keer uit te voeren. Klik op **Volgende**.
3.Klik op Bladeren en selecteer de app Rekenmachine.
4.Typ **UserOne:** voorafgaand aan het toepassingspad (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') en klik op **Volgende**.
5.Selecteer een tijd om de taak uit te voeren en klik op **Volgende**.
6.Selecteer een andere optie als de taak niet kan worden uitgevoerd en klik op **Volgende**.
7.Klik op **Voltooien**.
8.ESET Planner start de app Rekenmachine op de door u geselecteerde tijd.

Voorbeeld: Bijwerktaak

In dit voorbeeld maken wij een bijwerktaak die op een bepaalde tijd wordt uitgevoerd.
1.Ga naar de vervolgkeuzelijst **Geplande taak** en selecteer **Bijwerken**.
2.Voer de naam van de taak in het veld **Taaknaam** in.
3.Selecteer de frequentie van de taak in de vervolgkeuzelijst **Taak uitvoeren**. Op basis van de geselecteerde frequentie wordt u gevraagd om waarden voor verschillende updateparameters in te voeren. Als u **Door gebruiker gedefinieerd** selecteert, wordt u gevraagd een datum/tijd op te geven in cron-notatie (zie het gedeelte Door gebruiker gedefinieerde taak maken voor meer details).
4.In de volgende stap definieert u welke actie moet worden ondernomen als de taak niet kan worden uitgevoerd of voltooid op het geplande tijdstip.
5.In de laatste stap wordt een overzichtsvenster weergegeven met informatie over de huidige geplande taak. Klik op **Voltooien**. De nieuwe geplande taak wordt toegevoegd aan de lijst met actuele geplande taken.

ESET Cyber Security Pro bevat voorgedefinieerde geplande taken waarmee de juiste werking wordt gewaarborgd. Deze mogen niet worden gewijzigd en zijn standaard verborgen. Als u deze taken zichtbaar wilt maken, klik dan in het hoofdmenu op **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Planner** en selecteer **Systeemtaken weergeven**.

Scannen als mapeigenaar

U kunt mappen scannen als eigenaar van de map:

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

Ook kunt u de map `/tmp` als de momenteel aangemelde gebruiker scannen:

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

Door gebruiker gedefinieerde taken maken

De datum en tijd van een **door de gebruiker gedefinieerde** taak moeten worden opgegeven in cron-notatie met jaaruitbreiding (een tekenreeks bestaande uit zes velden, elk van elkaar gescheiden door een spatie):

```
minuut(0-59) uur(0-23) dag van maand(1-31) maand(1-12) jaar(1970-2099) dag van
week(0-7)(zondag = 0 of 7)
```

Voorbeeld:

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

Speciale tekens die worden ondersteund in cron-expressies:

- sterretje (`*`): expressie geldt voor alle waarden van het veld. Een sterretje in het derde veld (dag van maand) betekent bijvoorbeeld elke dag
- hyphen (`-`) – definieert bereiken, bijvoorbeeld `3-9`
- komma (`,`) – scheidt items in een lijst, bijvoorbeeld `1,3,7,8`
- schuine streep (`/`) – definieert verhogingen van bereiken; bijv. `3-28/5` in het derde veld (dag van maand) betekent de derde dag van elke maand en vervolgens elke vijf dagen.

Namen van dagen (Monday-Sunday) en namen van maanden (January-December) worden niet ondersteund.

> **Opdrachten uitvoeren**
> als u zowel de dag van de maand als de dag van de week definieert, wordt de opdracht alleen uitgevoerd als beide velden overeenkomen.

Quarantaine

Het hoofddoel van quarantaine is het veilig opslaan van geïnfecteerde bestanden. Bestanden moeten in quarantaine worden geplaatst als ze niet kunnen worden opgeschoond, als het niet veilig of raadzaam is om ze te verwijderen of als ze onterecht door ESET Cyber Security Pro zijn gedetecteerd.

U kunt elk bestand in quarantaine plaatsen. Dit is raadzaam als een bestand zich verdacht gedraagt maar niet wordt gedetecteerd door de antivirusscanner. In quarantaine geplaatste bestanden kunnen voor analyse naar het bedreigingslaboratorium van ESET worden verzonden.

Bestanden die zijn opgeslagen in de quarantainemap kunnen worden bekeken in een tabel waarin de datum en het tijdstip van de quarantaine, het pad naar de oorspronkelijke locatie van het geïnfecteerde bestand, de grootte van het bestand in bytes, de reden (bijvoorbeeld toegevoegd door gebruiker…) en het aantal bedreigingen (bijvoorbeeld of het een archief is dat meerdere infiltraties bevat) worden weergegeven. De quarantainemap met de bestanden in quarantaine () blijft aanwezig in het systeem, zelfs als u ESET Cyber Security Pro verwijdert. Bestanden in quarantaine worden veilig gecodeerd opgeslagen en kunnen weer worden teruggezet na installatie van ESET Cyber Security Pro.

Bestanden in quarantaine plaatsen

ESET Cyber Security Pro plaatst verwijderde bestanden automatisch in quarantaine (als u deze optie niet hebt gedeselecteerd in het waarschuwingsvenster). U kunt elk verdacht bestand in quarantaine plaatsen door op **Quarantaine...** te klikken . Het contextmenu kan eveneens worden gebruikt voor dit doel. Druk op Ctrl en klik in het lege veld, selecteer **Quarantaine**, selecteer het bestand dat u in quarantaine wilt plaatsen en klik op **Openen**.

Herstellen vanuit quarantaine

In quarantaine geplaatste bestanden kunnen ook worden hersteld naar hun oorspronkelijke locatie. Dit doet u door een in quarantaine geplaatst bestand te selecteren en op **Herstellen** te klikken. Herstellen is ook beschikbaar in het contextmenu. Klik met CTRL ingedrukt op een bestand in het venster Quarantaine en klik vervolgens op **Herstellen**. Het contextmenu biedt tevens de optie **Herstellen naar...**, waarmee u bestanden kunt herstellen naar een andere locatie dan waarvan ze zijn verwijderd.

Bestand verzenden vanuit quarantaine

Als u een verdacht bestand in quarantaine hebt geplaatst dat niet is gedetecteerd door het programma, of als een bestand ten onrechte als geïnfecteerd is beoordeeld (bijvoorbeeld door heuristische analyse van de code) en vervolgens in quarantaine geplaatst, stuurt u het bestand naar het bedreigingslaboratorium van ESET. U kunt een bestand vanuit quarantaine verzenden door er met Ctrl ingedrukt op te klikken en **Bestand verzenden voor analyse** te selecteren in het contextmenu.

Actieve processen

In de lijst **Actieve processen** worden de processen weergegeven die op uw computer worden uitgevoerd. ESET Cyber Security Pro biedt gedetailleerde informatie over actieve processen om gebruikers te beschermen met ESET Live Grid-technologie.

- **Proces** - de naam van het proces dat momenteel op uw computer wordt uitgevoerd. Als u alle actieve processen wilt zien, kunt u ook Activity Monitor gebruiken (te vinden in */Programma's/Hulpprogramma's*).
- **Risiconiveau** - in de meeste gevallen wijzen ESET Cyber Security Pro en ESET Live Grid-technologie risiconiveaus toe aan objecten (bestanden, processen enz.) met een reeks heuristische regels die de kenmerken van elk object onderzoeken en vervolgens afwegen wat hun potentieel is voor schadelijke activiteiten. Op basis van deze heuristiek wordt aan objecten een risiconiveau toegewezen. Bekende toepassingen die groen zijn gemarkeerd zijn zeker schoon (staan op de witte lijst) en worden uitgesloten van scannen. Hierdoor wordt de snelheid van zowel de On-demand scan als de Real-time scan verhoogd. Als een toepassing is gemarkeerd als onbekend (geel), hoeft deze geen schadelijke software te zijn. Gewoonlijk is het slechts een nieuwere

toepassing. Als u twijfelt hebt over een bestand, kunt u het bestand voor analyse naar het bedreigingslaboratorium van ESET te verzenden. Als het bestand een schadelijke toepassing blijkt te zijn, worden de kenmerken ervan toegevoegd aan een van de volgende updates.

- **Aantal gebruikers** - het aantal gebruikers dat een bepaalde toepassing gebruikt. Deze informatie wordt verzameld door de ESET Live Grid-technologie.
- **Tijdstip van detectie** - de periode sinds de toepassing werd gedetecteerd door de ESET LiveGrid®-technologie.
- **Toepassingsbundel-id** - de naam van de leverancier of het toepassingsproces.

Als u op een bepaald proces klikt, wordt de volgende informatie onder in het venster weergegeven:

- **Bestand**: de locatie van een toepassing op de computer
- **Bestandsgrootte**: de fysieke grootte van het bestand op de schijf
- **Beschrijving van bestand**: bestandskenmerken gebaseerd op de beschrijving van het besturingssysteem
- **Toepassingsbundel-id**: de naam van de leverancier of het toepassingsproces
- **Versie van bestand**: informatie over de uitgever van het bestand
- **Productnaam**: de naam van de toepassing en/of de bedrijfsnaam

Netwerkverbindingen

Netwerkverbindingen is een lijst met actieve netwerkverbindingen op uw computer. ESET Cyber Security Pro biedt uitvoerige informatie over elke verbinding en de mogelijkheid om een regel te maken voor blokkering van deze verbindingen.

Een blokkeringsregel maken voor deze verbinding

Met ESET Cyber Security Pro kunt u een blokkeringsregel maken voor elke verbinding in de beheerfunctie **Netwerkverbindingen**. U kunt een blokkeringsregel maken door met de rechtermuisknop te klikken op de verbinding en **Blokkeringsregel maken voor deze verbinding** te selecteren.

1. Selecteer het **Profiel** van de verbinding waarvoor u de regel wilt maken en typ de naam van de regel. Selecteer de toepassing waarvoor u de regel wilt laten gelden of schakel het selectievakje in om de regel voor alle toepassingen te laten gelden.
2. Selecteer een actie voor elke verbinding: weiger de verbinding (blokkeren) of sta de verbinding toe. Selecteer de communicatierichting waarvoor de regel moet gelden. U kunt een logboekbestand maken voor de regel door op **Logboekregel** te klikken.
3. Selecteer het verbindingsprotocol en de poorttypen. Selecteer de servicepoort of geef een reeks poorten op in de volgende indeling: van-tot.
4. Selecteer het doel en geef de informatie in de vereiste velden op, afhankelijk van uw doel.

Live Grid

Het Live Grid vroegtijdige waarschuwingssysteem houdt ESET onmiddellijk en continu op de hoogte van nieuwe infiltraties. Het bidirectionele Live Grid vroegtijdig waarschuwingssysteem heeft één enkel doel, namelijk de

beveiliging verbeteren die wij u kunnen bieden. Dit kunnen we het beste doen door ervoor te zorgen dat we nieuwe bedreigingen zo spoedig mogelijk in de gaten krijgen door deze aan zoveel mogelijk van onze klanten te 'koppelen' en hen te gebruiken als onze bedreigingsscouts. Er zijn twee opties:

1. U kunt ervoor kiezen om het Live Grid vroegtijdig waarschuwingssysteem niet in te schakelen. De software blijft op dezelfde wijze functioneren en u ontvangt nog steeds de beste beveiliging beveiliging die wij u kunnen bieden.

2. U kunt het Live Grid vroegtijdig waarschuwingssysteem zodanig configureren dat anonieme informatie wordt verzonden over nieuwe bedreigingen en waar de nieuwe bedreigingscode voorkomt. Deze informatie kan voor gedetailleerde analyse naar ESET worden verzonden. Door deze bedreigingen te bestuderen kan ESET de detectie-engine bijwerken en de detectiemogelijkheden van het programma verbeteren.

Het Live Grid vroegtijdig waarschuwingssysteem verzamelt informatie over uw computer met betrekking tot nieuw gedetecteerde bedreigingen. Deze informatie kan een voorbeeld of kopie bevatten van het bestand waarin de bedreiging voorkwam, het pad naar dat bestand, de bestandsnaam, de datum en tijd, het proces waarbij de bedreiging plaatsvond op uw computer en informatie over het besturingssysteem van uw computer.

Hoewel de kans bestaat dat het bedreigingslaboratorium van ESET hiermee nu en dan informatie over u of uw computer in bezit krijgt (gebruikersnamen in een directorypad enz.), wordt deze informatie niet gebruikt voor andere doelen dan ons te helpen onmiddellijk te reageren op nieuwe bedreigingen.

Als u Live Grid in het hoofdvenster wilt instellen, klik dan op **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Live Grid**. Selecteer **Vroegtijdig waarschuwingssysteem van Live Grid inschakelen** om Live Grid te activeren en klik op **Instellen...** naast **Geavanceerde opties**.

Live Grid installeren

ESET Cyber Security Pro is standaard geconfigureerd om verdachte bestanden voor gedetailleerde analyse naar het bedreigingslaboratorium van ESET te verzenden. Als u deze bestanden niet automatisch wilt laten verzenden, schakelt u **Bestanden indienen** uit.

Als u een verdacht bestand aantreft, kunt u dit naar ons bedreigingslaboratorium versturen voor analyse. Klik hiervoor in het hoofdvenster van het programma op **Hulpmiddelen** > **Voorbeeld verzenden voor analyse**. Als het een schadelijke toepassing is, wordt de detectie ervan toegevoegd aan een komende update.

Anonieme statistieken verzenden: het vroegtijdig waarschuwingssysteem van ESET Live Grid verzamelt anonieme informatie over uw computer met betrekking tot nieuw gedetecteerde bedreigingen. Deze informatie omvat de naam van de infiltratie, de datum en het tijdstip waarop deze is gedetecteerd, de versie van het ESET-beveiligingsproduct, de versie van uw besturingssysteem en de locatie-instelling. Deze statistische gegevens worden doorgaans een- of tweemaal per dag naar de servers van ESET verzonden.

Uitsluitingsfilter: met het uitsluitingsfilter kunt u bepaalde bestandstypen uitsluiten van verzending. Het kan bijvoorbeeld handig zijn bestanden uit te sluiten die mogelijk vertrouwelijke informatie bevatten, zoals documenten of spreadsheets. Veelgebruikte bestandstypen (DOC, RTF enz.) worden standaard uitgesloten. U kunt bestandstypen toevoegen aan de lijst met uitgesloten bestanden.

E-mailadres van contactpersoon (optioneel): uw e-mailadres kan worden gebruikt als meer informatie nodig is voor analyse. U zult geen antwoord van ESET ontvangen, tenzij nadere informatie nodig is voor de analyse.

Verzenden van voorbeeld voor analyse

Als u een verdacht bestand op uw computer ontdekt, kunt u dit aan het onderzoekslaboratorium van ESET sturen om te laten analyseren.

Alvorens voorbeelden naar ESET te verzenden

Verzend alleen een voorbeeld als die voldoet aan minimaal een van de volgende criteria:

- Het voorbeeld wordt helemaal niet door uw ESET-product gedetecteerd
- Het voorbeeld is onjuist als een bedreiging gedetecteerd
- Wij accepteren uw persoonlijke bestanden niet (die u door ESET op malware wilt scannen) als voorbeeld (het onderzoekslaboratorium van ESET voert geen scans op verzoek van gebruikers uit)
- Gebruik een beschrijvende onderwerpregel en geef zo veel mogelijk informatie over het bestand op als mogelijk is (bijvoorbeeld een schermafbeelding of het adres van de website waar u het bestand hebt gedownload)

Met het formulier voor het verzenden van voorbeelden in uw product kunt u een voorbeeld indienen. U vindt dit formulier bij **Hulpmiddelen** > **Bestand verzenden voor analyse**.

Vul in het volgende in het formulier **Bestand verzenden voor analyse** in:

Bestand: het pad naar het bestand dat u wilt verzenden.

Opmerking: beschrijf de reden waarom u het bestand verzendt.

E-mailadres van contactpersoon: het e-mailadres van de contactpersoon wordt samen met de verdachte bestanden naar ESET verzonden en kan worden gebruikt om contact met u op te nemen als meer informatie nodig is voor de analyse. Het invoeren van een e-mailadres voor de contactpersoon is optioneel.

Mogelijk krijgt u geen reactie van ESET

U krijgt geen reactie van ESET tenzij er meer informatie van u nodig is. Elke dag ontvangen onze servers tienduizenden bestanden, waardoor het onmogelijk is om iedereen te beantwoorden. Als het bestand een schadelijke toepassing of website blijkt te zijn, wordt de detectie ervan in een van de volgende ESET-updates opgenomen.

Gebruikersinterface

Via de configuratie-opties voor de gebruikersinterface kunt u de werkomgeving aan uw eigen behoeften aanpassen. Deze opties zijn toegankelijk vanuit het hoofdmenu door te klikken op **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Interface**.

- Als u het welkomscherm van ESET Cyber Security Pro wilt weergeven bij het opstarten van het systeem, selecteer dan **Welkomscherm weergeven bij opstarten**.
- Met **Toepassing in Dock weergeven** kunt u het ESET Cyber Security Pro-pictogram weergeven in het OS X Dock en heen en weer schakelen tussen ESET Cyber Security Pro en andere toepassingen die worden uitgevoerd door op *cmd+tab* te drukken. Wijzigingen worden van kracht nadat u ESET Cyber Security Pro opnieuw hebt gestart (doorgaans geactiveerd door het opnieuw opstarten van de computer).
- Via de optie **Standaardmenu gebruiken** kunt u bepaalde sneltoetsen gebruiken (zie Sneltoetsen) en de

standaardmenuopties zien (Gebruikersinterface, Instellingen en Hulpmiddelen) op de menubalk van macOS (boven in het scherm).

• U kunt knopinfo inschakelen voor bepaalde opties van ESET Cyber Security Pro door **Knopinfo weergeven** te selecteren.

• Met **Verborgen bestanden weergeven** kunt u verborgen bestanden weergeven en selecteren in de instellingen voor **Scandoelen** van een **Computerscan**.

• Standaard wordt het ESET Cyber Security Pro-pictogram weergegeven op de menubalk Extra die rechts van de macOS-menubalk (boven in het scherm) wordt weergegeven. Als u dit wilt uitschakelen, deselecteert u **Pictogram weergeven in Extra op menubalk**. Deze wijziging wordt van kracht nadat u ESET Cyber Security Pro opnieuw hebt gestart (doorgaans geactiveerd door het opnieuw opstarten van de computer).

Waarschuwingen en meldingen

In het gedeelte **Waarschuwingen en meldingen** kunt u configureren hoe waarschuwingen en systeemmeldingen bij bedreigingen worden verwerkt door ESET Cyber Security Pro.

Wanneer u **Waarschuwingen weergeven** uitschakelt, worden alle waarschuwingsvensters geannuleerd. Dit wordt alleen in bepaalde situaties aangeraden. Voor de meeste gebruikers adviseren wij de standaardoptie (ingeschakeld) voor deze optie te laten staan. Geavanceerde opties worden beschreven in dit hoofdstuk.

Wanneer u **Meldingen weergeven op bureaublad** selecteert, worden er waarschuwingsvensters op het bureaublad weergegeven waarvoor geen gebruikersinteractie nodig is (standaard rechtsboven in het scherm). U kunt opgeven hoe lang een melding wordt weergegeven door de waarde van **Meldingen automatisch sluiten** na X **seconden** te wijzigen (standaard 5 seconden).

Sinds ESET Cyber Security Pro versie 6.2 kunt u ook verhinderen dat bepaalde **Beveiligingsstatussen** in het hoofdvenster van het programma worden weergegeven (het venster **Beveiligingsstatus**). Zie Beveiligingsstatussen voor meer informatie hierover.

Waarschuwingen weergeven

In ESET Cyber Security Pro worden waarschuwingsdialoogvensters weergegeven om u te informeren over nieuwe programmaversies, nieuwe updates voor het besturingssysteem, het uitschakelen van bepaalde programmaonderdelen, het verwijderen van logboeken enz. U kunt elke melding afzonderlijk onderdrukken door **Dit dialoogvenster niet meer weergeven** te selecteren.

Via **Lijst met dialoogvensters** (**Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Waarschuwingen en meldingen** > **Instellen...**) kunt u de lijst weergeven met alle dialoogvensters die worden geactiveerd door ESET Cyber Security Pro. Als u elke melding wilt inschakelen of onderdrukken, schakelt u het selectievakje in links van de **Naam van dialoogvenster**. Daarnaast kunt u **Weergavevoorwaarden** definiëren op basis waarvan meldingen over nieuwe programmaversies en updates van het besturingssysteem worden weergegeven.

Beveiligingsstatussen

De huidige beveiligingsstatus van ESET Cyber Security Pro kan worden gewijzigd door statussen te activeren of deactiveren in **Instellingen** > **Voorkeuren voor toepassing opgeven...** > **Waarschuwingen en meldingen** >

Weergeven in het scherm Beveiligingsstatus: Instellingen. De status van verschillende programmafuncties worden weergegeven of verborgen in het hoofdvenster van ESET Cyber Security Pro (het venster **Beveiligingsstatus**).

U kunt de beveiligingsstatus van de volgende programmafuncties verbergen:

- Firewall
- Antiphishing
- Beveiliging van webtoegang
- Beveiliging van e-mailclient
- Updates voor besturingssysteem
- Licentie verloopt
- Computer moet opnieuw worden opgestart

Machtigingen

De instellingen van ESET Cyber Security Pro kunnen van groot belang zijn voor het beveiligingsbeleid van uw organisatie. Onbevoegde wijzigingen kunnen de stabiliteit en beveiliging van uw systeem in gevaar brengen. Om deze reden kunt u bepalen welke gebruikers de configuratie van het programma mogen wijzigen.

Als u gemachtigde gebruikers wilt opgeven, klikt u op **Instellingen** > **Voorkeuren voor toepassing opgeven** (of druk op *cmd+,*) > **Machtigingen**. Selecteer de gebruikers of groepen in de lijst links en klik op **Toevoegen**. Als u alle systeemgebruikers/systeemgroepen wilt weergeven, selecteert u **Alle gebruikers weergeven/Alle groepen weergeven**. Als u een gebruiker wilt verwijderen, selecteert u de naam van de gebruiker in de lijst **Geselecteerde gebruikers** aan de rechterkant en klikt u op **Verwijderen**.



Over upgrade uitvoeren
Als u de lijst Geselecteerde gebruikers leeglaat, worden alle gebruikers als bevoegd beschouwd.

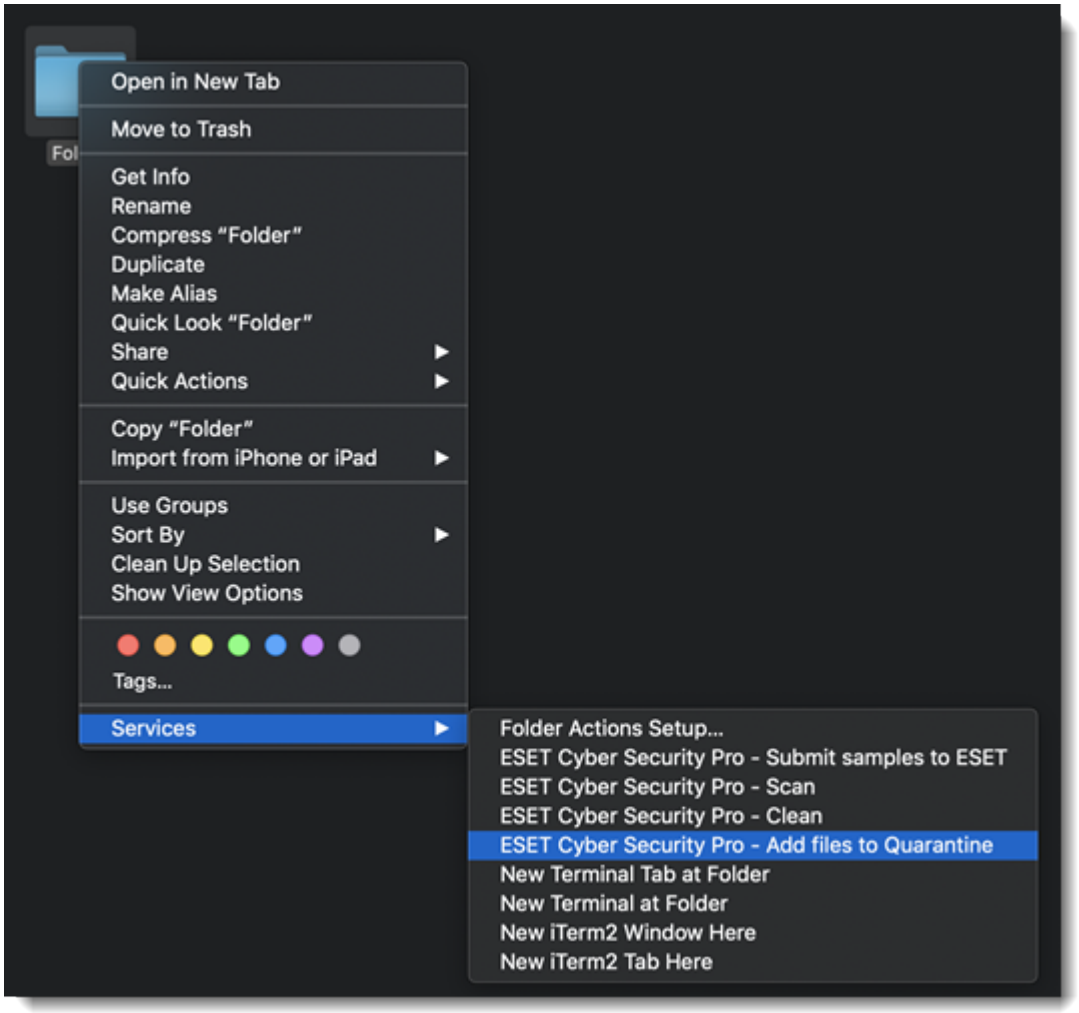
Contextmenu

U kunt de integratie in het contextmenu inschakelen door te klikken op **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Contextmenu** door de optie **Integreren in het contextmenu** te selecteren. Meld u af of start de computer opnieuw op om de wijzigingen door te voeren. Opties van het contextmenu zijn beschikbaar in het venster **Finder** als u CTRL+klikken op een bestand uitvoert.

U kunt opties selecteren die worden weergegeven in het contextmenu. U kunt de optie **Alleen scannen** weergeven, waarmee u alleen het geselecteerde bestand kunt scannen of de optie **Alleen opschonen**, waarmee u het geselecteerde bestand vanuit het contextmenu kunt opschonen. Pas opschonen toe als een bestand is aangevallen door een virus dat schadelijke code aan het bestand heeft toegevoegd. Als dit het geval is, probeert u eerst het geïnfecteerde bestand op te schonen zodat het in de oorspronkelijke staat kan worden hersteld. Als het bestand uitsluitend uit schadelijke code bestaat, wordt het verwijderd.

Als u op de optie **Alles** selecteert, kunt u de volgende taken uitvoeren vanuit het contextmenu:

- Voorbeelden verzenden naar ESET
- Scannen
- Opschonen
- Bestanden aan quarantaine toevoegen



Instellingen importeren en exporteren

Als u een bestaande configuratie wilt importeren of uw ESET Cyber Security Pro-configuratie wilt exporteren, klikt u op **Instellingen** > **Instellingen voor importeren of exporteren**.

Importeren en exporteren is nuttig wanneer u een back-up wilt maken van uw huidige configuratie van ESET Cyber Security Pro, zodat u deze later kunt gebruiken. Instellingen exporteren is ook handig voor gebruikers die hun voorkeursconfiguratie van ESET Cyber Security Pro op meerdere systemen willen gebruiken. U kunt eenvoudig het configuratiebestand importeren om zo de gewenste instellingen over te brengen.



Als u een configuratie wilt importeren, selecteert u **Instellingen importeren** en klikt u op **Bladeren** om naar het configuratiebestand te navigeren dat u wilt importeren. Als u wilt exporteren, selecteert u **Instellingen exporteren** en gebruikt u de browser om een locatie op uw computer te selecteren waar u het configuratiebestand opslaat.

Proxyserver instellen

Instellingen voor de proxyserver kunt u configureren in **Instellingen** > **Voorkeuren voor toepassing opgeven...** (of druk op *cmd+,*) > **Proxyserver**. Als u de proxyserver op dit niveau opgeeft, worden algemene instellingen voor de proxyserver gedefinieerd voor alle functies van ESET Cyber Security Pro. De hier gedefinieerde parameters hier worden gebruikt door alle modules die verbinding met internet vereisen. ESET Cyber Security Pro ondersteunt de basistoegang en NTLM-verificatie (NT LAN Manager).

U kunt instellingen voor de proxyserver op dit niveau opgeven door het selectievakje **Proxyserver gebruiken** in te schakelen en het IP-adres of de URL van de proxyserver in te voeren in het veld **Proxyserver**. Geef in het veld Poort de poort op waarop de proxyserver verbindingen accepteert (standaard is dit 3128). U kunt ook op **Detecteren** klikken om het programma beide velden te laten invullen.

Als voor communicatie met de proxyserver verificatie is vereist, geeft u een geldige **Gebruikersnaam** en **Wachtwoord** op in de desbetreffende velden.

Licentieovereenkomst voor eindgebruikers

BELANGRIJK: Lees de volgende voorwaarden en bepalingen voor de toepassing zorgvuldig voordat u deze gaat downloaden, installeren, kopiëren of gebruiken. **DOOR DE SOFTWARE TE DOWNLOADEN, INSTALLEREN, KOPIËREN OF GEBRUIKEN GEEFT U AAN AKKOORD TE GAAN MET DEZE VOORWAARDEN EN BEPALINGEN EN ERKENT U HET PRIVACYBELEID.**

Licentieovereenkomst voor eindgebruikers

Volgens de voorwaarden van deze licentieovereenkomst voor eindgebruikers (hierna 'Overeenkomst' genoemd) die wordt uitgevoerd door en tussen ESET, spol. s r. o., gezeteld op Einsteinova 24, 85101 Bratislava, Slovak Republic, Slowakije, ingeschreven in het handelsregister dat wordt beheerd door de rechtbank van Bratislava I, Sectie Sro, volgnummer 3586/B, bedrijfsregistratienummer: 31333532 (hierna te noemen 'ESET' of 'Provider') en U, een natuurlijke persoon of rechtspersoon (hierna aangeduid als 'U' of 'Eindgebruiker'), hebt U het recht de Software in de zin van artikel 1 van deze overeenkomst te gebruiken. De Software die in Artikel 1 van deze Overeenkomst wordt gedefinieerd, kan zijn opgeslagen op een gegevensdrager, verzonden via e-mail,

gedownload van internet, gedownload van de servers van de Provider of verkregen uit andere bronnen onder de voorwaarden die hieronder worden vermeld.

DIT IS EEN OVEREENKOMST OVER DE RECHTEN VAN DE EINDGEBRUIKER EN IS GEEN KOOPOVEREENKOMST. De Provider blijft eigenaar van het exemplaar van de Software en de fysieke media in het verkochte pakket en van andere kopieën die de Eindgebruiker krachtens deze Overeenkomst mag maken.

Door op 'Ik accepteer' of 'Ik accepteer...' te klikken tijdens het installeren, downloaden, kopiëren of gebruiken van de Software, gaat U akkoord met de voorwaarden en bepalingen van deze Overeenkomst. Als U niet akkoord gaat met alle voorwaarden en bepalingen van deze Overeenkomst, moet U onmiddellijk op de annuleerknop klikken, de installatie of het downloaden annuleren of de Software, installatiemedia, bijbehorende documentatie en kwitantie vernietigen of retourneren aan ESET of de winkel waar U de Software hebt gekocht.

U GAAT ERMEE AKKOORD DAT U DOOR HET GEBRUIKEN VAN DEZE SOFTWARE AANGEEFT DAT U DEZE OVEREENKOMST HEBT GELEZEN EN BEGREPEN, EN DAT U DE VOORWAARDEN EN BEPALINGEN VAN DEZE OVEREENKOMST ACCEPTEERT.

1. **Software.** Zoals gebruikt in deze Overeenkomst, betekent de term 'Software': (i) het computerprogramma behorende bij deze Overeenkomst en alle onderdelen ervan; (ii) de volledige inhoud van de schijven, cd-roms, dvd's, e-mails en eventuele bijlagen, of andere media waarbij deze Overeenkomst wordt verstrekt, inclusief de objectcodevorm van de geleverde software op een gegevensdrager, via e-mail of gedownload via internet, (iii) eventuele bijbehorende schriftelijke materialen en eventuele andere documentatie met betrekking tot de Software, met name een beschrijving van de Software, specificaties ervan, een beschrijving van de eigenschappen of de werking van de Software, een beschrijving van de operationele omgeving waarin de Software wordt gebruikt, instructies voor het gebruik of de installatie van de Software of een beschrijving van hoe de Software te gebruiken (hierna 'Documentatie' genoemd); (iv) kopieën van de Software, patches voor mogelijke fouten in de Software, toevoegingen aan de Software, uitbreidingen voor de Software, aangepaste versies van de Software en updates van Softwarecomponenten, indien van toepassing, aan U in licentie gegeven door de Provider op grond van artikel 3 van deze Overeenkomst. De Software wordt exclusief geleverd in de vorm van uitvoerbare objectcode.

2. **Installatie, Computer en Licentiecode**. Software die is geleverd op een gegevensdrager, via e-mail, gedownload van internet, gedownload vanaf de servers van de Provider of die op andere wijze is verkregen, moet worden geïnstalleerd. U moet de Software op een correct geconfigureerde Computer installeren, die minimaal moet voldoen aan de vereisten in de Documentatie. De installatiemethode staat beschreven in de Documentatie. Er mogen geen computerprogramma's of hardware worden geïnstalleerd op de computer waarop u de Software installeert die een negatieve invloed kunnen hebben op de Software. Computer betekent hardware, waaronder maar niet beperkt tot personal computers, laptops, werkstations, palmtopcomputers, smartphones, mobiele elektronische apparaten of andere elektronische apparaten waarvoor de Software is ontworpen, waarop de Software wordt geïnstalleerd en/of gebruikt. Licentiecode betekent de unieke reeks symbolen, letters, cijfers of speciale tekens die aan de Eindgebruiker wordt verstrekt om het legale gebruik, de specifieke versie of uitbreiding van de voorwaarden van de Licentie van de Software mogelijk te maken overeenkomstig deze Overeenkomst.

3. **Licentie**. Onderworpen aan de voorwaarde dat U akkoord bent gegaan met de voorwaarden van deze Overeenkomst en voldoet aan alle voorwaarden en bepalingen van deze Overeenkomst, verleent de Provider U de volgende rechten (hierna 'Licentie' genoemd):

a) **Installatie en gebruik.** U hebt het niet-exclusieve, niet-overdraagbare recht om de Software te installeren op de harde schijf van een computer of een andere permanent medium voor gegevensopslag, installatie en opslag van de Software in het geheugen van een computersysteem, en om de Software te implementeren, op te slaan en weer te geven.

b) **Bepaling van het aantal licenties.** Het recht om de Software te gebruiken zal gebonden zijn door het aantal

Eindgebruikers. Een Eindgebruiker wordt geacht het volgende in te houden: (i) installatie van de Software op één computersysteem; of (ii) indien de omvang van een licentie is gebonden aan het aantal postvakken, dan wordt een Eindgebruiker geacht een computergebruiker te zijn die e-mail ontvangt via een Mail User Agent (hierna aangeduid als 'een MUA'). Als een MUA e-mail ontvangt en deze vervolgens automatisch naar verschillende gebruikers distribueert, wordt het aantal Eindgebruikers bepaald op basis van het werkelijk aantal gebruikers waarvoor de e-mail wordt gedistribueerd. Indien een e-mailserver fungeert als e-mailgateway, is het aantal Eindgebruikers gelijk aan het aantal e-mailservergebruikers waarvoor een dergelijke gateway services verleent. Als een onbekend aantal e-mailadressen is gericht aan en wordt ontvangen door een gebruiker (bijvoorbeeld door middel van aliassen) en berichten niet automatisch worden gedistribueerd door de client aan een groter aantal gebruikers, is een licentie voor een computer nodig. U mag dezelfde Licentie niet op meerdere computers tegelijk gebruiken. De Eindgebruiker is alleen gerechtigd de Licentiecode op te geven in de Software voor zover de Eindgebruiker het recht heeft de Software te gebruiken overeenkomstig de beperking voor wat betreft het aantal Licenties die de Provider heeft verleend. De Licentiecode wordt vertrouwelijk beschouwd. U mag de Licentie niet delen met derden of derden toestaan de Licentiecode te gebruiken, tenzij dit wordt toegestaan door deze Overeenkomst of deze Provider. Als uw Licentiecode openbaar is geworden, stel de Provider hier dan onmiddellijk van op de hoogte.

c) **Business Edition.** Een Business Edition-versie van de Software moet worden verkregen om de Software te gebruiken op mailservers, mailrelais, mailgateways of internetgateways.

d) **Duur van de licentie.** Uw recht om de Software te gebruiken zal voor beperkte tijd gelden.

e) **OEM-software.** OEM-software zal worden beperkt tot de computer waarop deze is meegeleverd. Deze kan niet worden overgedragen naar een andere computer.

f) **NFR-, TRIAL-software.** Software die wordt geclassificeerd als 'Not-for-resale' (Niet voor wederverkoop), NFR of TRIAL, is gratis en mag alleen worden gebruikt voor de demonstratie of het testen van de functies van de Software.

g) **Beëindiging van de Licentie.** De Licentie zal automatisch worden beëindigd aan het einde van de periode waarvoor deze is verleend. Als U niet voldoet aan een van de bepalingen van deze Overeenkomst, heeft de Provider het recht zich terug te trekken uit de Overeenkomst, zonder afbreuk te doen aan enig recht of rechtsmiddel waarover de Provider beschikt voor dit soort gevallen. In geval van annulering van de Licentie, moet U onmiddellijk op eigen kosten de Software en alle back-upkopieën verwijderen, vernietigen of retourneren aan ESET of de winkel waar U de Software hebt gekocht. Bij beëindiging van de Licentie heeft de Provider ook het recht om het recht van de Eindgebruiker op het gebruik van de functies van de Software te annuleren die een verbinding met de servers van de Provider of van derden vereisen.

4. **Functies met gegevensverzameling en vereisten voor de internetverbinding.** De Software werkt alleen correct als er een verbinding met internet is en er regelmatig verbinding met de servers van de Provider of derden kan worden gemaakt en toepasselijke gegevens kunnen worden verzameld overeenkomstig het Privacybeleid. De verbinding met internet en het verzamelen van toepasselijke gegevens zijn nodig voor de volgende functies van de Software:

a) **Updates voor de Software.** De Provider zal het recht hebben van tijd tot tijd updates uit te geven voor de Software ('Updates'), maar zal niet verplicht zijn te voorzien in Updates. Deze functie is ingeschakeld onder de standaardinstellingen van de Software en Updates worden dus automatisch geïnstalleerd, tenzij de Eindgebruiker automatische installatie van Updates heeft uitgeschakeld. Om updates te kunnen aanbieden moet de echtheid van de licentie kunnen worden gecontroleerd, waarvoor het nodig is om overeenkomstig het Privacybeleid informatie te verzamelen over uw Computer en/of het platform waarop de Software is geïnstalleerd.

b) **Doorsturen van infiltraties en informatie naar de Provider.** De Software bevat functies die voorbeelden

verzamelen van computervirussen en andere kwaadwillige computerprogramma's en verdachte, problematische, mogelijk ongewenste of mogelijk onveilige objecten zoals bestanden, URL's, IP-pakketten en Ethernet-frames (hierna 'Infiltraties' genoemd) en verzenden ze vervolgens naar de Provider, met inbegrip van, maar niet beperkt tot informatie over het installatieproces, de computer en/of het platform waarop de Software geïnstalleerd is, informatie over de bewerkingen en functionaliteit van de Software en informatie over apparaten in het lokaal netwerk, zoals type, verkoper, model en/of naam van het apparaat (hierna 'Informatie' genoemd). De Informatie en Infiltraties kunnen informatie bevatten (met inbegrip van willekeurig of toevallig verkregen persoonlijke gegevens) over de Eindgebruiker of andere gebruikers van de computer waarop de Software is geïnstalleerd, en bestanden beïnvloed door Infiltraties met bijhorende metagegevens.

Informatie en Infiltraties kunnen door de volgende functies van de Software worden verzameld:

i. De LiveGrid-reputatiesysteemfunctie omvat het verzamelen en in één richting naar de Provider verzenden van hashes met betrekking tot Infiltraties. Deze functie wordt ingeschakeld via de standaardinstellingen van de Software.

ii. LiveGrid-feedbacksysteem is een functie die onder andere Infiltraties en bijbehorende metagegevens en Informatie verzamelt en naar de Provider stuurt. Deze functie wordt gedurende het installatieproces van de Software door de Eindgebruiker geactiveerd.

De Provider gebruikt de ontvangen Informatie en Infiltraties uitsluitend voor analyse van en onderzoek naar Infiltraties, verbetering van de Software en controle van de authenticiteit van de Licentie, en de Provider zal passende maatregelen nemen om de vertrouwelijkheid van ontvangen Informatie en Infiltraties te waarborgen. Door deze functie van de Software te activeren, worden er mogelijk infiltraties en informatie verzameld en verwerkt door de Provider zoals aangegeven in het Privacybeleid en overeenkomstig relevante juridische regels. U kunt deze functies op elk moment uitschakelen.

Voor het doel van deze Overeenkomst is het noodzakelijk om gegevens te verzamelen, verwerken en op te slaan, zodat de Provider kan controleren of U voldoet aan het Privacybeleid. U bevestigt hierbij dat U ermee akkoord gaat dat de Provider met zijn eigen middelen controleert of U de Software overeenkomstig de bepalingen van deze Overeenkomst gebruikt. U bevestigt hierbij dat U ermee akkoord gaat dat het voor het doel van deze Overeenkomst noodzakelijk is dat tijdens communicatie tussen de Software en de computersystemen van de Provider of die van diens zakelijke partners uw gegevens worden overgebracht als onderdeel van de verspreiding door de Provider en het ondersteuningsnetwerk met als doel de functionaliteit van de Software en autorisatie om de Software te gebruiken te garanderen en de rechten van de Provider te beschermen.

Na beëindiging van deze Overeenkomst, is de Provider of elk van diens zakelijk partners als onderdeel van het distributie- en ondersteuningsnewerk van de Provider, gerechtigd essentiële gegevens die u identificeren over te dragen, verwerken en op te slaan ten behoeve van factureringsdoeleinden, de prestaties van deze Overeenkomst en het overbrengen van meldingen naar uw Computer. U gaat er hierbij mee akkoord om meldingen en berichten te ontvangen, waaronder maar niet beperkt tot marketinginformatie.

Details over privacy, beveiliging van persoonlijke gegevens en Uw rechten als betrokkene vindt u in het Privacybeleid, dat als onderdeel van het installatieproces rechtstreeks toegankelijk is op de website van de Aanbieder. Of bezoek de Help-sectie van de Software.

5. **Eindgebruikersrechten uitoefenen**. U moet uw Eindgebruikersrechten persoonlijk of via uw medewerkers uitoefenen. U hebt alleen het recht om de Software te gebruiken om uw activiteiten te beschermen en deze Computers of computersystemen te beveiligen waarvoor U een Licentie hebt verkregen.

6. **Beperkingen op rechten.** U mag geen componenten kopiëren, verspreiden of uitnemen, of afgeleide producten van de Software maken. Bij gebruik van de Software bent U verplicht te voldoen aan de volgende beperkingen:

a) U mag een kopie van de Software opslaan op een permanent opslagmedium als back-upkopie voor uw archief, mits uw back-upkopie niet wordt geïnstalleerd of gebruikt op een computer. Alle andere kopieën die U van de Software maakt, gelden als schending van deze Overeenkomst.

b) U mag de Software niet gebruiken, wijzigen, vertalen of reproduceren of gebruiksrechten op de Software overdragen of kopieën van de Software gebruiken op een andere wijze dan in deze Overeenkomst is genoemd.

c) U mag de Software niet verkopen, onder sublicentie geven, leasen of huren of lenen of de Software gebruiken voor het verrichten van commerciële diensten.

d) U mag geen reverse engineering, decompilatie of disassemblage van de Software uitvoeren of anderszins trachten de broncode van de Software te achterhalen, behoudens voor zover deze beperking uitdrukkelijk is verboden door de wet.

e) U gaat akkoord dat U de Software alleen zult gebruiken op een manier die voldoet aan alle toepasselijke wetten in het rechtsgebied waarin U de Software gebruikt, met inbegrip van, maar niet beperkt tot, toepasselijke beperkingen betreffende auteursrecht en andere intellectuele eigendomsrechten.

f) U stemt ermee in dat U de Software en de functies ervan uitsluitend zult gebruiken op een wijze die de toegangsmogelijkheden van andere Eindgebruikers tot deze services niet belemmert. De Provider behoudt zich het recht voor het bereik van de services die worden geleverd aan afzonderlijke Eindgebruikers te beperken, om het gebruik van de services door een zo hoog mogelijk aantal Eindgebruikers te kunnen waarborgen. Onder het beperken van het bereik van de services wordt ook verstaan het volledig beëindigen van de mogelijkheid van het gebruik van functies van de Software en het verwijderen van Gegevens en informatie op de servers van de Provider en van derden in verband met een specifieke functie van de Software.

g) U gaat ermee akkoord geen activiteiten te ontplooien met de Licentiecode die in strijd zijn met de voorwaarden van deze Overeenkomst of die erin kunnen resulteren dat de Licentiecode in handen valt van iemand die niet gerechtigd is de Software te gebruiken, zoals onder andere het geval is bij overdracht in welke vorm dan ook van een gebruikte of ongebruikte Licentiecode, evenals de ongeoorloofde reproductie of distributie van gedupliceerde of gegenereerde Licentiecodes of het gebruik van de Software als gevolg van het gebruik van een Licentiecode die is verkregen uit een andere bron dan de Provider.

7. **Auteursrecht**. De Software en alle rechten, met inbegrip van, maar niet beperkt tot, eigendomsrechten en intellectuele-eigendomsrechten daarop, zijn het eigendom van ESET en/of zijn licentiegevers. Ze worden beschermd door internationale verdragen en door alle andere van toepassing zijnde nationale wetten van het land waarin de Software wordt gebruikt. De structuur, indeling en code van de Software zijn de waardevolle handelsgeheimen en vertrouwelijke informatie van ESET en/of zijn licentiegevers. U mag de Software niet kopiëren, behalve zoals uiteengezet in artikel 6 (a). Elke kopie die U mag maken overeenkomstig deze Overeenkomst, moet hetzelfde auteursrecht en andere eigendomsrechten bevatten die op de Software van toepassing zijn. Als U reverse engineering, decompilatie, disassemblage uitvoert of op andere wijze probeert de broncode van de Software te achterhalen, in strijd met de voorwaarden van deze Overeenkomst, gaat U ermee akkoord dat alle informatie die op deze wijze wordt verkregen, automatisch en onherroepelijk volledig zal worden geacht te zijn overgedragen aan de Provider en het eigendom te zijn van de Provider, vanaf het moment dat dergelijke informatie tot stand komt, onverminderd de rechten van de Provider met betrekking tot de breuk van deze Overeenkomst.

8. **Voorbehoud van rechten**. De Provider behoudt alle rechten op de Software voor, met uitzondering van de rechten die nadrukkelijk aan U als Eindgebruiker van de Software worden verleend krachtens de voorwaarden van deze Overeenkomst.

9. **Meerdere taalversies, dubbele mediasoftware, meerdere kopieën**. Indien de Software meerdere platforms of talen ondersteunt, of als U meerdere kopieën van de Software ontvangt, mag U de Software alleen gebruiken op

het aantal computersystemen en voor de versies waarvoor U een Licentie hebt verkregen. Het is niet toegestaan versies of exemplaren van de Software die U niet gebruikt, te verkopen, verhuren, leasen, onder sublicentie te geven, uit te lenen of over te dragen.

10. **Aanvang en beëindiging van de Overeenkomst**. Deze Overeenkomst is van kracht vanaf de datum waarop U akkoord gaat met de voorwaarden van deze Overeenkomst. U kunt deze Overeenkomst op elk moment beëindigen door de Software, alle back-upkopieën en alle gerelateerde materialen die door de Provider of zijn zakenpartners zijn geleverd, permanent te verwijderen, vernietigen en op eigen kosten te retourneren. Ongeacht de wijze van beëindiging van deze Overeenkomst, blijven de bepalingen in Artikel 7, 8, 11, 13, 19 en 21 van kracht zonder tijdsbeperking.

11. **VERKLARINGEN VAN DE EINDGEBRUIKER**. ALS EINDGEBRUIKER ERKENT U DAT DE SOFTWARE IN DE 'OORSPRONKELIJKE STAAT' IS GELEVERD, ZONDER EXPLICIETE OF IMPLICIETE GARANTIE VAN WELKE AARD DAN OOK EN VOOR ZOVER DAT VOLGENS DE TOEPASSELIJKE WETTEN IS TOEGESTAAN. NOCH DE PROVIDER, NOCH DE LICENTIEGEVERS OF GELIEERDE BEDRIJVEN, NOCH DE AUTEURSRECHTHOUDERS BIEDEN ENIGE EXPLICIETE OF IMPLICIETE VERTEGENWOORDIGINGEN OF GARANTIES, MET INBEGRIP VAN MAAR NIET BEPERKT TOT VERKOOPGARANTIES, GARANTIES DAT DE SOFTWARE GESCHIKT IS VOOR EEN BEPAALD DOEL OF GARANTIES DAT DE SOFTWARE GEEN INBREUK MAAKT OP OCTROOIEN, AUTEURSRECHT, HANDELSMERKEN OF ANDERE RECHTEN VAN DERDEN. DE PROVIDER OF ENIGE ANDERE PARTIJ GARANDEERT NIET DAT DE FUNCTIES IN DE SOFTWARE VOLDOEN AAN UW EISEN OF DAT DE WERKING VAN DE SOFTWARE ONONDERBROKEN OF FOUTLOOS ZAL ZIJN. U AANVAARDT ALLE VERANTWOORDELIJKHEID EN RISICO VOOR DE SELECTIE VAN DE SOFTWARE OM UW BEOOGDE RESULTATEN TE BEHALEN EN VOOR DE INSTALLATIE, HET GEBRUIK EN DE RESULTATEN DIE HIERUIT VOORTVLOEIEN.

12. **Geen verdere verplichtingen**. Deze Overeenkomst schept geen verplichtingen voor de Provider en zijn licentiegevers, anders dan specifiek is uiteengezet in deze Overeenkomst.

13. **BEPERKING VAN DE AANSPRAKELIJKHEID**. VOOR ZOVER IS TOEGESTAAN VOLGENS DE TOEPASSELIJKE WETTEN, ZULLEN DE PROVIDER, ZIJN WERKNEMERS OF LICENTIEGEVERS IN GEEN GEVAL AANSPRAKELIJK WORDEN GESTELD VOOR WINST-, INKOMSTEN- OF OMZETDERVING, VOOR GEGEVENSVERLIES, VOOR KOSTEN DIE ZIJN GEMAAKT OM VERVANGENDE GOEDEREN OF DIENSTEN AAN TE SCHAFFEN, VOOR BESCHADIGING VAN EIGENDOM, LICHAMELIJK LETSEL, ONDERBREKING VAN DE BEDRIJFSVOERING, VERLIES VAN BEDRIJFSINFORMATIE, OF VOOR ENIGE SPECIALE, DIRECTE, INDIRECTE, INCIDENTELE, ECONOMISCHE OF VERVANGENDE SCHADE, SCHADE ALS GEVOLG VAN VERNIELING, SPECIALE OF GEVOLGSCHADE, OP WELKE MANIER DAN OOK VEROORZAAKT, ONGEACHT OF DEZE HET GEVOLG IS VAN EEN CONTRACT, EEN OPZETTELIJKE OVERTREDING, NALATIGHEID OF EEN ANDER FEIT DAT DE SCHADE HEEFT VEROORZAAKT, ALS GEVOLG VAN HET GEBRUIK VAN OF HET ONVERMOGEN TOT HET GEBRUIK VAN DE SOFTWARE, ZELFS ALS DE PROVIDER OF ZIJN LICENTIEGEVERS ZIJN GEWEZEN OP DE MOGELIJKHEID VAN DERGELIJKE SCHADE. AANGEZIEN IN BEPAALDE LANDEN EN RECHTSGEBIEDEN HET NIET IS TOEGESTAAN AANSPRAKELIJKHEID UIT TE SLUITEN, MAAR HET MOGELIJK WEL IS TOEGESTAAN AANSPRAKELIJKHEID TE BEPERKEN, WORDT IN DERGELIJKE GEVALLEN DE AANSPRAKELIJKHEID VAN DE PROVIDER, ZIJN MEDEWERKERS OF LICENTIEGEVERS OF GELIEERDE BEDRIJVEN BEPERKT TOT HET BEDRAG DAT U VOOR DE LICENTIE HEBT BETAALD.

14. Niets in deze Overeenkomst doet afbreuk aan de wettelijke rechten van enige partij die als consument handelt indien deze hiermee in strijd zijn.

15. **Technische ondersteuning**. ESET of derden in opdracht van ESET verlenen naar eigen inzicht technische ondersteuning zonder enige garanties of verklaringen. De Eindgebruiker is verplicht een back-up te maken van alle bestaande gegevens, software en programmavoorzieningen voorafgaand aan het verlenen van de technische ondersteuning. ESET en/of derden in opdracht van ESET kunnen geen aansprakelijkheid aanvaarden voor schade of verlies van gegevens, eigendom, software of hardware of verlies van winst als gevolg van het verlenen van technische ondersteuning. ESET en/of derden in opdracht van ESET behouden het recht voor om te beslissen of

het oplossen van het probleem buiten het bereik valt van de technische ondersteuning. ESET behoudt het recht voor om naar eigen inzicht technische ondersteuning te weigeren, op te schorten of de verlening ervan te beëindigen. Licentie-informatie, Informatie en andere gegevens overeenkomstig het Privacybeleid zijn mogelijk vereist om technische ondersteuning te verkrijgen.

16. **Overdracht van de licentie**. De Software kan van het ene computersysteem naar het andere worden overgedragen, tenzij dit in strijd is met de voorwaarden van de Overeenkomst. Indien dit niet in strijd is met de voorwaarden van de Overeenkomst, heeft de Eindgebruiker alleen het recht om de Licentie en alle rechten die voortvloeien uit deze overeenkomst, permanent over te dragen aan een andere Eindgebruiker met toestemming van de Provider, onder voorwaarde dat (i) de oorspronkelijke Eindgebruiker geen kopieën van de Software behoudt; (ii) de overdracht van rechten direct is, dat wil zeggen van de oorspronkelijke Eindgebruiker naar de nieuwe Eindgebruiker; (iii) de nieuwe Eindgebruiker alle rechten en verplichtingen van de oorspronkelijke Eindgebruiker moet overnemen volgens de voorwaarden van deze Overeenkomst; (iv) de oorspronkelijke Eindgebruiker de nieuwe Eindgebruiker de documentatie moet verstrekken waardoor verificatie van de echtheid van de Software zoals gespecificeerd in artikel 17 mogelijk is.

17. **Verificatie van de echtheid van de Software**. De Eindgebruiker kan het recht hebben de Software op een van de volgende manieren te gebruiken: (i) door middel van een licentiecertificaat dat door de Provider of een door de Provider aangewezen derde partij is uitgegeven; (ii) door middel van een schriftelijke licentieovereenkomst, indien een dergelijke overeenkomst is gesloten; (iii) door middel van e-mail aan de Provider met de licentiegegevens (gebruikersnaam en wachtwoord) om Updates mogelijk te maken. Om de echtheid van de Software te controleren is het mogelijk noodzakelijk om in overeenstemming met het Privacybeleid Licentie-informatie en Eindgebruikersgegevens te verzamelen waaraan U bent te identificeren.

18. **Licenties voor de overheid en de Amerikaanse regering**. De Software zal worden verstrekt aan de overheid, met inbegrip van de Amerikaanse regering, met de licentierechten en beperkingen die in deze Overeenkomst zijn beschreven.

19. **Naleving van handelscontroles**.

a) U zult de Software niet direct of indirect uitvoeren, wederuitvoeren, overdragen of anderszins ter beschikking stellen aan enig persoon, of deze op enigerlei wijze gebruiken, of betrokken zijn bij enige handeling die ertoe kan leiden dat ESET of haar holdingmaatschappijen, haar dochterondernemingen en de dochterondernemingen van een van haar holdingmaatschappijen, als ook entiteiten die door haar holdingmaatschappijen (hierna 'Gelieerde ondernemingen' genoemd) worden gecontroleerd, in strijd handelt met, of onderworpen is aan negatieve gevolgen krachtens Handelscontrolewetten, die het volgende omvatten:

i. alle wetten die de uitvoer, wederuitvoer of overdracht van goederen, software, technologie of diensten controleren, beperken of aan vergunningsvereisten onderwerpen en die zijn uitgevaardigd of aangenomen door een regering, staat of regelgevende instantie van de Verenigde Staten van Amerika, Singapore, het Verenigd Koninkrijk, de Europese Unie of een van haar lidstaten, of een land waarin de verplichtingen uit hoofde van de overeenkomst moeten worden uitgevoerd, of waarin het ESET of een van aan haar Gelieerde ondernemingen is gevestigd of werkzaam is (hierna 'Exportcontrolewetten' genoemd), en

ii. alle economische, financiële, handels- of andere sanctie, beperking, embargo, invoer- of uitvoerverbod, verbod op de overdracht van fondsen of activa of op het verrichten van diensten, of elke gelijkwaardige maatregel die wordt opgelegd door een regering, staat of regelgevende autoriteit van de Verenigde Staten van Amerika, Singapore, het Verenigd Koninkrijk, de Europese Unie of een van haar lidstaten, of een land waarin verplichtingen uit hoofde van de Overeenkomst moeten worden uitgevoerd, of waarin het ESET of een van aan haar Gelieerde ondernemingen is gevestigd of werkzaam is (hierna 'Sanctiewetgeving' genoemd).

b) ESET heeft het recht om haar verplichtingen uit hoofde van deze Voorwaarden met onmiddellijke ingang op te schorten of te beëindigen in het geval dat:

i. ESET naar haar redelijke mening vaststelt dat de Gebruiker de bepaling van artikel 19.a van de Overeenkomst heeft overtreden of waarschijnlijk zal overtreden; of

ii. de Eindgebruiker en/of de Software wordt onderworpen aan Handelscontrolewetten en als gevolg daarvan ESET vaststelt dat, naar haar redelijke mening, het voortbestaan van haar verplichtingen krachtens de Overeenkomst ertoe kan leiden dat ESET of aan haar Gelieerde ondernemingen de Handelscontrolewetten schendt of onderworpen wordt aan negatieve gevolgen.

c) Niets in de Overeenkomst is bedoeld om een van de partijen ertoe aan te zetten of te verplichten te handelen of af te zien van handelen (of ermee in te stemmen te handelen of af te zien van handelen), en niets mag als zodanig worden geïnterpreteerd, op een wijze die niet in overeenstemming is met, wordt bestraft met of is verboden onder toepasselijke Handelscontrolewetten.

20. **Kennisgevingen**. Alle kennisgevingen en de geretourneerde Software en Documentatie moeten worden gestuurd naar: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. **Toepasselijk recht**. Op deze Overeenkomst is het Slowaakse recht van toepassing en deze Overeenkomst wordt geïnterpreteerd in overeenstemming met het Slowaakse recht. De Eindgebruiker en de Provider gaan ermee akkoord dat conflictbepalingen van het toepasselijke recht en het Weens koopverdrag niet van toepassing zijn. U stemt er uitdrukkelijk mee in dat alle geschillen of vorderingen die voortvloeien uit deze Overeenkomst met betrekking tot de Provider of eventuele geschillen of vorderingen met betrekking tot het gebruik van de Software, zullen worden behandeld door de rechtbank te Bratislava I en U stemt er uitdrukkelijk mee in dat de genoemde rechtbank jurisdictie zal hebben.

22. **Algemene bepalingen**. Indien een van de voorwaarden van deze Overeenkomst ongeldig of niet-afdwingbaar blijkt, heeft dat geen gevolgen voor de geldigheid van de overige bepalingen van de Overeenkomst. Deze bepalingen blijven geldig en afdwingbaar volgens de voorwaarden van deze Overeenkomst. In geval van een discrepantie tussen taalversies van deze Overeenkomst heeft de Engelstalige versie voorrang. Deze Overeenkomst kan slechts worden gewijzigd in schriftelijke vorm, ondertekend door een bevoegde vertegenwoordiger van de Provider of een persoon die uitdrukkelijk bevoegd is om in die hoedanigheid te handelen onder de voorwaarden van een volmacht.

Dit is de volledige Overeenkomst tussen de Provider en U met betrekking tot de Software en deze vervangt alle voorgaande verklaringen, besprekingen, toezeggingen, mededelingen of bekendmakingen met betrekking tot de Software.

EULA ID: HOM-ECS-20-01

Privacybeleid

ESET, spol. s r. o., gezeteld op Einsteinova 24, 851 01 Bratislava, Slowaakse Republiek, ingeschreven in het handelsregister dat wordt beheerd door de rechtbank Bratislava I District Court, sectie Sro, volgnr. 3586/B, bedrijfsregistratienummer: 31333532 als een Gegevensbeheerder (“ESET” of “Wij”, “We”, “Ons” of “Onze”) wil graag transparant zijn als het gaat om de verwerking van persoonlijke gegevens en de privacy van onze klanten. Om dit doel te verwezenlijken, publiceren Wij dit Privacybeleid met als enige doel om onze klant (“Eindgebruiker” of “U”) over de volgende onderwerpen te informeren:

- Verwerking van persoonsgegevens,
- Vertrouwelijkheid van gegevens,
- Rechten van de persoon van wie de gegevens afkomstig zijn.

Verwerking van persoonsgegevens

Door ESET geleverde services geïmplementeerd in ons product worden geleverd overeenkomstig de voorwaarden van de Licentieovereenkomst voor eindgebruikers ("EULA"), maar sommige daarvan vereisen mogelijke specifieke aandacht. Wij willen u graag meer informatie geven over het verzamelen van gegevens in verband met de levering van onze services. Wij verzorgen verschillende services die zijn beschreven in de EULA en productdocumentatie, zoals een update-/upgradeservice, ESET LiveGrid®, beveiliging tegen misbruik van gegevens, ondersteuning, enz. Om dit te kunnen doen, moeten wij de volgende informatie verzamelen:

- Updatestatistieken en andere statistieken met informatie over het installatieproces en uw computer, waaronder het platform waarop ons product is geïnstalleerd en informatie over de bewerkingen en functionaliteit van onze producten, zoals besturingssysteem, hardware-informatie, installatie-id's, licentie-id's, IP-adres, MAC-adres, configuratie-instellingen van het product.
- Eénrichtings-hashes met betrekking tot infiltraties als onderdeel van het ESET LiveGrid®-reputatiesysteem, die de efficiëntie verbeteren van de antimalwareoplossingen door gescande bestanden te vergelijken met een database met items die op een witte of zwarte lijst in de cloud zijn geplaatst.
- Verdachte voorbeelden en metagegevens uit de praktijk als onderdeel van het ESET LiveGrid®-feedbacksysteem waarmee ESET direct kan reageren op de behoeften van onze eindgebruikers en snel kan inspelen op de nieuwste bedreigingen. Wij zijn afhankelijk van toezending door u
  - van infiltraties zoals potentiële voorbeelden van virussen en andere schadelijke programma's en verdachte, problematische, potentieel ongewenste of potentieel onveilige objecten, zoals uitvoerbare bestanden, e-mailberichten die u als spam hebt gemeld of door ons product zijn gemarkeerd;
  - informatie over apparaten in het lokale netwerk, zoals het type, de leverancier, het model en/of de naam van het apparaat;
  - informatie over het gebruik van internet, zoals IP-adressen en geografische informatie, IP-pakketten, webadressen en ethernetframes;
  - crashdumpbestanden en informatie daarin.

We willen op zich geen gegevens verzamelen buiten dit bereik, maar soms is het onmogelijk om dit te voorkomen. Gegevens die per ongeluk worden verzameld, kunnen in malware zelf zijn opgenomen (verzameld zonder uw kennis of goedkeuring) of als onderdeel van bestandsnamen of webadressen en het is niet onze bedoeling om deze gegevens deel te laten uitmaken van onze systemen of deze gegevens te verwerken voor het doel dat in dit Privacybeleid is beschreven.

- Licentie-informatie, zoals licentie-ID en persoonlijke gegevens zoals naam, achternaam, adres, e-mailadres, is vereist voor factureringsdoeleinden, verificatie van de echtheid van uw licentie en voor de levering van onze services.
- Contactgegevens en gegevens in uw ondersteuningsaanvragen kunnen vereist zijn, zodat ESET u ondersteuningsservices kan bieden. Op basis van het kanaal dat u kiest om contact met ons op te nemen, kunnen Wij mogelijk uw e-mailadres, telefoonnummer, licentie-informatie, productdetails en beschrijving van uw ondersteuningsaanvraag verzamelen. Mogelijk wordt u gevraagd om ons andere informatie te verschaffen teneinde u ondersteuningsservices te kunnen bieden.

Vertrouwelijkheid van gegevens

ESET is een internationaal bedrijf via gelieerde rechtspersonen of partners als onderdeel van ons distributie-, service- en ondersteuningsnetwerk. Informatie die door ESET wordt verwerkt, kan worden overgedragen naar en van gelieerde entiteiten of partners om uitvoering te geven aan de Gebruiksrechtovereenkomst voor Eindgebruikers zoals de levering van services, ondersteuning of facturering. Op basis van uw locatie en de service die U hebt gekozen te gebruiken, moeten Wij mogelijk uw gegevens overbrengen naar een land zonder het beschermingsniveau dat is voorgeschreven door de Europese Commissie. Zelfs als dat het geval is, is elke overdracht van gegevens onderworpen aan wettelijke regelgeving inzake gegevensbescherming en vindt dit alleen plaats als dit ook echt nodig is. Er dienen zonder uitzondering modelcontractbepalingen, bindende bedrijfsvoorschriften of andere gepaste vormen van beveiliging van kracht te zijn.

Wij streven ernaar te voorkomen dat gegevens langer worden opgeslagen dan nodig is terwijl wij ESET-services aanbieden. Onze bewaarperiode kan langer zijn dan de geldigheid van uw licentie om u de tijd te geven uw licentie gemakkelijk te vernieuwen. Minimale en gepseudonimiseerde statistieken en andere gegevens van ESET LiveGrid® kunnen verder worden verwerkt voor statistische doeleinden.

ESET implementeert gepaste technische en organisatorische maatregelen om een beveiligingsniveau te realiseren dat afdoende is voor potentiële risico's. Wij doen Ons best om de vertrouwelijkheid, integriteit, beschikbaarheid en bestendigheid van verwerkingssystemen en -services blijvend te garanderen. In het geval van een gegevensschending waarbij een risico bestaat dat uw rechten en vrijheden in gevaar komen, zullen Wij de toezichthoudende autoriteit alsmede iedereen bij wie wij gegevens hebben verzameld, hiervan op de hoogte stellen. Als gegevensonderwerp hebt u het recht om een klacht in te dienen bij een toezichthouder.

Rechten van degene van wie de gegevens afkomstig zijn.

ESET is onderworpen aan regelgeving van Slowaakse wetten en Wij zijn gebonden aan gegevensbeschermingswetgeving van de Europese Unie. Onder voorbehoud van de voorwaarden die zijn vastgelegd in van toepassing zijnde gegevensbeschermingswetten, hebt U de volgende rechten als betrokkene:

- het recht om toegang te krijgen tot uw persoonsgegevens bij ESET,
- het recht op rectificatie van uw persoonsgegevens indien onjuist (U hebt ook het recht om onvolledige persoonsgegevens aan te vullen),
- het recht om uw persoonsgegevens te laten verwijderen,
- het recht op beperking van het verwerken van uw persoonsgegevens,
- het recht om verwerking te weigeren,
- het recht om bezwaar in te dienen alsmede,
- het recht op overzetbaarheid van gegevens.

Als u uw recht als betrokkene wilt uitoefenen of een vraag hebt of een zorg wilt uiten, stuur ons dan een bericht op:

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

dpo@eset.sk