ESET Cloud Office Security

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 Cloud Office Security 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. 20-12-2023

1 Overzicht 1
1.1 Belangrijke functies 2
1.2 Nieuwe functies 5
1.3 Integratie 6
2 Specificaties 7
2.1 Vereisten 7
2.2 Ondersteunde Microsoft 365-abonnementen 8
2.3 Ondersteunde Google Workspace-abonnementen 9
2.4 Ondersteunde webbrowsers 9
2.5 Beperkingen en beleid voor gegevensretentie 9
3 Licenties voor ESET Cloud Office Security 11
3.1 ESET Business Account 12
3.1 Een nieuw ESET Business Account-account maken 12
3.1 ESET Cloud Office Security-licentie toevoegen aan ESET Business Account 12
3.1 Beheren ESET Business Account 13
3.2 ESET MSP Administrator 14
4 Activeren ESET Cloud Office Security 15
4.1 Deactiveren ESET Cloud Office Security 17
5 Uw tenants beheren in Instellingen 18
5.1 Uw eerste tenant toevoegen 20
5.2 Microsoft 365-tenant 22
5.3 Google Workspace-tenant 25
5.4 Tenant verwijderen uit ESET Cloud Office Security 31
5.5 ESET Cloud Office Security uit de Azure-portal verwijderen 32
6 Navigeren in ESET Cloud Office Security 32
7 ESET LiveGuard Advanced 34
8 Dashboard 35
9 Gebruikers 37
10 Teams en sites 38
11 Detecties 39
12 Rapporten 41
13 Quarantaine 43
14 Scanlogboeken 45
15 Beleid 46
15.1 Beveiligingsinstellingen voor Exchange Online 49
15.2 Beveiligingsinstellingen voor Gmail 52
15.3 Beveiligingsinstellingen voor OneDrive 55
15.4 Beveiligingsinstellingen voor Google Drive 56
15.5 Beveiligingsinstellingen voor Teamgroepen 57
15.6 Beveiligingsinstellingen voor SharePoint-sites 58
15.7 Beveiligingsinstellingen voor ESET LiveGuard Advanced 59
15.8 Rapportage en beveiliging door zelflerende systemen 60
16 Licentiebeheer 62
16.1 ESET Cloud Office Security-gebruikerstoegang voor een specifiek bedrijf 64
17 Controlelogboek 65
18 Feedback verzenden 66
19 Technische ondersteuning 66
20 Beschikbaarheid van de service 67

20.1 Beveiliging voor ESET Cloud Office Security 67
20.2 Gebruiksvoorwaarden 71
20.2 Licentieovereenkomst voor eindgebruikers 76
20.2 Gegevensverwerkingsovereenkomst 83
20.2 Modelcontractbepalingen 85
20.3 Privacybeleid 109

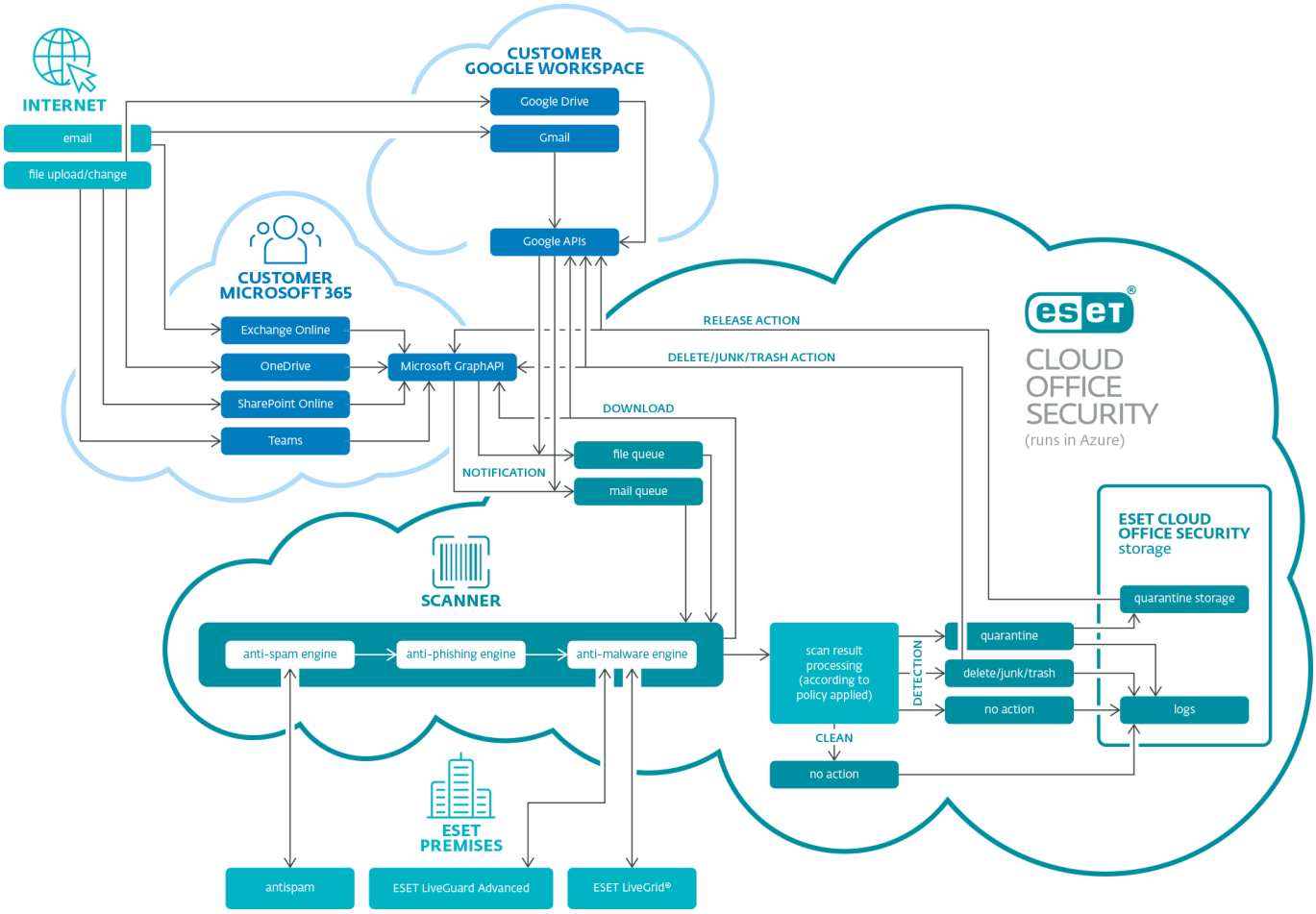
Overzicht

ESET Cloud Office Security is een multitenant en schaalbare cloudservice in Microsoft Azure. ESET Cloud Office Security wordt aangeboden als een Software-as-a-Service-product (SaaS) dat volledig in de cloud werkt zonder dat er hardware nodig is. Het is de ultieme combinatie van spamfiltering, anti-malwarescanning en anti-phishing. Het helpt uw bedrijfscommunicatie te beschermen tegen malware, minimaliseert de nadelige effecten van ongevraagde berichten op de dagelijkse productiviteit en helpt voorkomen dat binnenkomende externe e-mails worden gebruikt als kanaal voor gerichte aanvallen.

ESET Cloud Office Security-beveiligingsservices dekken de bekendste cloudplatformproviders en bieden uitgebreide e-mailbeveiliging met geavanceerde anti-malware-engines en ESET LiveGuard Advanced. Deze oplossing biedt geavanceerde bescherming tegen bedreigingen via cloud sandboxing, waarbij verdachte samples worden geanalyseerd in een geïsoleerde omgeving.

Dankzij de ESET Cloud Office Security-architectuur kunt u beveiliging snel initiëren door verbinding te maken met uw cloudplatform: Microsoft 365 of Google Workspace. U kunt de beveiliging beheren via een webconsole die overal toegankelijk is.

ESET Cloud Office Security biedt geavanceerde preventieve beveiliging om de Microsoft 365-apps van uw bedrijf te beschermen: Exchange Online, OneDrive, SharePoint Online en Teams. En dezelfde beveiliging wordt ook geboden voor uw Google Workspace-apps: Gmail en Google Drive.



ESET Cloud Office Security beveiligt OneDrive en Postvak van gelicentieerde gebruikers, evenals teamgroepen en SharePoint-sites. Elke store van deze Microsoft 365-toepassingen wordt beveiligd, ongeacht wie er een bestand heeft geüpload of wie er een e-mail heeft verzonden. De inhoud zelf wordt beschermd, ongeacht wie de maker ervan is. De maker kan ook een gastgebruiker zijn om de best mogelijke beveiliging te garanderen.

Belangrijke functies

In de volgende tabel staat een lijst met functies die beschikbaar zijn in ESET Cloud Office Security.

Multitenant	U kunt meerdere Microsoft 365- en Google Workspace-tenants beveiligen en beheren vanuit één ESET Cloud Office Security-console. Azure Active Directory (Azure AD) organiseert objecten zoals gebruikers en apps in groepen die tenants worden genoemd. Op basis van tenants kunt u beleid instellen voor gebruikers en apps binnen uw organisatie om te voldoen aan het beveiligingsbeleid en het operationele beleid.

Antispam	Antispam is een essentieel onderdeel van elke mailserver. ESET Cloud Office Security gebruikt de nieuwste antispam-engine die ongewenste e-mail en pogingen tot phishing zeer efficiënt tegenhoudt. ESET Cloud Office Security heeft opeenvolgende keren de spamfiltertest van Virus Bulletin gewonnen. Virus Bulletin is een autoriteit op het gebied van beveiligingstesten en heeft ons een aantal jaar op rij het certificaat VBSpam+ toegekend. De Antispam-engine filtert 99,99% van ongewenste e-mail met geen enkel vals-positief resultaat uit, wat de engine tot een toonaangevende spambeveiligingstechnologie maakt. ESET Cloud Office Security Antispam is op de cloud gebaseerd en de meeste cloud-databases bevinden zich in ESET-datacenters. Dankzij antispamdiensten in de cloud kan informatie snel worden geactualiseerd, waardoor sneller kan worden gereageerd op nieuwe spam.
Anti-phishing-beveiliging	Deze functie voorkomt dat gebruikers toegang krijgen tot webpagina's waarvan bekend is dat er phishing plaatsvindt. In e-mailberichten kunnen koppelingen zijn opgenomen die naar phishingwebpagina's verwijzen en ESET Cloud Office Security maakt gebruik van een geavanceerde parser die de berichttekst en het onderwerp van inkomende e-mailberichten doorzoekt om dergelijke koppelingen (URL's) te identificeren. De koppelingen worden vergeleken met een phishingdatabase die steeds wordt bijgewerkt.
Antimalwarebeveiliging	Deze bekroonde en innovatieve verdediging tegen malware is een toonaangevende technologie die aanvallen voorkomt. Deze technologie voorkomt aanvallen en maakt dankzij cloudgebaseerde scans een einde aan allerlei soorten bedreigingen, zoals virussen, ransomware, rootkits, wormen en spyware. Dankzij de cloudgebaseerde scans is de detectiesnelheid nog hoger. De kleine voetafdruk vergt weinig van de systeembronnen en doet geen afbreuk aan de prestaties. Bij antimalwaredetectie wordt gebruikgemaakt van een gelaagd beveiligingsmodel. Elke laag, of fase, heeft verschillende kerntechnologieën. Bij de fase voorafgaand aan uitvoering zijn de volgende technologieën betrokken: UEFI-scanner (Unified Extensible Firmware Interface), netwerkaanvalbeveiliging, reputatie & cache, In-product Sandbox en DNA-detecties ingezet. De technologieën die tijdens de uitvoeringsfase worden toegepast zijn Exploit blocker, Ransomware Shield, Geavanceerde geheugenscanner en Scriptscanner (AMSI). Bij de fase na uitvoering wordt gebruikgemaakt van Botnetbeveiliging, Cloud Malware Protection System en Sandboxing. De kerntechnologieën bevatten een rijke set functies en bieden een ongeëvenaard niveau van bescherming.
Beleid	Grotere organisaties hebben meestal meerdere afdelingen en willen verschillende beveiligingsinstellingen voor elke organisatie-eenheid configureren. ESET Cloud Office Security biedt beveiliging op basis van beleidsinstellingen die kunnen worden toegewezen aan geselecteerde Tenants, Gebruikers, Teamgroepen en SharePoint-sites. U kunt elk beleid aan uw behoeften aanpassen.
Quarantainebeheer	Inspecteer in quarantaine geplaatste objecten en voer een toepasselijke actie uit (downloaden, verwijderen of vrijgeven). Deze functie maakt eenvoudig beheer mogelijk van e-mailberichten, bijlagen en bestanden van Exchange Online/OneDrive/Teamgroepen/SharePoint-sites die door ESET Cloud Office Security in quarantaine zijn geplaatst. Downloaden geeft u de mogelijkheid om, indien nodig, in quarantaine geplaatste objecten te analyseren met hulpmiddelen van derden, waarmee u kunt bepalen welke actie u wilt ondernemen.

Dashboard met detectiestatistieken	Krijg een overzicht van de beveiligingsactiviteiten in Microsoft 365. Op het dashboard vindt u op elk van de overzichtstabbladen (Exchange Online/OneDrive/Teamgroepen/SharePoint-sites) onmisbare informatie. Op het overzichtstabblad Gebruiker staan het aantal tenants en het licentiegebruik, evenals statistieken per tenant: Aantal gebruikers, Belangrijkste ontvangers van spam/phishing/malware, Belangrijkste verdachte OneDrive-accounts, Belangrijkste verdachte teamgroepen en SharePoint-sites. U kunt een tijdsduur en een tenant kiezen en daarvoor de statistieken weergeven. Meer detectiestatistieken en -grafieken vindt u op de tabbladen Exchange Online, OneDrive, Teamgroepen en SharePoint-sites. Dit zijn statistieken zoals het aantal gescande e-mails en bestanden, en de hoeveelheid gedetecteerde spam/phishing/malware. De grafieken geven het verkeer weer voor elk detectietype: spam, malware en phishing.
Detecties met filteropties	Deze functie bevat alle records over detecties. In de records vindt u logs van elke detectie per e-mailscan op het tabblad Exchange Online en bestandsscan op de tabbladen OneDrive/Teamgroepen/SharePoint-sites. Zo kunt u filteren en snel vinden wat u zoekt dankzij aanvullende informatie over een specifieke detectie (bijvoorbeeld een naam van een infiltratie, bestandshash, enz.).
Gebruikers	De centrale entiteit die ESET Cloud Office Security beveiligt, is het gebruikersaccount. Vind nuttige informatie door de details van een gebruiker te openen, zoals Overzicht, Instellingen die zijn gedefinieerd door beleid, de lijst met beleidsregels die zijn toegewezen aan de gebruiker en Detecties voor Exchange Online en OneDrive. Deze functie is nuttig wanneer u detecties met betrekking tot een specifieke gebruiker wilt onderzoeken. U kunt ook kiezen welke gebruikers u wilt beveiligen. Gebruikers worden ingedeeld in groepen. Elke groep is een Microsoft 365-tenant met gebruikers. Met filters kunt u gemakkelijk op basis van meerdere criteria zoeken naar een bepaalde gebruiker binnen een groep.
Rapportage en beveiliging door zelflerende systemen	Geavanceerde zelflerende systemen maken nu als een geavanceerde beveiligingslaag onderdeel uit van de detectie-engine, wat detectie op basis van zelflerende systemen verbetert. Lees meer over dit type beveiliging in de woordenlijst. U kunt Rapportageniveaus configureren in de volgende categorieën: Malware, Potentieel ongewenste toepassingen, Potentieel verdachte toepassingen en Potentieel onveilige toepassingen.
Rapporten (statistische en E-mailquarantaine)	Ontvang statistische gegevens voor de beveiliging van Exchange Online, OneDrive, Teamgroepen en SharePoint-sites via e-mail of genereer en download een rapport voor een gekozen periode. U kunt rapporten plannen zodat er regelmatig rapporten worden gegenereerd en naar opgegeven e-mailontvangers worden verzonden. Kies PDF of CSV als uitvoerindeling. In rapporten vindt u gegevens zoals het aantal gescande e-mails, gedetecteerde malware, phishing en spam. Gegevens worden als grafieken in PDF-indeling weergegeven. Er is voor alles een grafiek: gescande e-mails, malwareverkeer, phishingverkeer en spamverkeer. Ook ziet u aparte statistieken voor degenen die de meeste malware, phishing en spam ontvangen. Er zijn verschillende opties om rapporten te genereren. Daarnaast kunt u een rapport van E-mailquarantaine (een lijst met e-mailberichten die in quarantaine staan) bij geselecteerde ontvangers laten bezorgen. Het rapport van E-mailquarantaine wordt op de opgegeven datum en het opgegeven tijdstip verzonden, maar alleen als er nieuwe items kunnen worden gemeld.
Teams en sites	ESET Cloud Office Security biedt beveiliging aan Teamgroepen en SharePoint-sites. De beveiliging van Microsoft 365-samenwerkingsoplossingen wordt verruimd doordat SharePoint en Teams worden beveiligd en bestanden veilig kunnen worden gedeeld. Als u een ESET Cloud Office Security hebt gebruikt, wordt u mogelijk gevraagd om toestemming bij te werken voordat u Team en sites gebruikt.

ESET LiveGuard Advanced	Een extra beveiligingslaag tegen geavanceerde zero-day bedreigingen. ESET LiveGuard Advanced is een sandboxing-oplossing in de cloud die ingediende bestanden analyseert door verdachte code in een geïsoleerde omgeving uit te voeren om het gedrag ervan te beoordelen. ESET Cloud Office Security dient verdachte e-mailbijlagen en bestanden van Exchange Online, OneDrive, Teamgroepen en SharePoint-sites in bij ESET LiveGuard Advanced om deze te laten analyseren. ESET LiveGuard Advanced-functie inschakelen en configureren met behulp van beleid. Resultaten van de analyse worden weergegeven in Scanlogboeken.
Controlelogboek	Met het Controlelogboek kan de beheerder de activiteiten inspecteren die in de ESET Cloud Office Security worden uitgevoerd. Deze functie kan handig zijn, vooral als u meerdere ESET Cloud Office Security-consolegebruikers hebt. De records in controlelogboeken zijn bewijs van de activiteiten en tonen de volgorde waarin deze activiteiten plaatsvonden. In controlelogboeken wordt informatie over de specifieke bewerking of gebeurtenis geregistreerd. Controlelogboeken worden gemaakt wanneer een ESET Cloud Office Security-object (licentiepool, gebruiker, beleid, rapport, quarantaine-item zoals een bijlage) wordt gemaakt of gewijzigd.
Google Workspace (Gmail- en Google Drive-beveiliging)	ESET Cloud Office Security breidt de dekking van de beveiligingsservices uit naar een andere toonaangevende cloud-e-mailprovider: Google Workspace. ESET Cloud Office Security biedt uitgebreide beveiliging met volledige functionaliteit voor gebruikers van Gmail en Google Drive. Hiermee worden Google Workspace-gebruikers beveiligd tegen malware, phishing en spam.

Nieuwe functies

Informatie over nieuwe functies en verbeteringen die in elke versie zijn ESET Cloud Office Security geïmplementeerd:

Portalversie 353 uitgebracht op 23 November 2023

- Google Workspace-integratie toegevoegd.
- Productnavigator om snel toegang te krijgen tot ESET Business Account (meer consoles volgen in de komende maanden).
- *Andere bugfixes en verbeteringen van de backend.*

Portalversie 342.3 uitgebracht op 24 oktober 2023

- Verificatie van Google Workspace-beheerdersaccount toegevoegd.
- Kolom Gebruikerstype toegevoegd.
- *Andere bugfixes en verbeteringen van de backend.*

Portalversie 311.2 uitgebracht op 31 juli 2023

- Google Workspace toegevoegd (Gmail- en Google Drive-beveiliging) – open de preview-functies via Snelle koppelingen.
- Thema donkere modus toegevoegd.
- Productnavigator toegevoegd voor ESET HUB Early Access-gebruikers.
- *Andere bugfixes en verbeteringen van de backend.*

Portalversie 293.7 uitgebracht op 13 juli 2023

- Tenant-koppeling toegevoegd aan ESET Business Account (EBA)-sites. Deze wijziging zorgt voor compatibiliteit met de toekomstige klantenportal ESET PROTECT HUB, die in plaats komt van ESET MSP Administrator (EMA) en ESET Business Account (EBA). Dit is slechts van toepassing voor enkele klanten die licenties van meerdere sites gebruiken om één tenant te beveiligen. Als dit het geval is, wordt u gevraagd uw tenants te koppelen aan EBA-sites.
- Andere kleine verbeteringen en bugfixes.

Portalversie 251.1 uitgebracht op 21 maart 2023

- Verbeteringen in vertraagd laden van schermen om tenants met tienduizenden gebruikers beter te ondersteunen.
- Wijzigingen in de wizard Tenant toevoegen
- Updates op de pagina Info.
- Updates van de gebruiksvoorwaarden en het privacybeleid (Beperkingen en beleid voor gegevensretentie).

Portalversie 205 uitgebracht op 9 November 2022

- Er is een venster Nieuwe functies toegevoegd. Wanneer u zich voor het eerst aanmeldt bij de ESET Cloud Office Security-console, wordt dit venster weergegeven, met een beschrijving van de nieuwe functies.
- Optie om scanlogboeken en het controlelogboek te exporteren naar een CSV-bestand.
- Een nieuwe instelling toegevoegd voor het samenvoegen van beleid met lijsten en e-mails met meldingen.

Portalversie 180.2 uitgebracht op 27 juli 2022

- De nieuwe functie Controlelogboek.
- Het gedeelte Logboeken wijzigen in Scanlogboeken.

Portalversie 156.2 uitgebracht op 26 april 2022

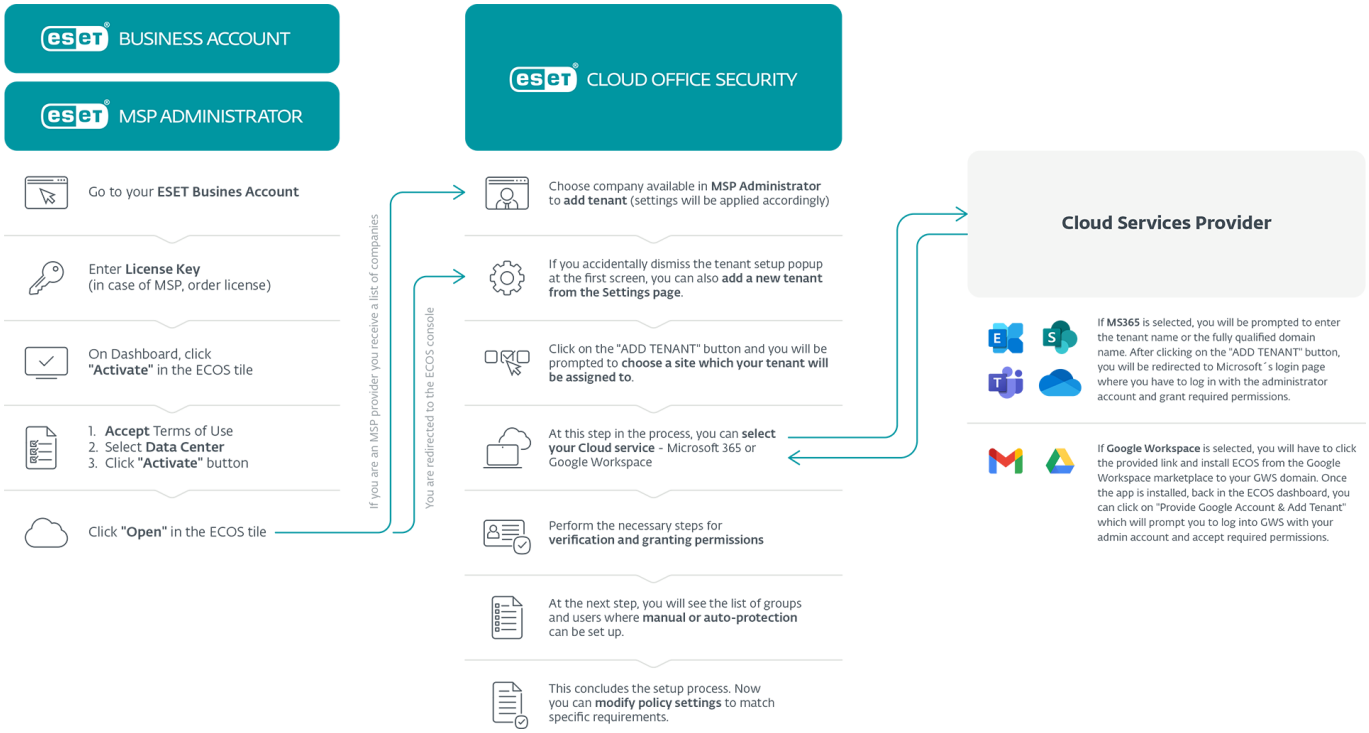
- Dynamic Threat Defense heet nu ESET LiveGuard Advanced.
- Ter analyse verzenden van vals-positieve/vals-negatieve samples.
- Lijsten met goedgekeurde, geblokkeerde en genegeerde lijsten importeren/exporteren in beleid.
- Dashboard toont het aantal onbeveiligde gebruikers op het tabblad Overzicht.
- Bug opgelost die e-mails met meldingen in quarantaine plaatste.

Portalversie 140.6 uitgebracht op 9 februari 2022

- Mogelijkheid om rapporten van een white label te voorzien (alleen co-branding of aangepast logo).
- Optie om de voorkeurstaal voor e-mails met meldingen te definiëren (meldingen voor postvakeigenaren).
- Optie om de voorkeurstaal voor e-mailmeldingen te definiëren voor tenantleden.
- E-mails filteren op bericht-id.

Integratie

De workflow van ESET Cloud Office Security-integratie met uw cloudserviceprovider:



Specificaties

Technische specificaties voor ESET Cloud Office Security (ter referentie):

- Vereisten
- Ondersteunde Microsoft 365-abonnementen
- Ondersteunde Google Workspace-abonnementen
- Ondersteunde webbrowsers
- Beperkingen en beleid voor gegevensretentie

Vereisten

Als u wilt profiteren van de ESET Cloud Office Security-service die Microsoft 365 beveiligt, is het volgende vereist:

- Ondersteund Microsoft 365-abonnement
- Beheerderstoegang tot Azure Active Directory (Azure AD)
- Azure Cloud Services – Exchange | OneDrive

- Een account in de ESET Business Account-portal of ESET MSP Administrator-portal

Ondersteunde Microsoft 365-abonnementen

ESET Cloud Office Security ondersteunt de volgende Microsoft 365-, Exchange Online- en OneDrive-abonnementen.

Microsoft 365-abonnementen voor grote ondernemingen:

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Office 365 E1
- Office 365 E3
- Office 365 E5
- Office 365 F3

Microsoft 365-abonnementen voor bedrijven:

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Microsoft 365-abonnementen voor onderwijsinstellingen:

- Microsoft 365 A3
- Microsoft 365 A5

Exchange Online-plannen:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

OneDrive-plannen:

- OneDrive for Business (Plan 1)

- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Ondersteunde Google Workspace-abonnementen

ESET Cloud Office Security ondersteunt de volgende Google Workspace-abonnementen.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Ondersteunde webbrowsers

> Voor de beste ervaring met ESET Cloud Office Security, raden wij aan uw webbrowsers up-to-date te houden.

U kunt de ESET Cloud Office Security-console met de volgende webbrowsers gebruiken:

- Mozilla Firefox 69 en nieuwer
- Microsoft Edge 44 en nieuwer
- Google Chrome 77 en nieuwer
- Opera 63 en nieuwer
- Safari 13.x en nieuwer

> Microsoft Internet Explorer wordt niet ondersteund.

Beperkingen en beleid voor gegevensretentie

In bepaalde omstandigheden zijn er ESET Cloud Office Security-scanbeperkingen. Een bestand wordt niet gescand en wordt in Scanlogboeken weergegeven als **Niet gescand** in de volgende gevallen:

- De bestandsgrootte is meer dan 200 MB
- De scan duurt langer dan 2 minuten en er treedt een time-out op.
- Het archiefbestand heeft een nestingsniveau van 10 of meer (doorgaans een bestand dat een archiefbom of zipbom wordt genoemd)

- Het archiefbestand is beveiligd met een wachtwoord
- Het bestand is beschadigd

Quarantainelimieten (wanneer vrijgegeven uit quarantaine):

- 15 MB voor één e-mailbijlage
- 150 MB voor het gehele e-mailbericht, met inbegrip van bijlagen

Beleid voor gegevensretentie:

Entiteit	Retentieperiode	Opmerking
In quarantaine geplaatste objecten	30 dagen	Objecten ouder dan 30 dagen worden definitief verwijderd.
Detecties	90 dagen	Records ouder dan 90 dagen worden definitief verwijderd.
Scanlogboekrecords	90 dagen	Records ouder dan 90 dagen worden definitief verwijderd.
Scanlogboekrecords met schoon scanresultaat	3 dagen	Als u een beleid hebt dat gebruikmaakt van Alle objecten in logbestand registreren, worden schone scanresultaten ouder dan 3 dagen permanent verwijderd.
ESET Cloud Office Security-database-back-up	90 dagen	Back-ups ouder dan 90 dagen worden definitief verwijderd.
Controlelogboeken	90 dagen	Records ouder dan 90 dagen worden definitief verwijderd.
Application Insights-logboeken	90 dagen	Records ouder dan 90 dagen worden definitief verwijderd.

Tenant verwijderd uit ESET Cloud Office Security-console

Wanneer u een tenant uit de ESET Cloud Office Security-console verwijdert, is de retentieperiode voor tenantgegevens 30 dagen (quarantaine, scanlogboeken en statistieken worden na 30 dagen verwijderd). Als u de tenant binnen 30 dagen opnieuw toevoegt, worden alle gegevens hersteld. Andere objecten (tenants, gebruikers, groepen, sites, rapporten, beleidsregels) worden na 90 dagen permanent verwijderd.

ESET Cloud Office Security gedeactiveerd in ESET Business Account of ESET MSP Administrator

Bij deactivering van ESET Cloud Office Security in ESET Business Account of ESET MSP Administrator worden ook de tenants verwijderd uit ESET Cloud Office Security. Het verwijderen van ESET Cloud Office Security is permanent en verwijderde gegevens kunnen niet worden hersteld.

Anti-spamscan:

E-mailberichten die zijn opgeslagen in postvakken, worden door ESET Cloud Office Security gescand op spam. Daarom kan ESET Cloud Office Security niet voorkomen dat een gebruiker een spam-bericht verzendt naar een extern e-mailadres. In een onwaarschijnlijk scenario, wanneer Office 365-gebruikersreferenties zijn gestolen, kunnen de referenties door een spammer worden gebruikt om spam-berichten in bulk te verzenden (uitgaand e-mailverkeer).

Licenties voor ESET Cloud Office Security

Beheer ESET Cloud Office Security-licenties in ESET Business Account of ESET MSP Administrator. Probeer ESET Cloud Office Security uit met een proeflicentie van 30 dagen.

- Zie ESET Business Account voor informatie over hoe u een account kunt maken of een licentie kunt toevoegen of beheren.
- Zie ESET MSP Administrator als u een MSP bent.

ESET Business Account en ESET MSP Administrator (hybride licentieaccount)

Als u hetzelfde e-mailadres hebt geregistreerd in zowel ESET MSP Administrator als ESET Business Account (eenmalige aanmelding), kunt u schakelen tussen de ESET Business Account- en de ESET MSP Administrator-weergave. Beveilig gebruikers of bedrijven die Licentiebeheer gebruiken voor ESET Cloud Office Security.

Respijtperiode voor aflopende licentie in ESET Business Account

Wanneer uw licentie bijna is afgelopen, wordt er een waarschuwing weergegeven in de ESET Business Account-interface. Als de vervaldatum voorbij is en u uw licentie niet hebt verlengd of een nieuwe licentie hebt geactiveerd, wordt de waarschuwing over de verlopen licentie weergegeven in ESET Business Account. Als er geen in aanmerking komende licentie is, wordt er een melding in ESET Business Account weergegeven dat uw licentie binnen 14 dagen wordt opgeschort en ontvangt u een e-mail op het adres dat in uw beheerdersaccount is opgegeven.

U hebt een respijtperiode van 14 dagen om uw licentie te verlengen nadat deze is verlopen. U wordt halverwege de respijtperiode nog een keer in ESET Business Account en per e-mail geïnformeerd. Na 14 dagen wordt uw ESET Cloud Office Security opgeschort. Het account wordt ontoegankelijk en is niet langer functioneel. Een opgeschort ESET Cloud Office Security-account wordt gearchiveerd en kan opnieuw worden geopend door een nieuwe ESET Cloud Office Security-licentie toe te voegen aan ESET Business Account. Uw ESET Cloud Office Security-account kan gedurende maximaal 30 dagen 'opgeschort' blijven. Daarna wordt het account definitief verwijderd.

Als uw account de opgeschorte status heeft, ontvangt u een melding in ESET Business Account en per e-mail wanneer er nog 14 dagen over zijn voordat uw account wordt verwijderd. U moet een nieuwe ESET Cloud Office Security-licentie activeren om de toegang tot uw ESET Cloud Office Security-account te herstellen.

> Gebruikers blijven volledig beveiligd tijdens de respijtperiode. Wanneer de respijtperiode voorbij is, zijn de gebruikers niet meer beschermd.

Geschorste licentie

Als er geen geldige ESET Cloud Office Security-licentie aanwezig is in ESET Business Account, wordt uw ESET Cloud Office Security-exemplaar opgeschort. Het exemplaar wordt ontoegankelijk en niet-functioneel. Uw ESET Cloud Office Security-exemplaar kan gedurende maximaal 30 dagen 'opgeschort' blijven. Daarna wordt het definitief verwijderd. U moet een nieuwe ESET Cloud Office Security-licentie activeren om de toegang tot uw ESET Cloud Office Security-exemplaar te herstellen.

ESET Business Account

ESET Business Account werkt als een uniform toegangspunt voor ESET Business Account en ESET Cloud Office Security. Gebruik de ESET Cloud Office Security- of ESET Business Account-aanmeldingspagina om toegang te krijgen tot ESET Cloud Office Security. Beide pagina's leiden u door ESET Business Account-verificatie heen om uw aanmelding te verifiëren.

- Maak een nieuw account als u geen geregistreerd account hebt in ESET Business Account.
- Als u een ESET Business Account-account hebt, kunt u uw ESET Cloud Office Security-licentie toevoegen.
- Beheren ESET Business Account.

Een nieuw ESET Business Account-account maken

1. Open de aanmeldingspagina voor ESET Business Account en klik op **Registreer u gratis**. Vul het formulier zorgvuldig in om u te registreren. Het ingevoerde e-mailadres wordt als uw aanmeldingsnaam gebruikt.

2. Het wachtwoord moet uit ten minste 10 tekens bestaan. Vul uw **Naam** en **Bedrijfsgegevens** in en klik op **Doorgaan**. Lees de **ESET-gebruiksvoorwaarden** en bevestig dat u hiermee akkoord gaat. Vul het reCAPTCHA-formulier in en klik op **Registreren**.

3. U ontvangt een bevestigingsmail nadat u zich hebt geregistreerd (dit kan tot 15 minuten duren). Klik op de koppeling in de bevestigingsmail om het nieuwe venster **Account activeren** te openen.

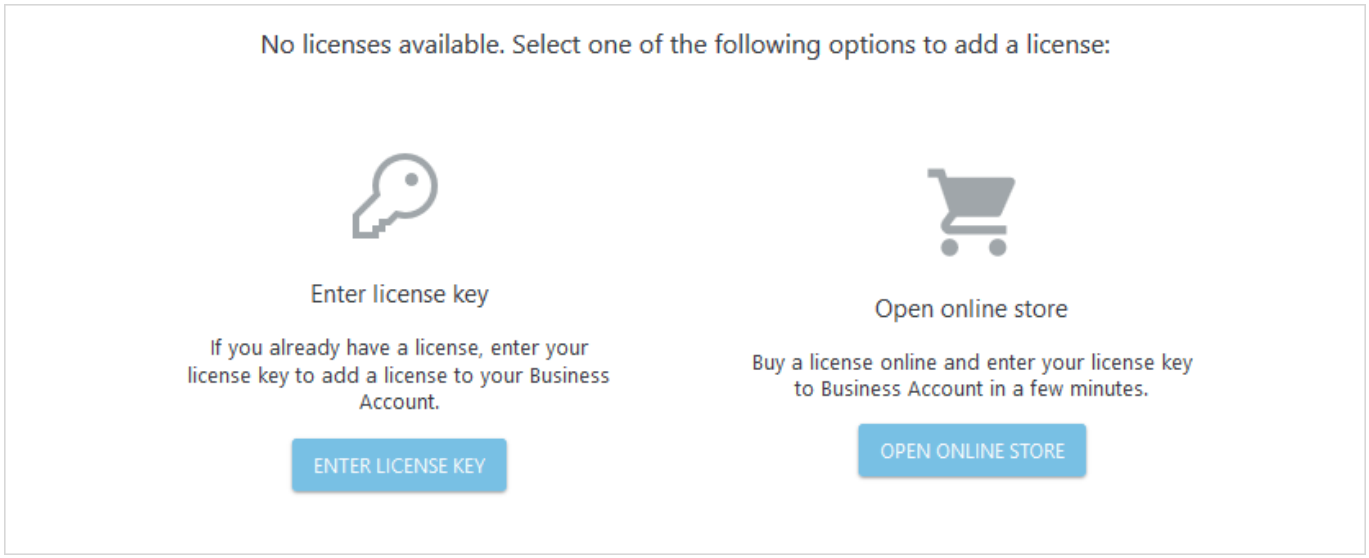
4. Voer uw wachtwoord in en klik op **Activeren** om uw ESET Business Account-account te activeren. U ontvangt nog een e-mail waarin wordt bevestigd dat uw ESET Business Account-account is gemaakt. U bent nu klaar om in te loggen bij ESET Business Account.

Wanneer u ESET Business Account hebt geactiveerd, kunt u uw ESET Cloud Office Security-licentie toevoegen.

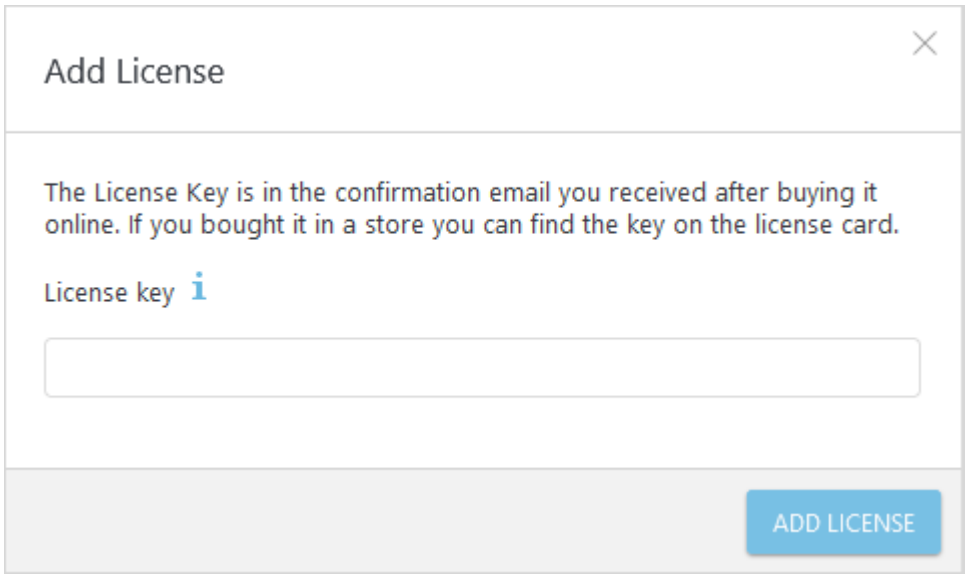
ESET Cloud Office Security-licentie toevoegen aan ESET Business Account

Na een succesvolle aanmelding bij ESET Business Account ziet u een welkomstscherm voor ESET Business Account als u dit de eerste keer gebruikt.

1. Klik op **Licentie toevoegen** om het licentievenster te openen. Als u een reguliere ESET Business Account-gebruiker bent, gaat u naar het tabblad **Licentie** en klikt u op **Licentie toevoegen**.



2. Voer uw **Licentiecode** in en klik op **Licentie toevoegen**.



3. U ontvangt een e-mail met een verificatiekoppeling. Klik op de koppeling en voer uw aanmeldingsgegevens voor de ESET Business Account-portal in wanneer daarom wordt gevraagd. Zie ESET Business Account-gids voor meer informatie over licentiebeheer, gebruikers en sites.

Beheren ESET Business Account

Algemene activiteiten voor licenties:

Sites en licentiepool

De licenties en licentiepools worden vanuit ESET Business Account geladen. Licentiepools zijn alleen beschikbaar als u bestaande sites in ESET Business Account hebt.

Een nieuwe gebruiker maken in ESET Business Account

U kunt een gebruiker maken die u helpt een deel van uw licenties te beheren.

1. Open ESET Business Account en meld u aan.

2. Selecteer **Gebruikersbeheer**, klik op **Nieuwe gebruiker** en typ de vereiste gegevens.

3. Selecteer ESET Cloud Office Security **Toegangsrechten** voor een gebruiker:

   • **Lezen** — Gebruiker heeft toegang tot ESET Cloud Office Security, ziet gebruikers, logboeken en detecties, maar kan geen beleid beheren, gebruikers beveiligen of berichten uit quarantaine vrijgeven.

   • **Schrijven** — Gebruiker heeft volledige toegang tot ESET Cloud Office Security, ziet en beheert gebruikers, quarantaine en kan beleid maken.

   • **Geen toegang** — Gebruiker heeft geen toegang tot ESET Cloud Office Security

4. Stel een taal in bij **Voorkeuren** voor de ESET Cloud Office Security-console.

5. Klik op **Maken** om de gebruiker te definiëren.

Een nieuwe site maken in ESET Business Account

Dankzij sites kunt u uw licenties opsplitsen of samenvoegen tot licentiepools. Sites zijn individuele groepen die hun eigen locatie en beheerders kunnen hebben.

1. Open ESET Business Account en meld u aan.

2. Selecteer **Details**, klik op **Site maken** en typ de vereiste persoonlijke gegevens.

3. Klik op **Gebruiker toevoegen**, selecteer gebruiker en klik op **Bevestigen**.

4. Klik in de licentiepool op **Eenheden toevoegen** en selecteer de ESET Cloud Office Security-licentie. U kunt **Subeenheden** wijzigen en op **Bevestigen**klikken.

5. Klik op **Maken** om de site te definiëren.

ESET MSP Administrator

ESET MSP Administrator is een licentiebeheersysteem waarmee MSP-gebruikers meerdere MSP-klanten kunnen definiëren en specifieke licenties met een aantal seats kunnen genereren. De ESET MSP Administrator-licentieportal ondersteunt volumeprijzen en facturering op basis van een exact aantal gekochte seat-dagen.

ESET Cloud Office Security is beschikbaar voor alle MSP Managers, MSPs en managed MSPs. Een ESET MSP Administrator-gebruiker met schrijftoegang komt in aanmerking om ESET Cloud Office Security om te activeren. ESET Cloud Office Security kan worden benaderd door gebruikers met schrijf-, lees- of aangepaste toegangsrechten.

• Een nieuwe MSP-klant maken (Het e-mailadres van de klant is vereist voor activering van de ESET Cloud Office Security-console).

• Activeren ESET Cloud Office Security vanuit ESET MSP Administrator

Activeren ESET Cloud Office Security

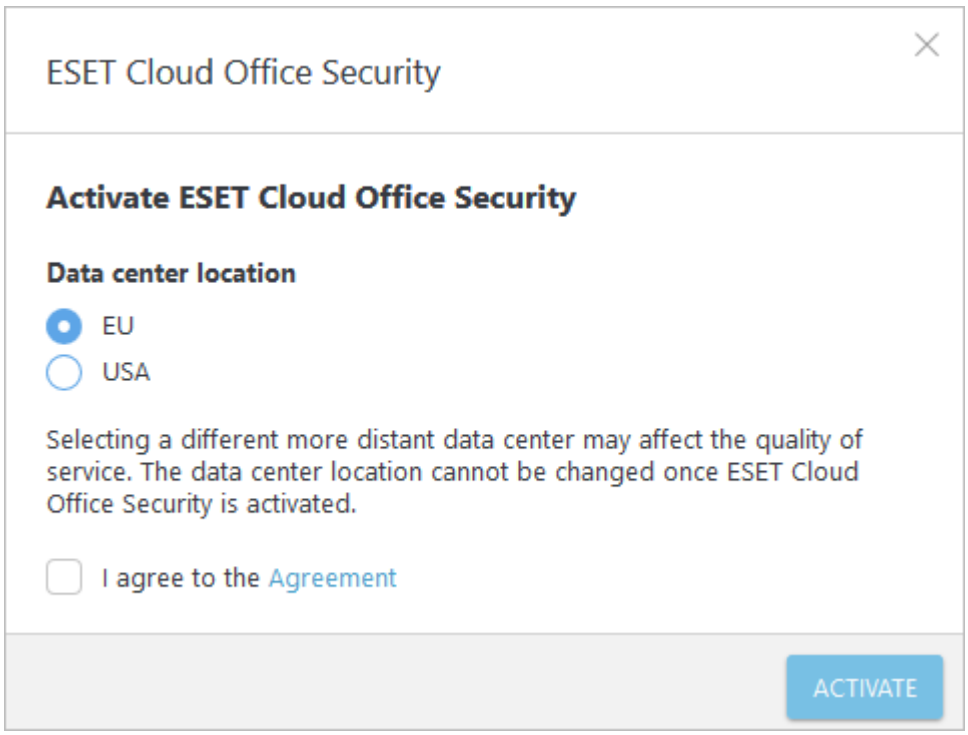
1. Log in bij ESET Business Account of zoek de tegel in ESET MSP Administrator in het ESET Cloud Office Security-**dashboard**.

2. Klik op **Activeren** in de rechterbenedenhoek van de ESET Cloud Office Security-tegel.

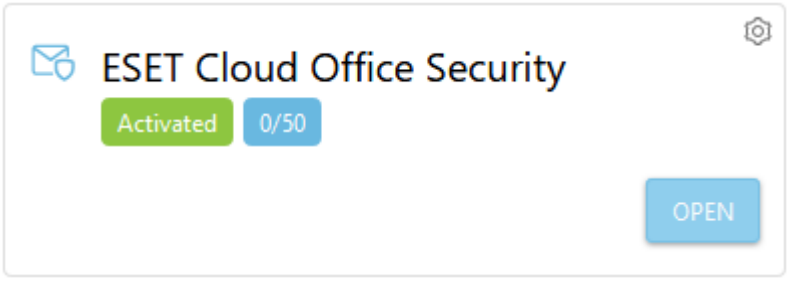


3. De activeringswizard verwijst naar de ESET Cloud Office Security-gebruiksvoorwaarden en geeft de optimale locatie van het datacenter weer op basis van uw huidige locatie. Selecteer **Ik ga akkoord met de gebruiksvoorwaarden** en klik op **Activeren**. We raden af de locatie van het datacenter te wijzigen. Als u echter een andere locatie wilt gebruiken, kunt u uw keuze maken.

> Datacenters zijn volledig van elkaar gescheiden. Zodra u de locatie van het datacenter hebt geselecteerd, kan deze niet meer worden gewijzigd en u kunt niet naar een andere locatie migreren. Als u het datacenter wilt wijzigen, moet u het activeringsproces opnieuw vanaf het begin af aan starten.

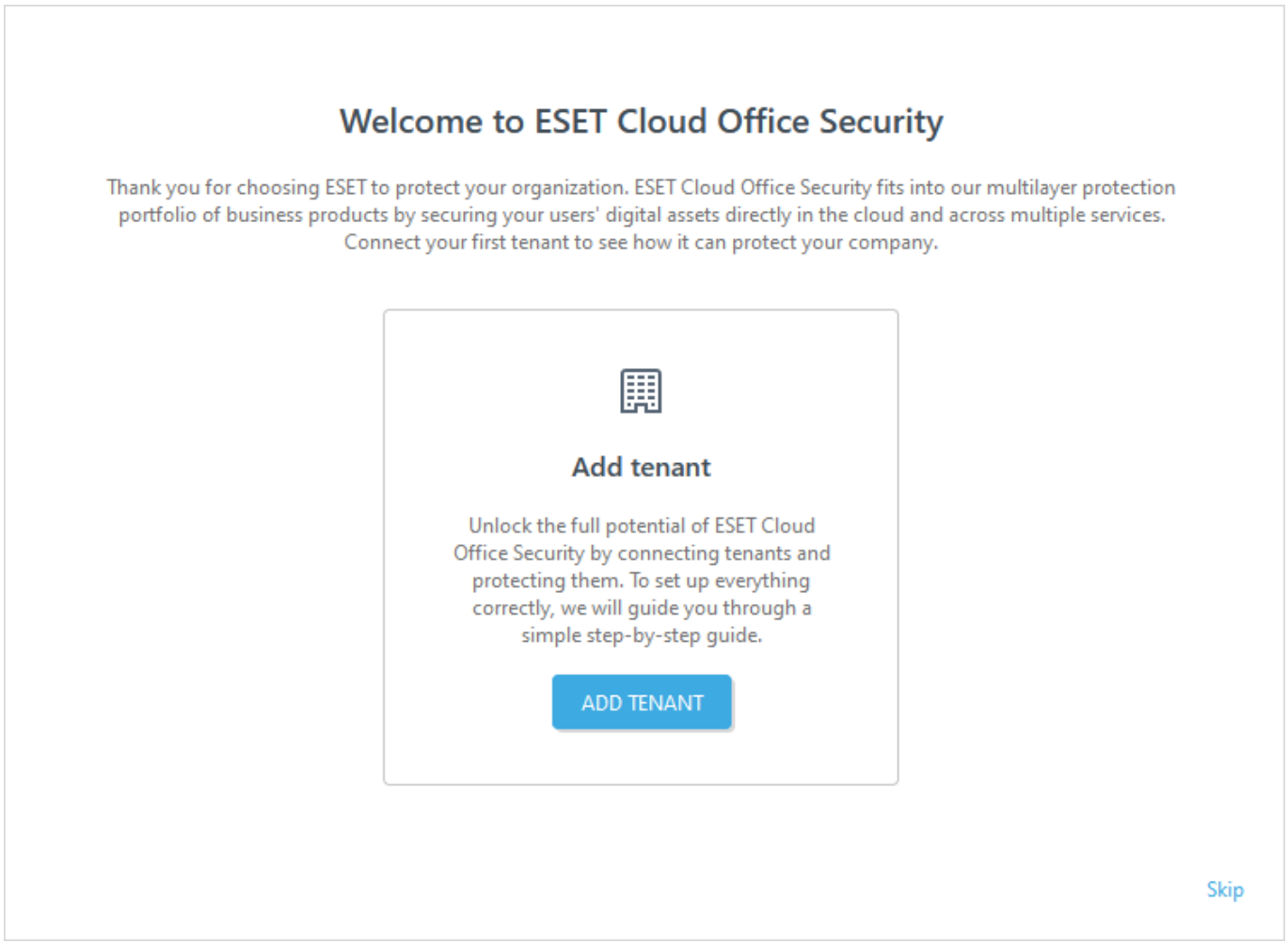


4. Klik op **Openen** in de ESET Cloud Office Security-tegel. ESET Cloud Office Security Dashboard wordt geopend in een nieuw browsertabblad.

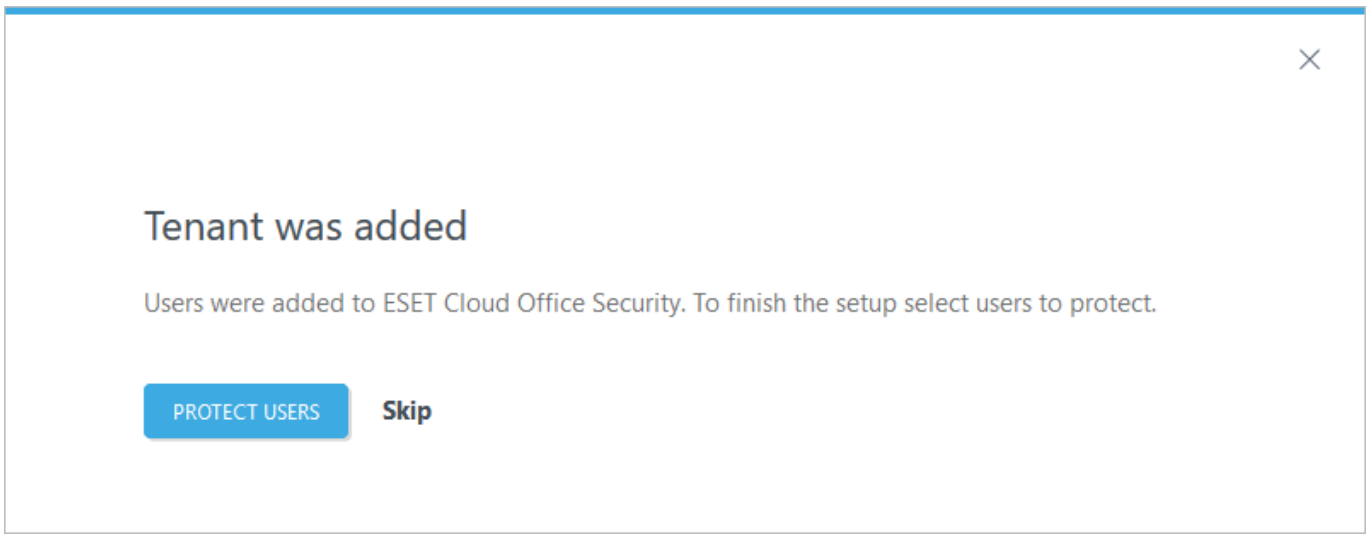


Wanneer u zich voor de eerste keer aanmeldt bij ESET Cloud Office Security, wordt de **wizard Opstarten** weergegeven. Met deze wizard doorloopt u het eerste implementatieproces.

1. Voeg uw tenant toe (Microsoft 365 of Google Workspace).



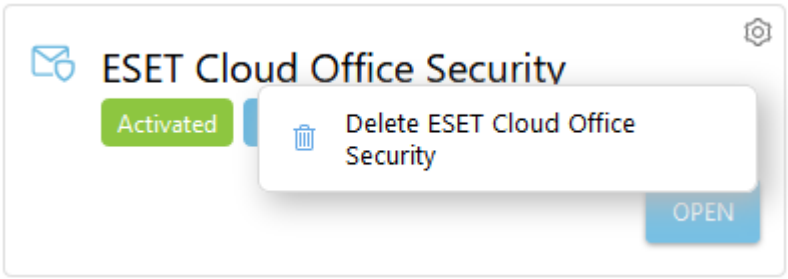
2. Gebruikers beveiligen. Als u **overslaat**, kunt u gebruikers of bedrijven later beveiligen met Licentiebeheer voor ESET Cloud Office Security.



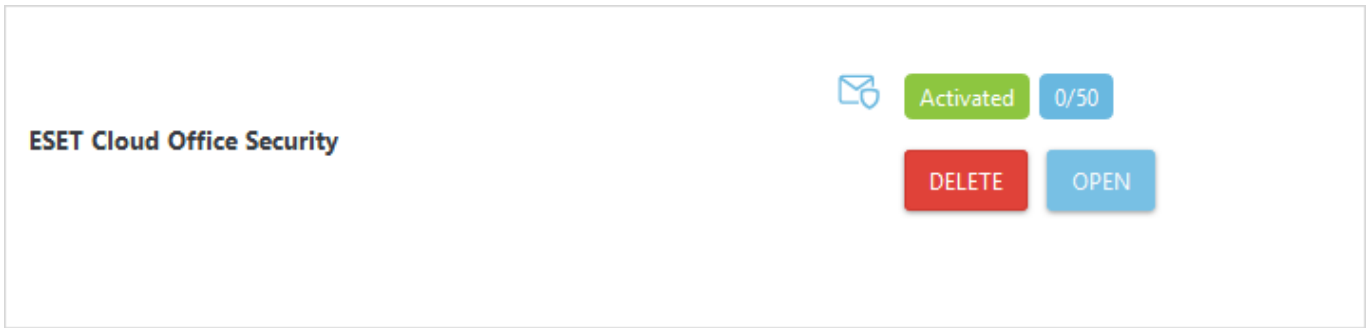
Deactiveren ESET Cloud Office Security

1. Log in bij ESET Business Account of zoek de tegel in ESET MSP Administrator in het ESET Cloud Office Security-**dashboard**.

2. Klik op het tandwielpictogram in de rechterbovenhoek van de ESET Cloud Office Security-tegel en selecteer **ESET Cloud Office Security verwijderen**.

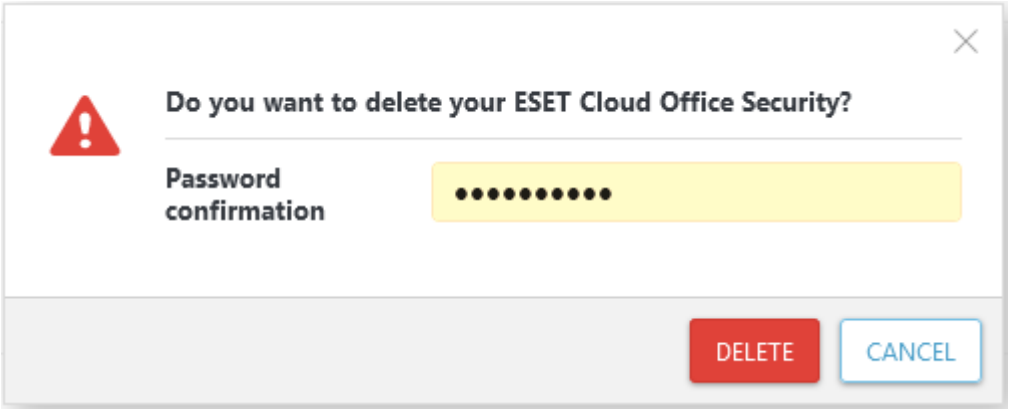


3. Of navigeer naar het gedeelte **Details** en klik op **Verwijderen**.



4. Er wordt een waarschuwingsvenster weergegeven waarin u wordt gewaarschuwd dat alle gegevens op het punt staan te worden verwijderd. Voer ter bevestiging uw ESET Business Account-wachtwoord in en klik op **Verwijderen**.

Verwijdering van ESET Cloud Office Security is permanent. Verwijderde gegevens kunnen niet worden hersteld.



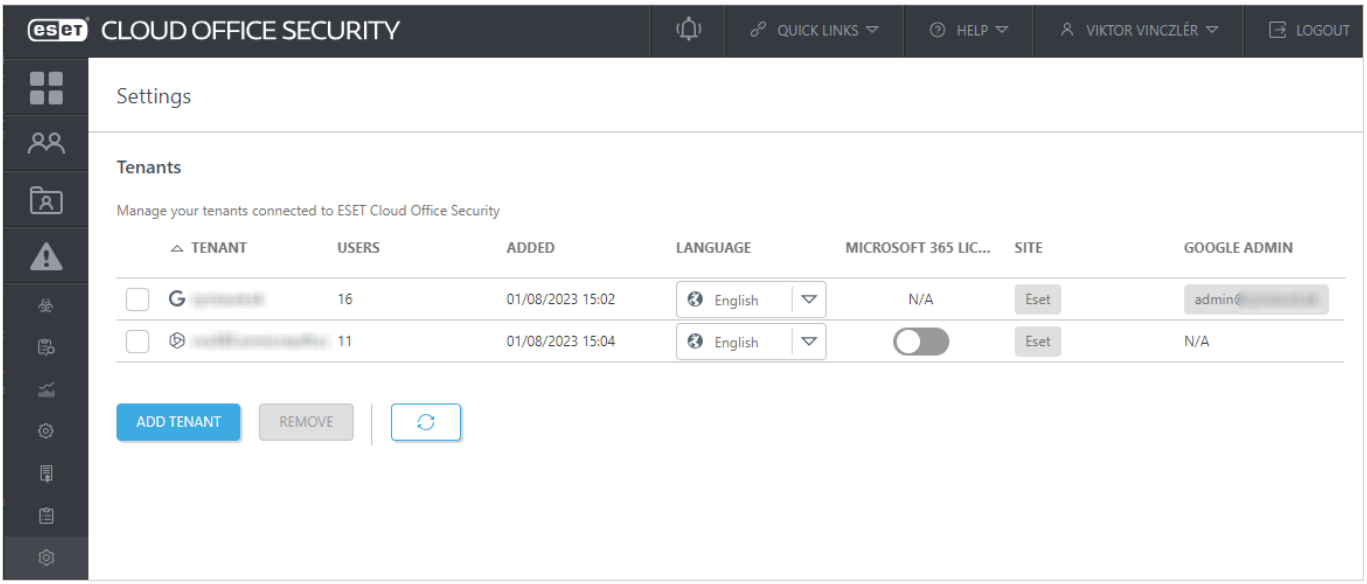
Het ESET Cloud Office Security-exemplaar wordt nu verwijderd en de ESET Cloud Office Security-producttegel krijgt opnieuw de status **Niet geactiveerd**. U ontvangt ook een bevestigingsmail van ESET Business Account.

Uw tenants beheren in Instellingen

Tenants beheren die zijn verbonden met ESET Cloud Office Security. U kunt alle geregistreerde tenants in de tabel zien met details voor elke tenant. Gebruik de knop Vernieuwen om de tabel opnieuw met tenants te laden.

Als u een nieuwe tenant wilt toevoegen, klikt u op Tenant toevoegen en kiest u Microsoft 365 of Google Workspace, afhankelijk van het cloudplatform dat u wilt beveiligen. Nadat u het registratieproces voor tenants hebt voltooid, is uw Microsoft 365 of Google Workspace beveiligd door ESET Cloud Office Security.

Nadat u de tenant hebt toegevoegd, verandert het scherm en wordt de lijst met tenants weergegeven die aan een site zijn gekoppeld. Hier kunt u uw bestaande tenant beheren of meer tenants toevoegen. De tabel bevat de naam van de tenant, het aantal gebruikers, wanneer de tenant is toegevoegd, de taalinstelling, gebruikers met een Microsoft 365-licentie, de sitenaam en de Google-beheerder.



Taal

Deze instelling bepaalt de taal van e-mailberichten aan tenantleden. U kunt de taal voor elke tenant afzonderlijk definiëren, bijvoorbeeld in het geval van een MSP die meerdere bedrijven beheert.

Als u een tenant wilt verwijderen uit ESET Cloud Office Security, selecteert u de desbetreffende tenant en klikt u op Verwijderen. Er wordt een bevestigingsvenster weergegeven waarin u een definitieve beslissing kunt nemen.

Na verwijdering worden alle gebruikersgegevens na 30 dagen verwijderd.

Gelicentieerde gebruikers van Microsoft 365

Deze optie is standaard ingeschakeld. Dit komt overeen met een lijst met gebruikers in Microsoft 365-beheercentrum onder **Gebruikers** > **Actieve gebruikers** > Filter: **Gelicentieerde gebruikers**.

Als u deze optie uitschakelt, geeft ESET Cloud Office Security alle gebruikers weer, ook gebruikers zonder Microsoft 365-licentie (bijvoorbeeld gedeelde postvakken). Als u automatische beveiliging gebruikt voor groep- of tenantgebruikers zonder Microsoft 365-licentie, worden deze gebruikers zichtbaar, beveiligd en maken ze gebruik van ESET Cloud Office Security-licentie-eenheden. De beveiligingsstatus van nieuw zichtbare gebruikers kan maximaal 1 uur **In behandeling** zijn. Zodra het proces voor automatische beveiliging is voltooid, wordt de beveiligingsstatus gewijzigd in **Beveiligd** of een andere mogelijke status in het gedeelte Gebruikers.

> Als zich in uw tenant of groep met automatische beveiliging een gebruiker zonder postvak en OneDrive bevindt, wordt voor deze gebruiker een ESET Cloud Office Security-licentie-eenheid gebruikt. U ziet een **waarschuwing** over de beveiligingsstatus voor deze gebruiker.

Wanneer u Gelicentieerde gebruikers van Microsoft 365 opnieuw inschakelt, worden alleen nog gebruikers met een Microsoft 365-licentie weergegeven. Als u automatisch beveiligde gebruikers zonder Microsoft 365-licentie had, verdwijnen deze gebruikers uit het gedeelte Gebruikers en worden er ESET Cloud Office Security-licentie-eenheden vrijgemaakt. Het kan tot 1 uur duren voordat de wijziging plaatsvindt.

> Als u handmatig beveiligde gebruikers zonder Office 365-licentie hebt (terwijl de instelling **Gelicentieerde gebruikers van Microsoft 365** is ingeschakeld), blijven deze gebruikers zichtbaar en beveiligd, zelfs nadat u **Gelicentieerde gebruikers van Microsoft 365** hebt ingeschakeld (tot de gebruikers niet meer beveiligd zijn).

Site

Als u de site wilt wijzigen waaraan de tenant is gekoppeld, klikt u op de sitenaam: het venster **Selecteer een site om te beveiligen** wordt geopend en hier kunt u de nodige wijzigingen aanbrengen.

Google-beheerder

De Google-beheerder moet een actief e-mailadres zijn van uw Google Workspace-beheerder.

> Als de rol of het e-mailadres van de beheerder gaat veranderen, klikt u op de Google-beheerder en werkt u de gegevens bij. Doe dit van tevoren om te waarborgen dat de functionaliteit van de tenant en de beveiliging van uw site gehandhaafd blijven.

Toestemming bijwerken

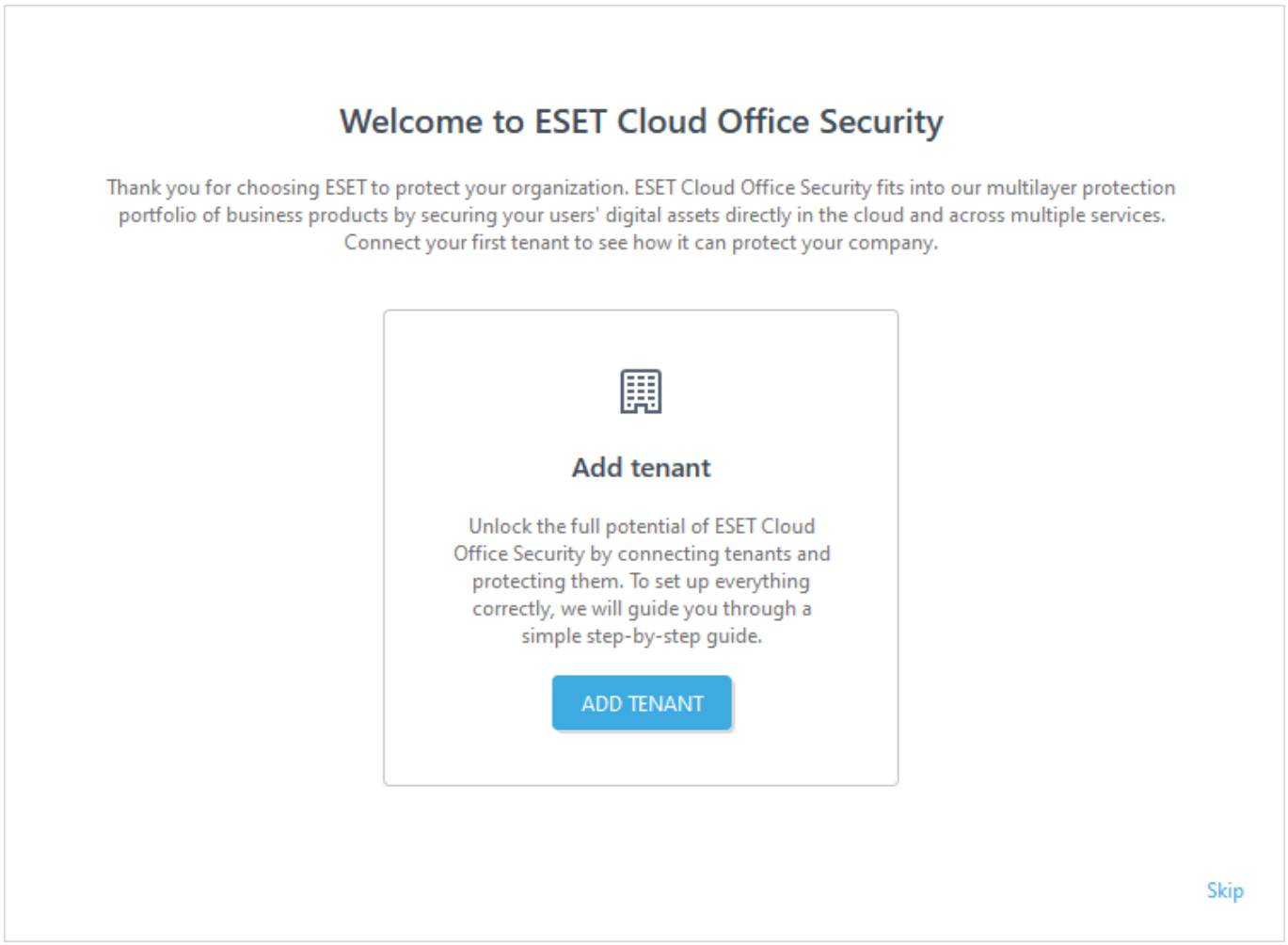
Als er een gele knop wordt weergegeven, kunt u uw toestemming bijwerken. Als u de toestemming voor een bestaande tenant bijwerkt, worden de ESET Cloud Office Security-machtigingen uitgebreid naar uw Microsoft 365-account, waardoor een functie wordt ingeschakeld die informatie biedt over het gebruikerstype. Het gebruikerstype wordt gedefinieerd in Azure Active Directory en wordt weergegeven in een speciale kolom in het gedeelte Gebruikers. U kunt bijvoorbeeld Microsoft 365-gebruikers filteren op basis van hun type als u alleen gedeelde postvakken wilt weergeven.

Klik op de knop **Bijwerken** voor elke tenant waarvoor u deze functie wilt inschakelen. Het kan tot 24 uur duren om het gebruikerstype van uw Azure AD bij te werken.

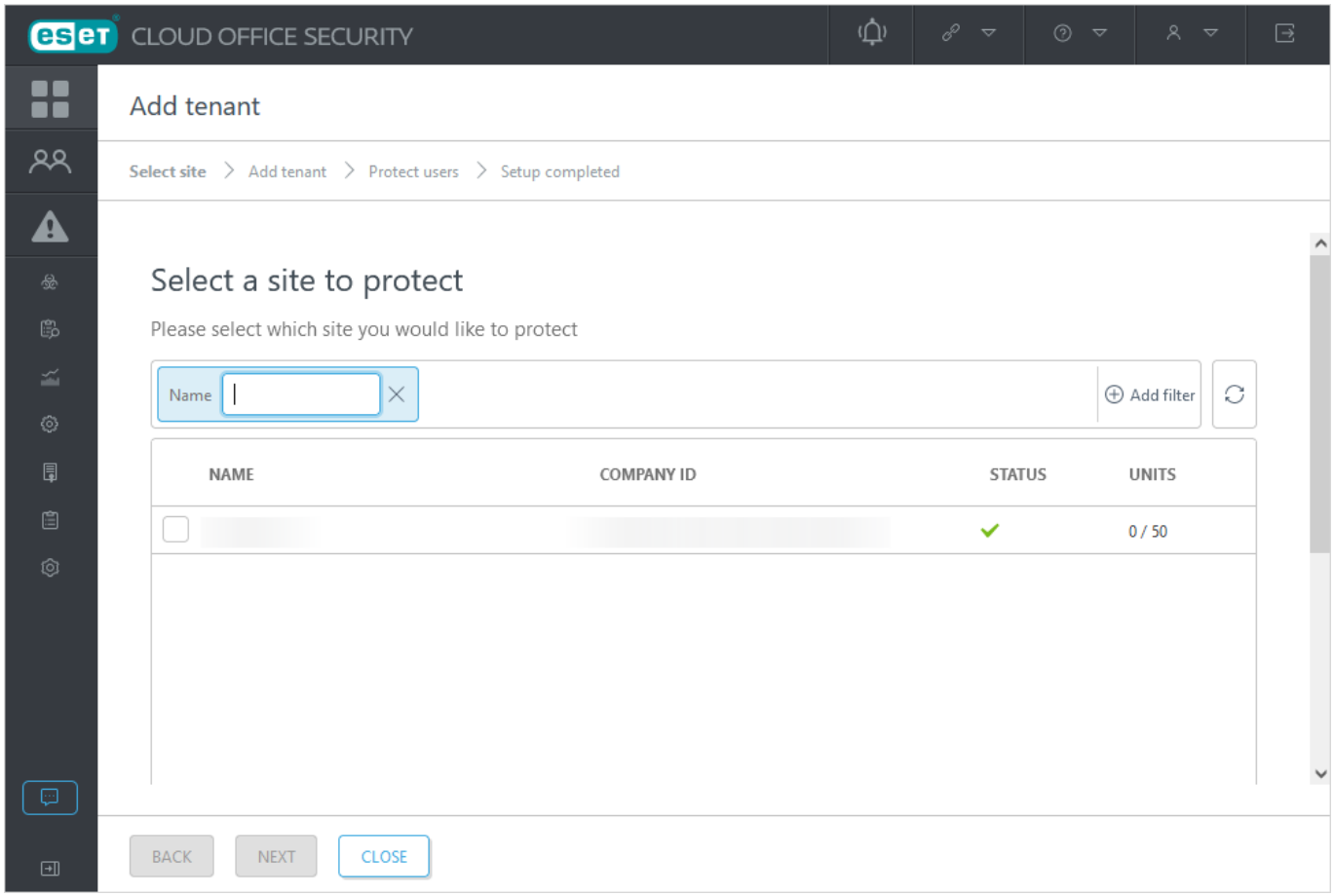
Als er een rode knop wordt weergegeven, is de toestemming ingetrokken of is er een andere wijziging aangebracht die van invloed is op de integratie van de tenant met ESET Cloud Office Security. Klik op de knop **Bijwerken** als u gebruikers wilt blijven beveiligen.

Uw eerste tenant toevoegen

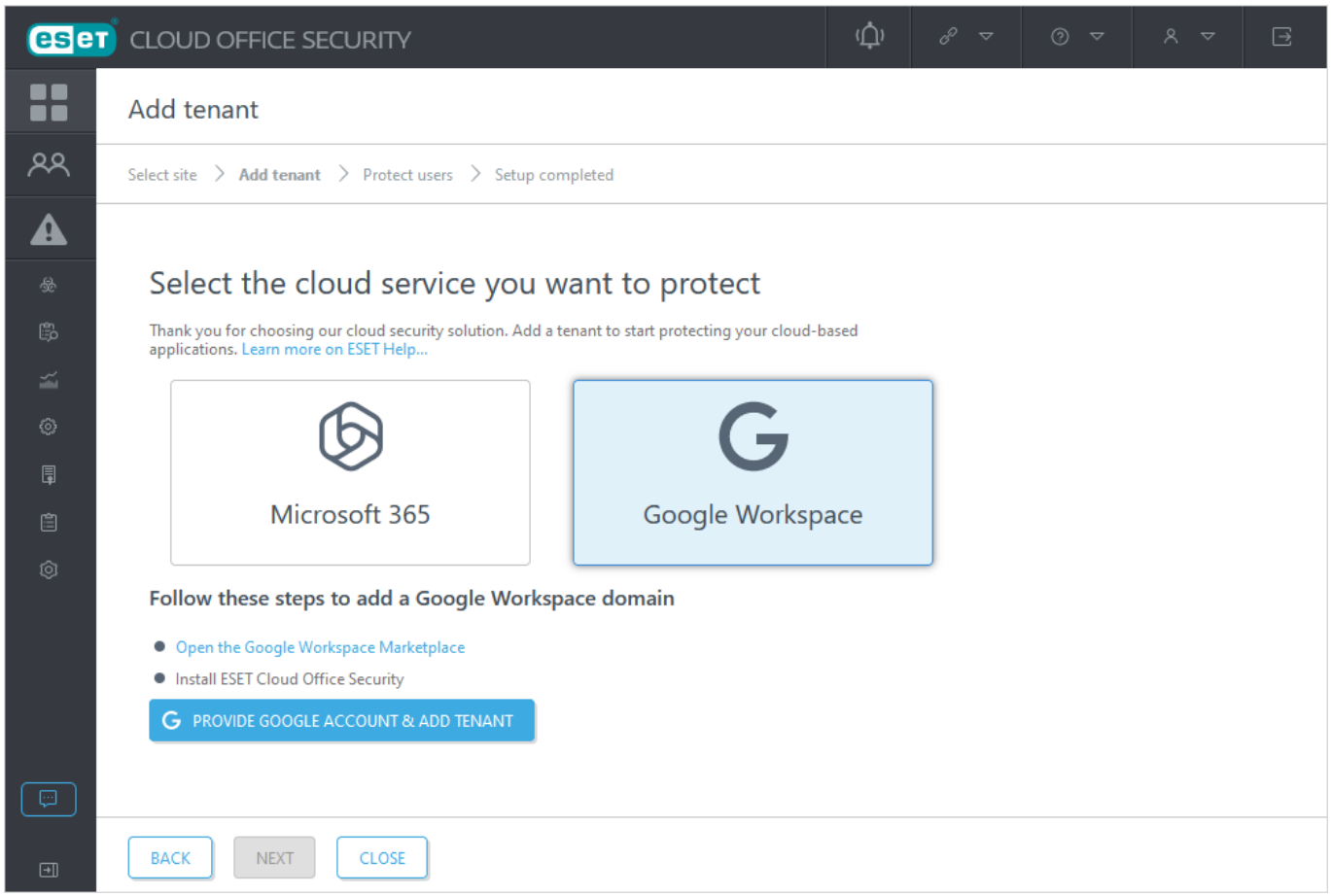
Als u uw cloudplatform wilt beveiligen, klikt u op **Tenant toevoegen** om uw Microsoft 365 of Google Workspace te verbinden met ESET Cloud Office Security.



U ziet een lijst met beschikbare sites in het venster **Selecteer een site om te beveiligen**. Gebruik het selectievakje om de site te selecteren die u aan een tenant wilt koppelen en klik op **Volgende**.



Klik op de tegel Microsoft 365 of Google Workspace in het venster **Selecteer de cloudservice die u wilt beveiligen** en volg de stapsgewijze instructies:



Microsoft 365-tenant

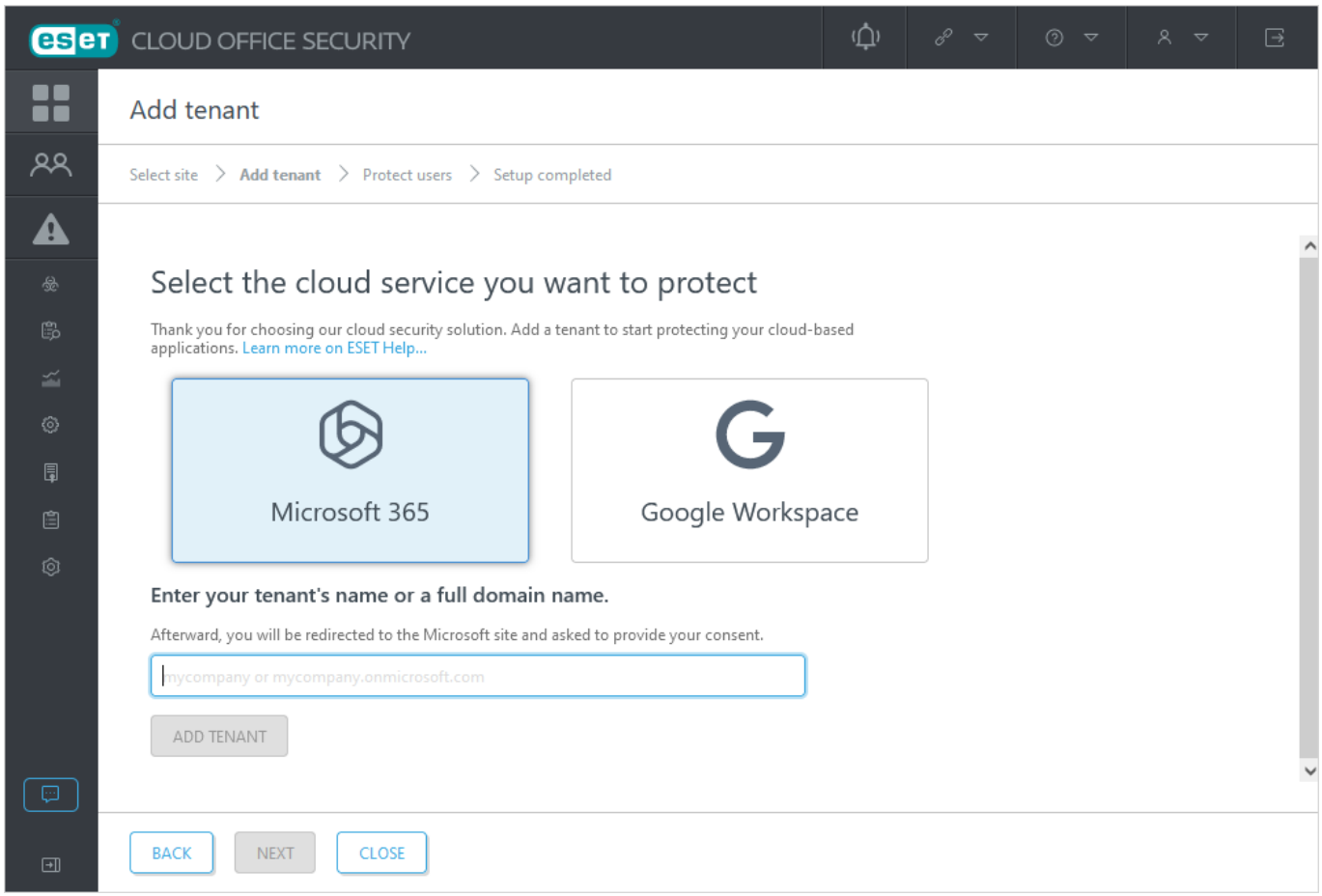
Azure Active Directory (Azure AD) organiseert objecten zoals gebruikers en apps in groepen die tenants worden genoemd. Een tenant wordt doorgaans geïdentificeerd aan de hand van de domeinnaam. Als meerdere gebruikers dezelfde domeinnaam hebben, maken deze gebruikers deel uit van dezelfde tenant. Op basis van tenants kunt u beleid instellen voor gebruikers en apps binnen uw organisatie om te voldoen aan het beveiligingsbeleid en het operationele beleid. U kunt meerdere Microsoft 365-tenants vanuit één ESET Cloud Office Security-console beveiligen en beheren.

Zie het artikel van Microsoft over Tenancy in Azure Active Directory voor meer informatie.

Tenant toevoegen

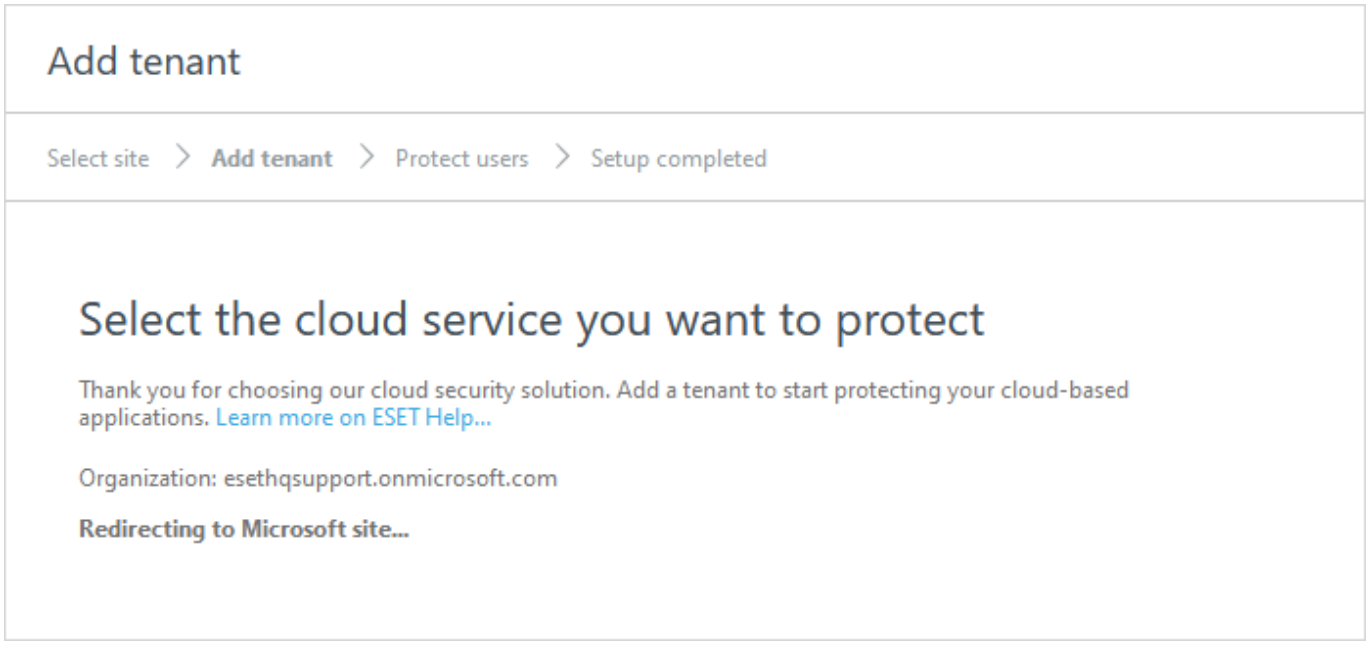
1. Ga naar **Instellingen** en klik op **Tenant toevoegen** (of klik ergens waar u de knop **Tenant toevoegen** ziet).

2. Klik op de tegel **Microsoft 365**.

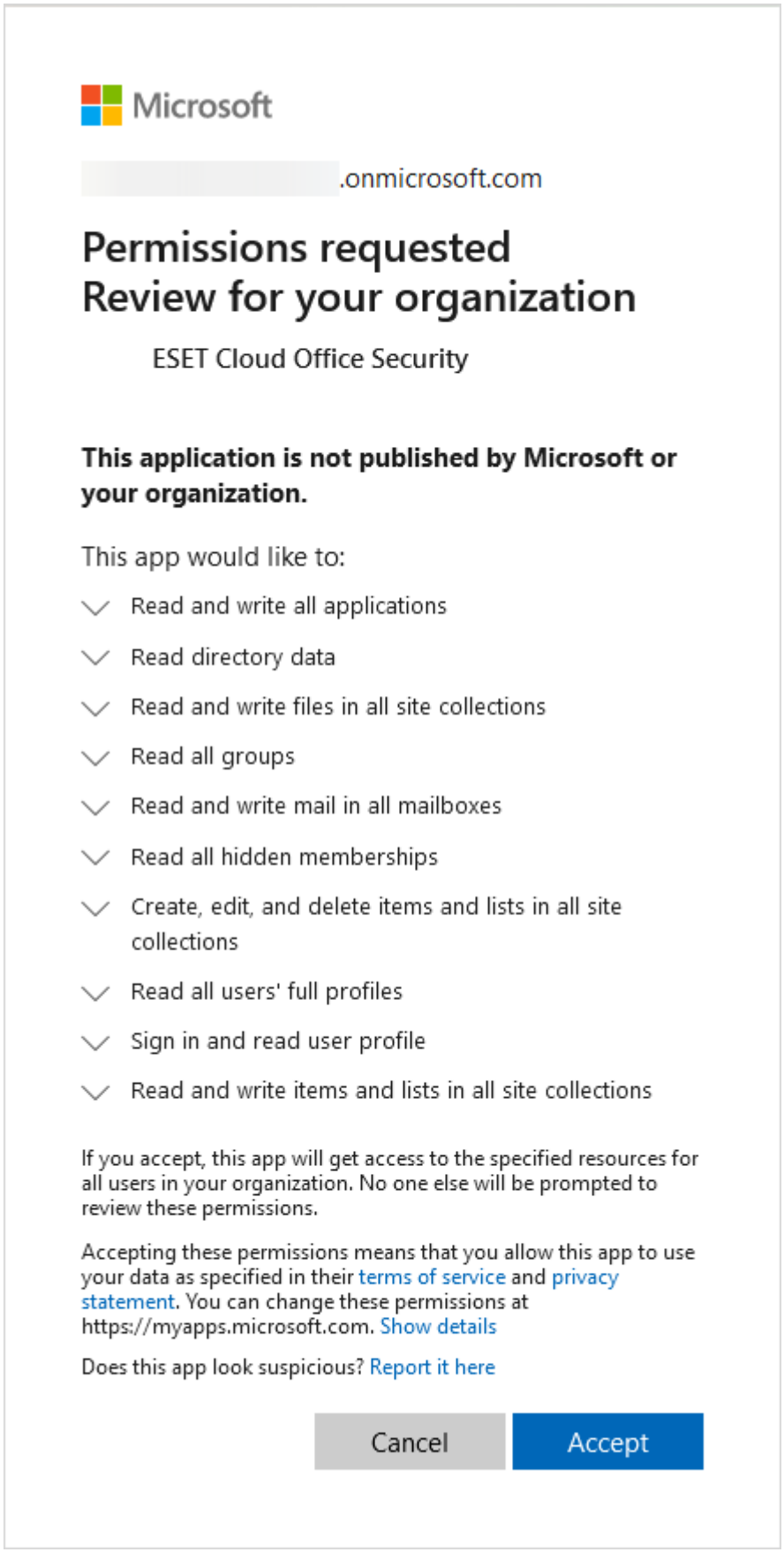


3. Typ uw Microsoft 365-tenantnaam of volledige domeinnaam en klik op **Tenant toevoegen**.

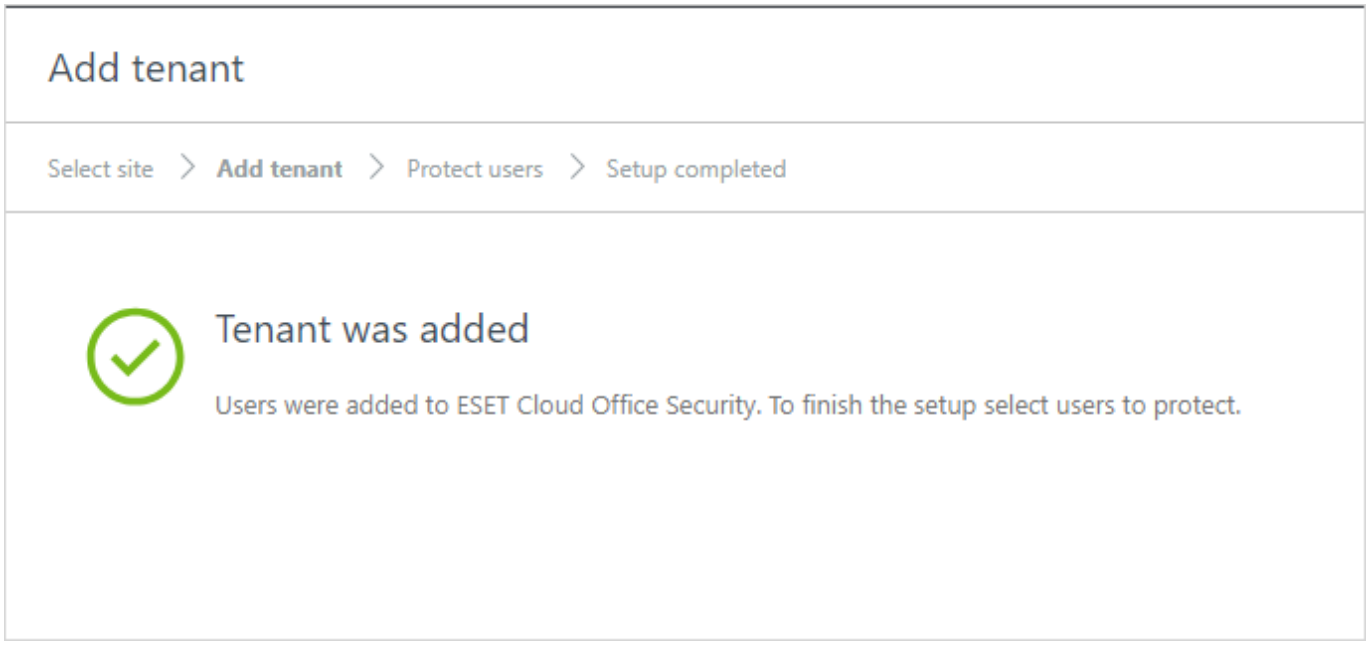
4. U wordt doorgestuurd naar de toestemmingspagina van Microsoft Online waarop zich een lijst met machtigingen bevindt die door ESET Cloud Office Security worden vereist.



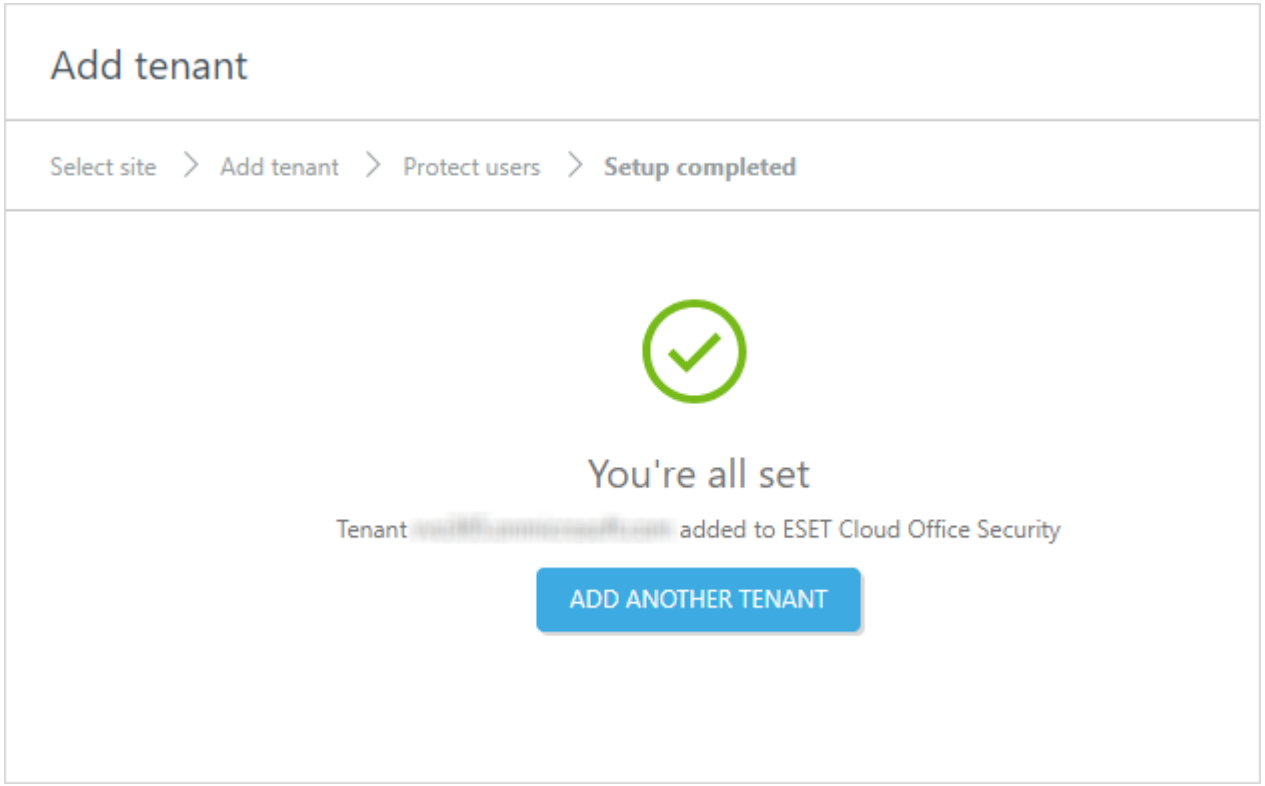
5. Als u ESET Cloud Office Security toegang wilt geven tot gegevens die zich in uw Microsoft-account bevinden, klikt u op **Accepteren** en voert u de referenties voor uw Microsoft 365-beheerdersaccount in.



6. Uw Microsoft 365-tenant is toegevoegd, inclusief de gebruikers.



7. Als u de installatie wilt voltooien, klikt u op **Volgende** en selecteert u de gebruikers die u wilt **beveiligen**.



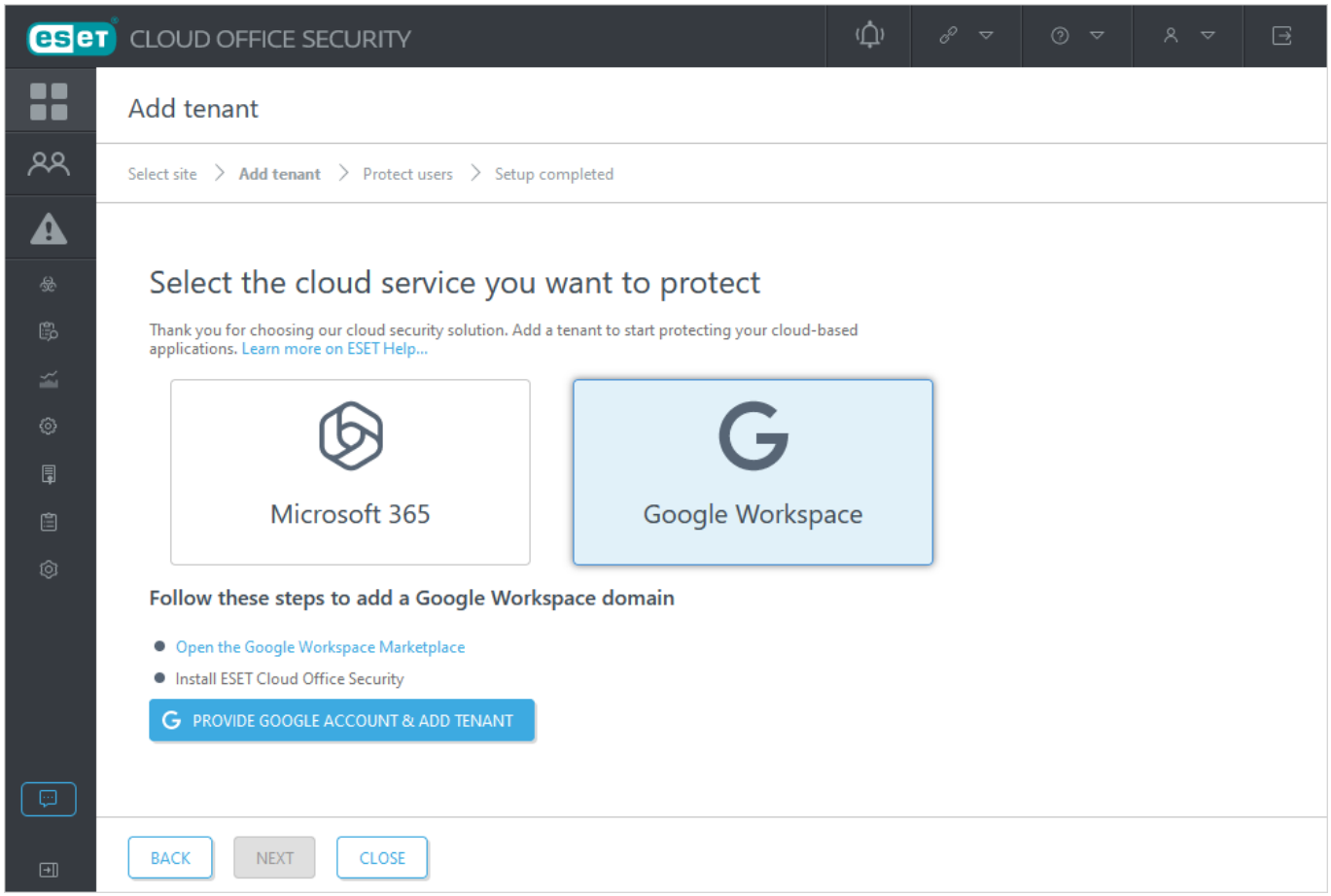
Google Workspace-tenant

Integreer uw Google Workspace-tenant met ESET Cloud Office Security om de beveiliging voor Google Workspace-gebruikers in te schakelen.

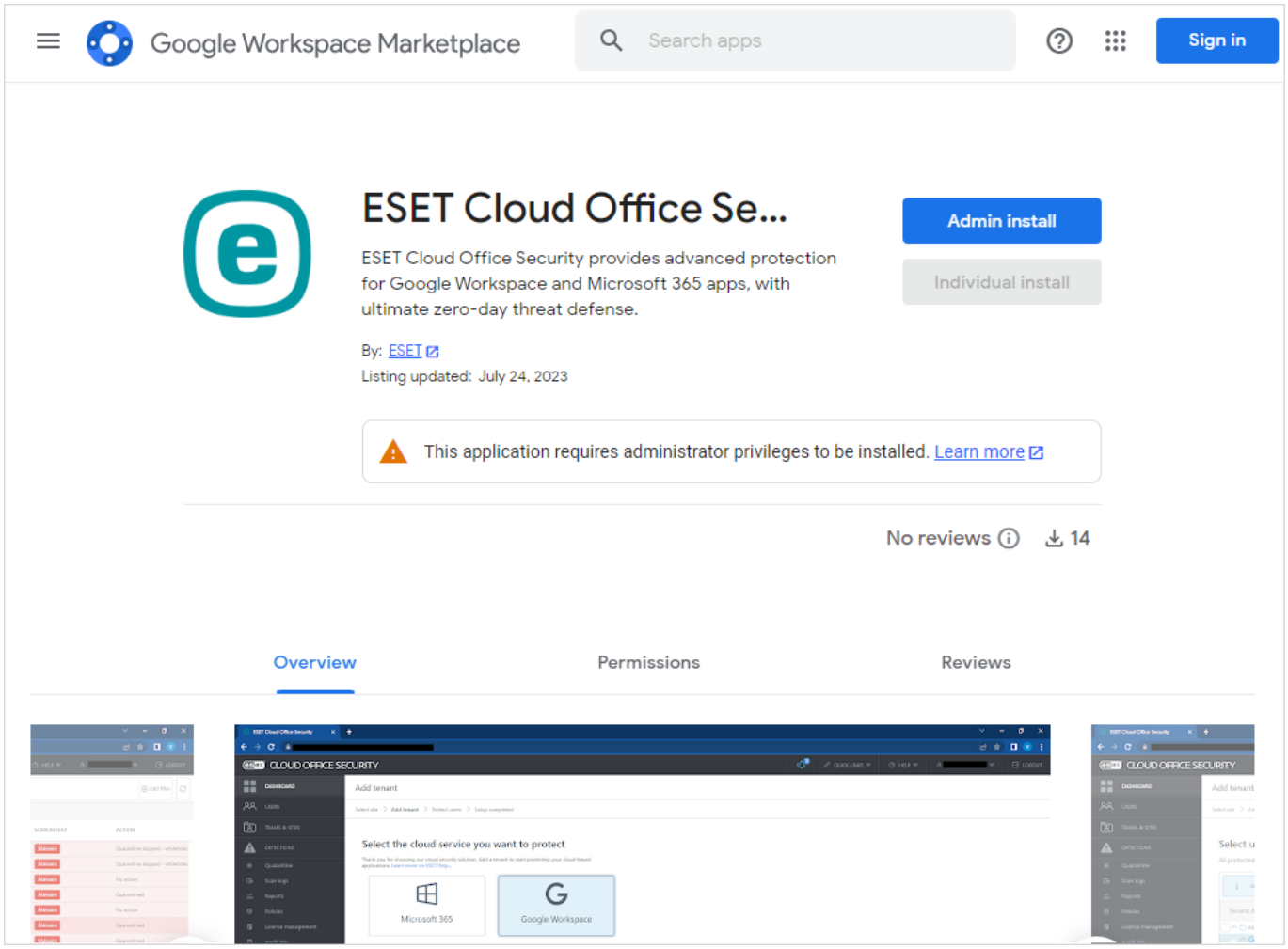
Tenant toevoegen

1. Ga naar **Instellingen** en klik op **Tenant toevoegen** (of ergens waar u de knop **Tenant toevoegen** ziet).

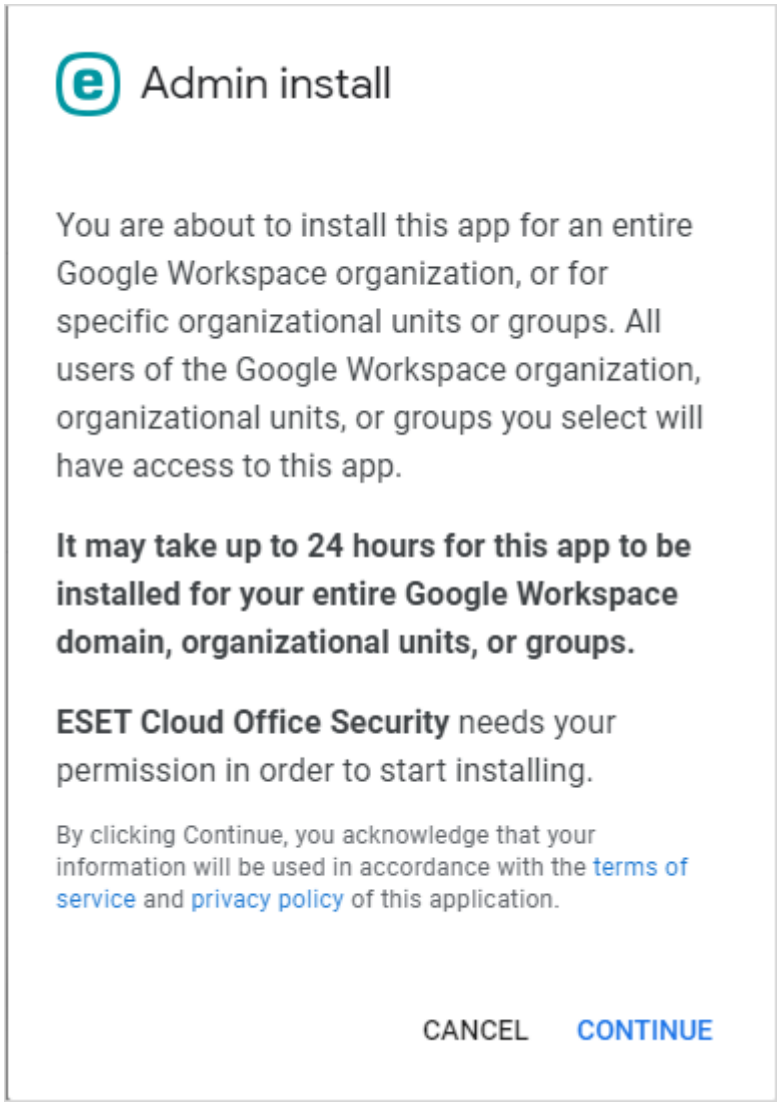
2. Klik op de tegel **Google Workspace**.



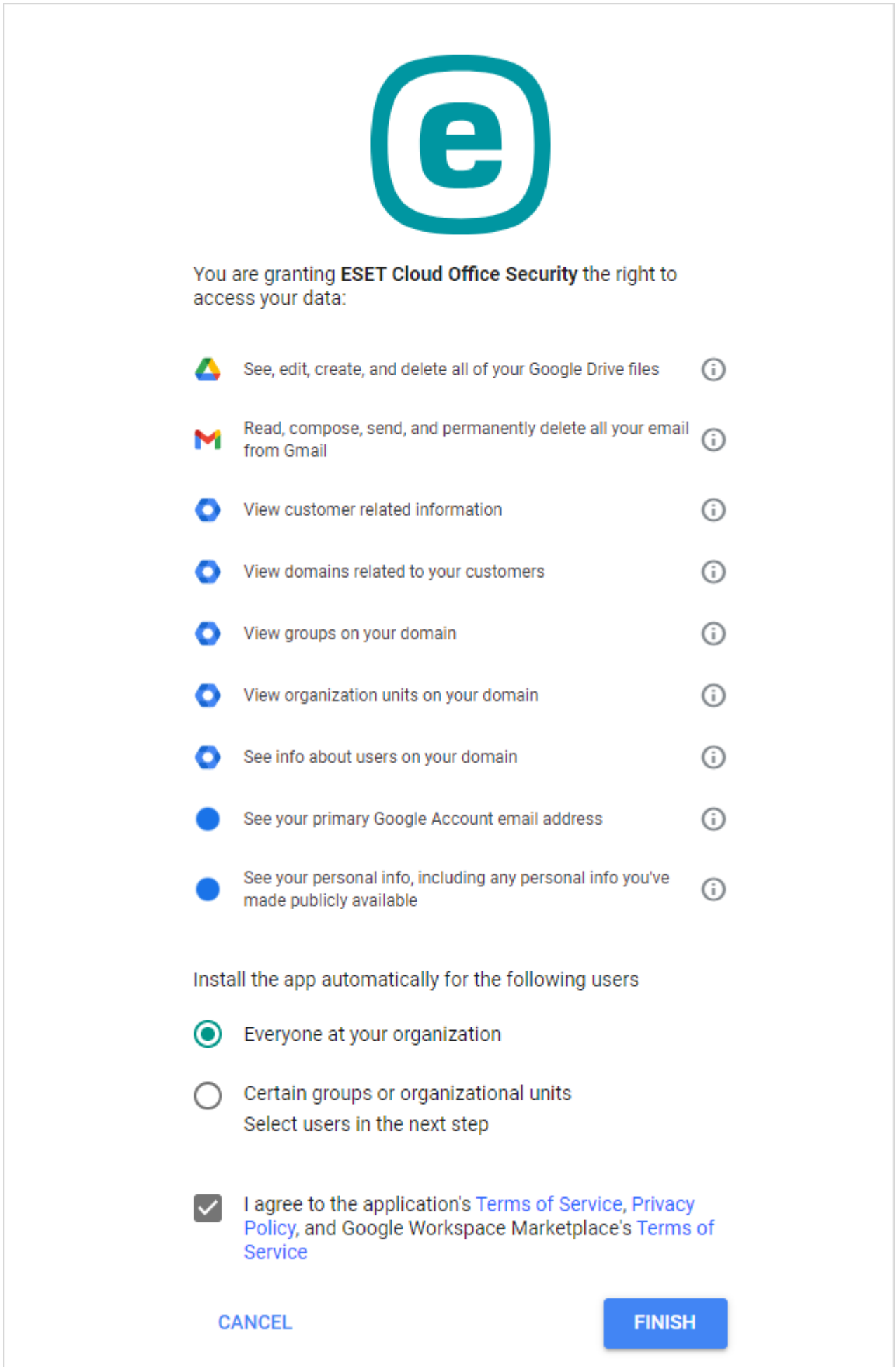
3. Klik op Google Workspace Marketplace openen en installeer de ESET Cloud Office Security-app met een beheerdersaccount. De ESET Cloud Office Security-app is momenteel alleen beschikbaar in de Google Workspace Marketplace via de directe koppeling vanuit deze wizard.



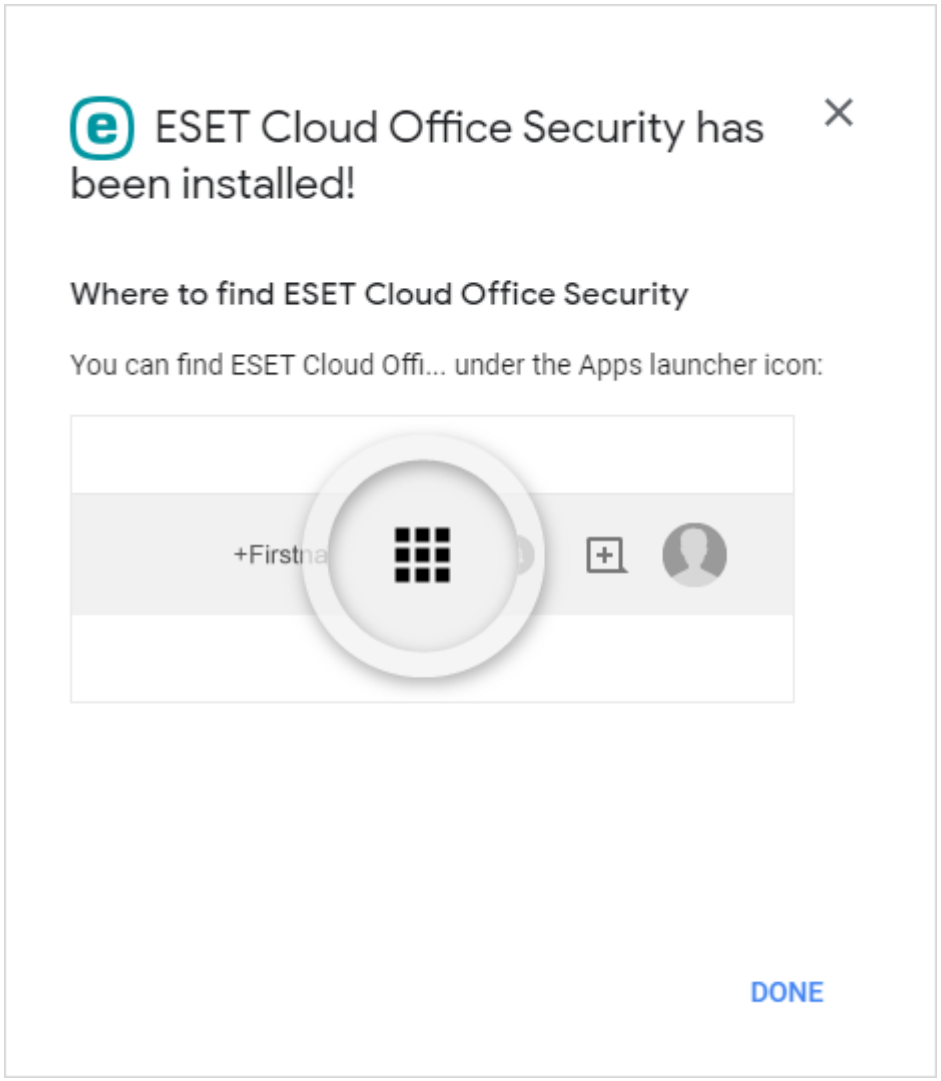
4. Klik op **Continue** (Doorgaan) in het scherm **Admin install** (Admin-installatie).



5. Controleer of de optie **Everyone at your organization** (Iedereen in uw organisatie) is geselecteerd op het scherm met toegangsrechten. Ook moet het selectievakje Terms of service and Privacy Policy (Servicevoorwaarden en Privacybeleid) worden ingeschakeld voordat u op **Finish** (Voltooien) klikt.

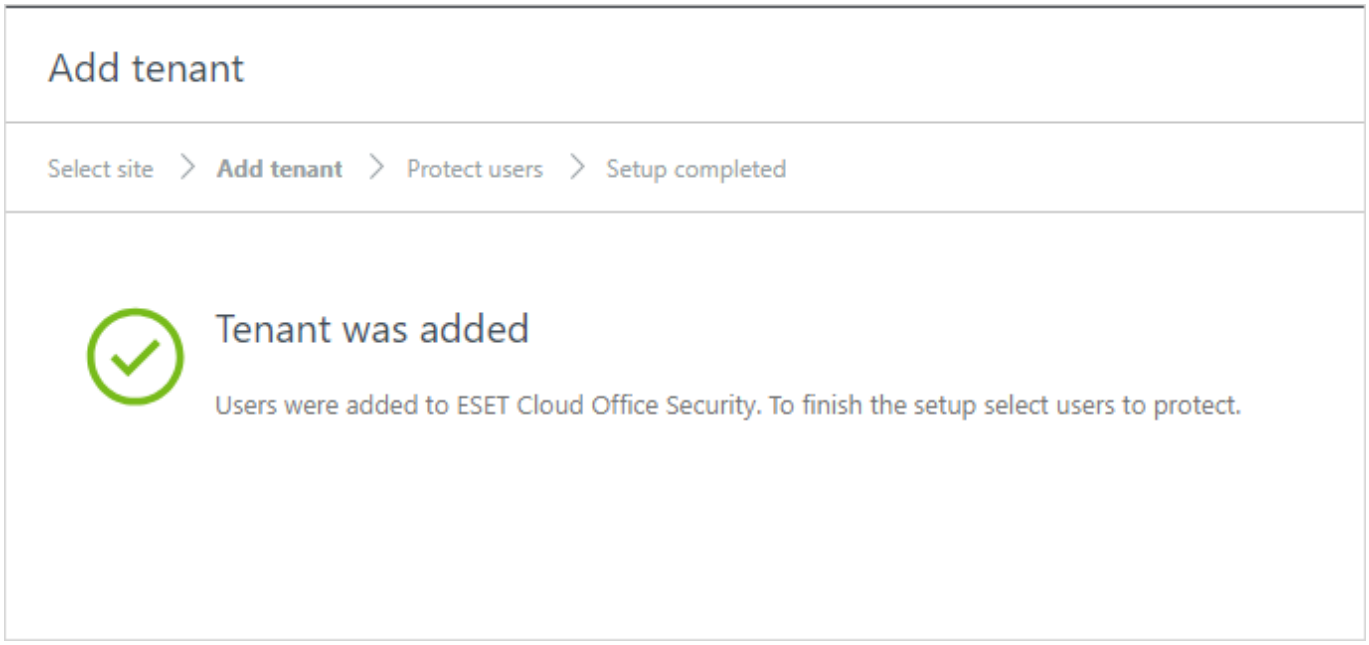

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your domain
View organization units on your domain
See info about users on your domain
See your primary Google Account email address
See your personal info, including any personal info you've made publicly available
Install the app automatically for the following users
Everyone at your organization
Certain groups or organizational units
Select users in the next step
I agree to the application's Terms of Service, Privacy Policy, and Google Workspace Marketplace's Terms of Service
CANCEL
FINISH

6. De ESET Cloud Office Security-app is geïnstalleerd, klik op **Done** (Gereed).

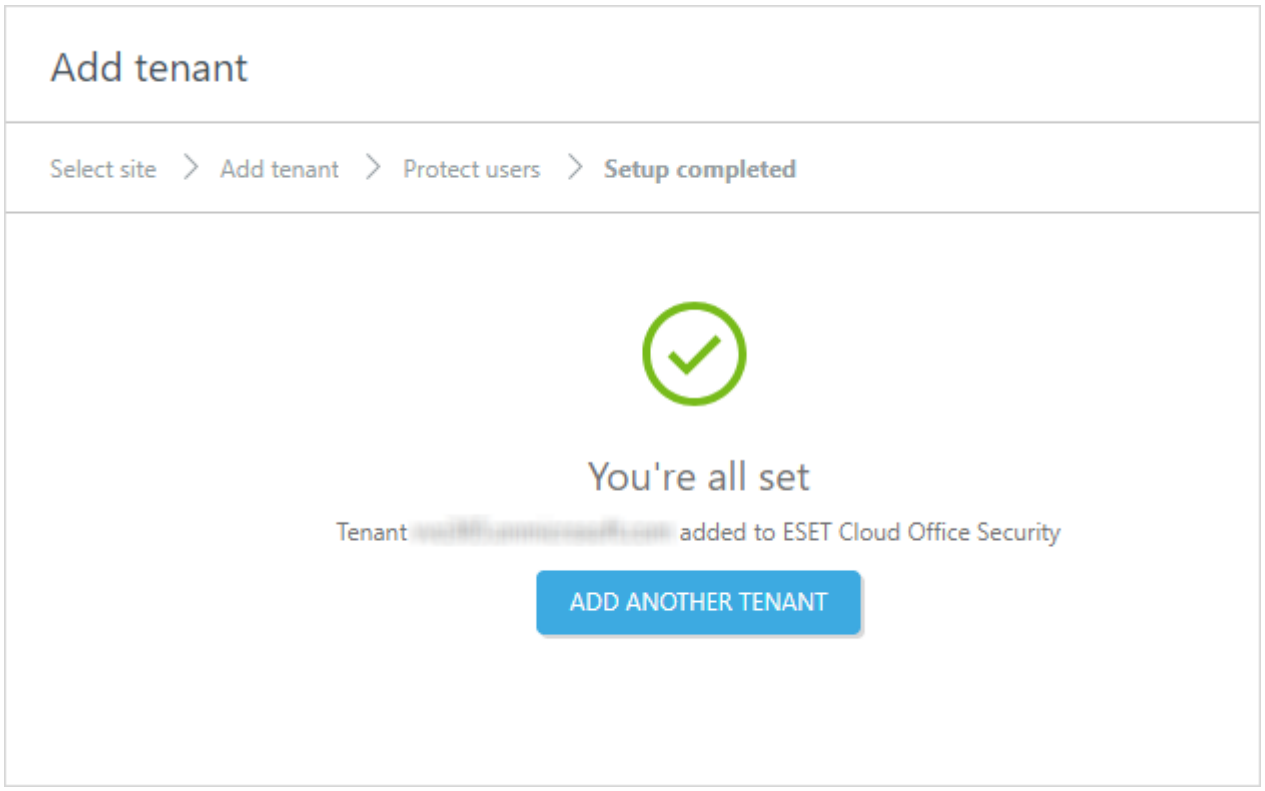


7. Wanneer de ESET Cloud Office Security-app gereed is, gaat u terug naar de ESET Cloud Office Security-console. Klik op **Google-account opgeven en tenant toevoegen** om het eigendom te verifiëren en door te gaan.

8. Uw Google Workspace-tenant is toegevoegd, inclusief de gebruikers.



9. Als u de installatie wilt voltooien, klikt u op **Volgende** en selecteert u de gebruikers die u wilt **beveiligen**. U bent helemaal klaar!

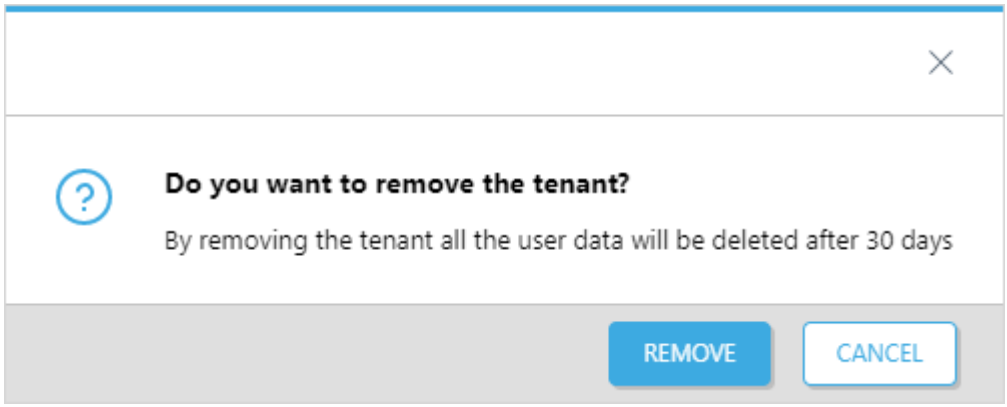


Tenant verwijderen uit ESET Cloud Office Security

1. Selecteer **Instellingen**.

2. Selecteer de toepasselijke tenant en klik op **Verwijderen**.

3. Er wordt een venster weergegeven met de melding dat er bij dit proces gegevens worden verwijderd zoals beschreven in Beperkingen en beleid voor gegevensretentie en dat gebruikers niet meer beveiligd zullen zijn. Klik op **Verwijderen** om het verwijderen te bevestigen.



Wanneer u een tenant uit de ESET Cloud Office Security-console verwijdert, worden tenantgegevens gedurende 30 dagen bewaard (quarantaine, scanlogboeken en statistieken worden na 30 dagen verwijderd). Als u de tenant binnen 30 dagen opnieuw toevoegt, worden alle gegevens hersteld. Andere objecten (tenants, gebruikers, groepen, sites, rapporten, beleidsregels) worden na 90 dagen permanent verwijderd. Zie Beperkingen en beleid voor gegevensretentie voor meer informatie.

ESET Cloud Office Security uit de Azure-portal verwijderen

1. Meld u met een beheerdersaccount aan bij de Azure-portal.

Als u een toepassing wilt verwijderen, moet u als eigenaar van de toepassing bekend zijn of beheerdersrechten hebben.

2. Navigeer naar de **Azure Active Directory-service** en selecteer **Enterprise-toepassingen**.

3. Zoek en klik op de **ESET Cloud Office Security**-toepassing op de overzichtspagina, ga naar **Eigenschappen** en klik op **Verwijderen**.

Navigeren in ESET Cloud Office Security

Bekijk hier hoe u kunt navigeren in de ESET Cloud Office Security-interface. U kunt snel vertrouwd raken met de navigatie-elementen en -tools van ESET Cloud Office Security, die intuïtief, gebruiksvriendelijk én interactief zijn.

Gebruik de navigatiebalk aan de linkerkant om te schakelen tussen verschillende onderdelen van de ESET Cloud Office Security-console:

- Gebruikers
- Teams en sites
- Detecties
- Quarantaine
- Scanlogboeken
- Rapporten

Beleid

Licentiebeheer

Controlelogboek

Instellingen

Samenvouwen — Vouw het navigatiemenu uit en vouw het samen. Het uitvouwen van het paneel geeft het dashboard meer ruimte op het scherm. Als u het navigatiedeelvenster wilt uitvouwen, klikt u op het pictogram .

De werkbalk bovenaan is altijd beschikbaar:



Productnavigator: snelle toegang tot ESET-consoles en andere nuttige koppelingen. (U kunt de betreffende producten bekijken al naargelang uw licentie en toegangsrechten).

ESET Business Account en **ESET MSP Administrator** (hybride licentieaccount) – Als u hetzelfde e-mailadres hebt geregistreerd in zowel ESET MSP Administrator als ESET Business Account (eenmalige aanmelding), kunt u schakelen tussen de ESET Business Account- en ESET MSP Administrator-weergave.

Meldingen weergeven — Klik op het belpictogram op de bovenste balk om alle meldingen weer te geven.

Snelle koppelingen — Biedt gemakkelijk toegang tot Tenant toevoegen, Nieuw beleid, ESET Business Account en ESET MSP Administrator.

Help — De eerste koppeling in dit menu verwijst altijd naar de online-Help voor het weergegeven scherm. Als u een probleem niet kunt oplossen, zoek dan in de ESET-kennisbank of het Supportforum. U kunt ook Feedback verzenden of een **Sample ter analyse verzenden**. Open de pagina Info met uitvoerige informatie over de ESET Cloud Office Security-versie en met koppelingen naar juridische documenten.

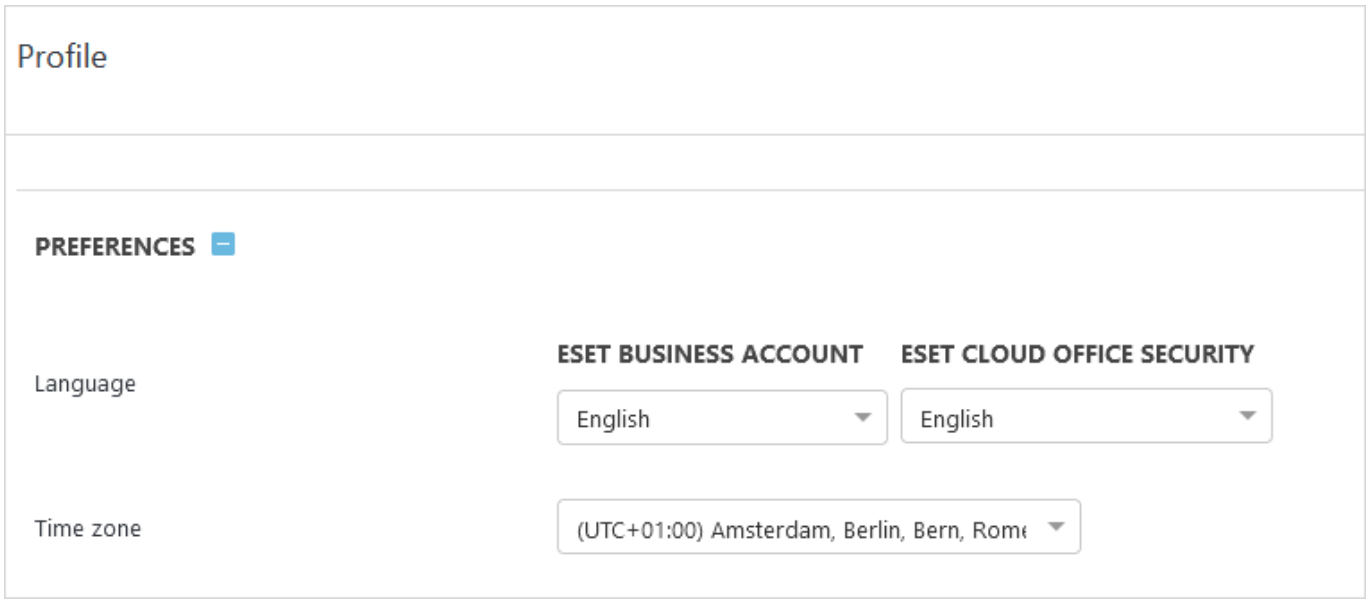
Gebruiker (momenteel aangemeld) – Geeft de gebruikersnaam weer. Klik op **Thema instellen** en selecteer het gewenste thema in het vervolgkeuzemenu:

- **Standaardthema (licht)**: ESET Cloud Office Security wordt weergegeven met een licht kleurenschema (standaard).
- **Donker thema**: ESET Cloud Office Security wordt weergegeven met een donker kleurenschema (donkere modus).
- **Thema van besturingssysteem**: het kleurenschema van ESET Cloud Office Security wordt gebaseerd op de instellingen van uw besturingssysteem.

Afmelden — Druk op dit pictogram dat overal aanwezig is om de ESET Cloud Office Security-console te verlaten.

Taal van de ESET Cloud Office Security-portal wijzigen

Meld u aan bij ESET Business Account op ESET MSP Administrator of navigeer naar **Gebruikersbeheer** en kies voor **Bewerken** van de gebruiker. Zoek naar de taalinstelling voor ESET Cloud Office Security, wijzig deze in uw voorkeurstaal en klik op **Opslaan** voordat u het scherm **Profiel** sluit.



ESET LiveGuard Advanced

ESET LiveGuard Advanced biedt een extra beveiligingslaag dankzij geavanceerde op ESET Cloud gebaseerde technologie om nieuwe, nooit eerder geziene bedreigingstypen te detecteren. ESET LiveGuard Advanced geeft u het voordeel dat u beschermd bent tegen mogelijke gevolgen die door nieuwe bedreigingen worden veroorzaakt. Als ESET LiveGuard Advanced verdachte code of gedrag detecteert, voorkomt het programma verdere bedreigingsactiviteit door de code tijdelijk in quarantaine te plaatsen.

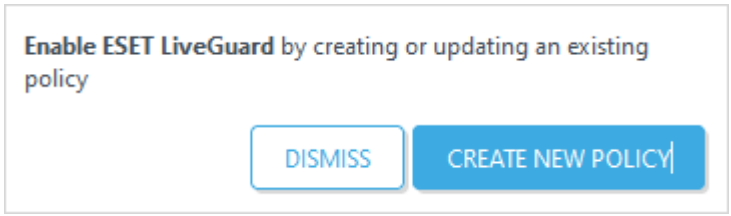
Er wordt automatisch een sample van de verdachte code (een bestand of e-mailbericht) bij ESET Cloud ingediend, waar de ESET LiveGuard Advanced-server de sample met de geavanceerde malwaredetectie-engines analyseert. Terwijl bestanden of e-mails zich in quarantaine bevinden, wacht ESET Cloud Office Security op de resultaten van de ESET LiveGuard Advanced-server.

Nadat de analyse is voltooid, ontvangt uw ESET Cloud Office Security een rapport met een samenvatting van het gedrag van de waargenomen sample. Als de sample onschadelijk blijkt, wordt het vrijgegeven en uit quarantaine gehaald. Anders blijft het in quarantaine staan.

ESET LiveGuard Advanced-resultaten van samples zijn meestal binnen een paar minuten beschikbaar voor e-mailberichten. Het standaardwachtinterval is echter ingesteld op 5 minuten. In zeldzame gevallen, wanneer de ESET LiveGuard Advanced-resultaten er niet binnen het interval zijn, wordt het bericht vrijgegeven. U kunt het interval wijzigen in de gewenste tijd (alles tussen 5-60 minuten, in stappen van één minuut).

Met een ESET Cloud Office Security-licentie kunt u de ESET LiveGuard Advanced-functie zonder extra kosten gebruiken. U vindt het ELG-label naast de licentie-id in Licentiebeheer.

Wanneer er een klein pop-upvenster wordt weergegeven, kunt u ESET LiveGuard Advanced activeren door nieuw beleid te maken of bestaand beleid bij te werken.



Zie Hoe ESET LiveGuard Advanced-detectielagen werken voor meer informatie over ESET LiveGuard Advanced .

Dashboard

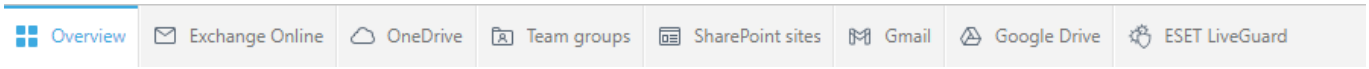
Het dashboard is een verzameling widgets die een overzicht geven van de beveiligingsactiviteiten van Microsoft 365. De overzichtstabbladen (Overzicht, Exchange Online, OneDrive, Teamgroepen, SharePoint-sites, Gmail, Google Drive en ESET LiveGuard Advanced) van het dashboard bevatten essentiële informatie. **Overzicht** is het hoofdscherm van het dashboard, dat u elke keer ziet wanneer u bij de ESET Cloud Office Security-console inlogt. Hierop staat algemene en statistische informatie.

> Het vernieuwingsinterval van Dashboard is 10 minuten. Als u niet de recentste informatie in Dashboard ziet, druk dan op **F5** om de weergave ervan handmatig te vernieuwen.

Als u dashboardstatistieken wilt bekijken, gebruikt u de filters bovenaan om de toepasselijke **Tijdsduur** (Afgelopen 24 uur, Afgelopen 7, 30 of 90 dagen) en **Tenant** te kiezen. Aanvullende detectiestatistieken en -grafieken vindt u op de overzichtstabbladen **Exchange Online**, **OneDrive**, **Teamgroepen**, **SharePoint-sites**, **Gmail**, **Google Drive** en **ESET LiveGuard Advanced**. Dit zijn statistieken zoals het aantal gescande e-mails en bestanden, en de hoeveelheid gedetecteerde spam/phishing/malware. De grafieken geven het verkeer weer voor elk detectietype: spam, malware en phishing.

Af en toe wordt de aankondigingsbalk weergegeven. Kleuren geven het type aankondiging aan (blauw = nieuws, geel = informatie, rood = waarschuwing).

Gebruik de tabbladen van Dashboard om tussen de weergavevensters te schakelen:



Overzicht

toont
- het aantal tenants en licentiegebruik
- statistieken per tenant:
  - Totaal aantal gebruikers/onbeveiligde gebruikers
  - Ontvangers met de meeste spam/phishing/malware
  - Belangrijkste verdachte OneDrive-accounts
  - Belangrijkste verdachte teamgroepen
  - Belangrijkste verdachte SharePoint-sites

doorklikken
- klik op de tegel Totaal aantal gebruikers om het gedeelte Gebruikers te openen
- klik op een gebruiker in het gedeelte met statistieken (spam/phishing/malware/OneDrive) om relevante detecties te zien, of klik op een groep of site om detecties en meer informatie over een verdachte Teamgroep of SharePoint-site te zien.

Exchange Online

toont
- totaal aantal gescande e-mails
- statistieken van gedetecteerde spam, malware en phishingmails
- grafieken, waarbij elke grafiek verkeer vertegenwoordigt van spam, malware en phishing

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

OneDrive

toont
- het aantal beveiligde gebruikers
- totaal aantal gescande bestanden
- statistieken van gedetecteerde malware
- een grafiek die malwareverkeer vertegenwoordigt

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

Teamgroepen

toont
- het aantal beveiligde groepen
- totaal aantal gescande bestanden
- statistieken van gedetecteerde malware
- een grafiek die malwareverkeer vertegenwoordigt

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

SharePoint-sites

toont
- het aantal beveiligde sites
- totaal aantal gescande bestanden
- statistieken van gedetecteerde malware
- een grafiek die malwareverkeer vertegenwoordigt

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

Gmail

toont
- totaal aantal gescande e-mails
- statistieken van gedetecteerde spam, malware en phishingmails
- grafieken, waarbij elke grafiek verkeer vertegenwoordigt van spam, malware en phishing

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

Google Drive

toont
- het aantal beveiligde gebruikers
- totaal aantal gescande bestanden
- statistieken van gedetecteerde malware
- een grafiek die malwareverkeer vertegenwoordigt

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

ESET LiveGuard Advanced

toont
- ingediende bestanden (het aantal omvat duplicaten en kan dus hoger zijn dan het aantal unieke bestanden)
- aantal detecties
- gemiddelde analysetijd
- een grafiek die ingediende bestanden vertegenwoordigt
- eigenaren van belangrijkste ingediende bestanden
- ingediende bestandstypen

De tegels zijn interactief. Klik op een tegel naar keuze en ga naar het relevante gedeelte in de ESET Cloud Office Security-console. Zo wordt bijvoorbeeld het gedeelte Scanlogboeken met relevante logboekrecords geopend.

Gebruikers

De centrale entiteit die ESET Cloud Office Security beveiligt, is het gebruikersaccount. Dubbelklik op een gebruiker om nuttige informatie te vinden, zoals Overzicht, Instellingen gedefinieerd door beleid, lijst met beleid dat is toegewezen aan de gebruiker en Detecties voor Gmail, Google Drive, Exchange Online en OneDrive. U kunt ook kiezen welke gebruikers worden beveiligd of niet worden beveiligd. Gebruikers worden gesorteerd in groepen en elke groep is een Microsoft 365-tenant met gebruikers. Als u het zoeken naar een bepaalde gebruiker binnen een groep gemakkelijker wilt maken, kunt u filteren op meerdere criteria.

> Gebruikers zonder Microsoft 365-licentie worden niet weergegeven in de ESET Cloud Office Security-console. Dit geldt ook voor gedeelde postvakken zonder Microsoft 365-licentie.
> Als u alle Microsoft 365-gebruikers wilt zien en beheren, ga dan naar Instellingen en schakel Gelicentieerde gebruikers van Microsoft 365 uit.

Beveiligingsstatus:

Status	Beschrijving
Niet-beveiligd	Een gebruiker is momenteel niet beveiligd.
Automatisch beveiligd	Beveiligde gebruiker met automatische beveiliging.
In behandeling	Overgangsstatus die optreedt tijdens het beveiligingsproces van een gebruiker. Zodra dit is voltooid, wordt de status van de gebruiker gewijzigd in Beveiligd.
Beveiligd	Het postvak en OneDrive van de gebruiker worden beveiligd door het standaardbeleid of door aangepast beleid.
WAARSCHUWING	Het beveiligingsproces van een gebruiker is mislukt. Er is mogelijk een fout opgetreden voor de bronnen, het postvak of OneDrive. Het is waarschijnlijk dat beide bronnen niet beschikbaar zijn voor de gebruiker. Controleer of aan de gebruiker een geldige Microsoft 365-licentie is toegewezen.

Navigeer binnen de structuur om gebruikers van een bepaalde tenant of groep te zien. Als u alle gebruikers in elke tenant en groep wilt zien, klikt u op **Alles**.

Dubbelklik op een gebruiker of klik op het pictogram  en selecteer een actie (**Details weergeven**, **Beveiligen** of **Beveiliging opheffen**). Klik op een gebruiker om het venster **Details weergeven** te openen, dat uit vier delen bestaat:

Actie	Syntaxis
Overzicht	Geeft basisinformatie weer over de gebruiker die vanuit Microsoft 365 is geladen (e-mail, groep, taakprofiel, enz.). Ook wordt de huidige beveiligingsstatus voor het postvak en OneDrive weergegeven.
Configuratie	Bevat een lijst met Instellingen (alleen-lezen) en toegewezen Beleid voor deze gebruiker. Schakel tussen de tabbladen om de configuratie of een lijst met toegewezen beleidsregels weer te geven. U kunt instellingen niet wijzigen of beleid aan gebruikers toewijzen. Ga in plaats hiervan naar het gedeelte Beleid.
Detecties	Alle detecties voor dit gebruikersaccount weergeven (Gmail, Google Drive, Exchange Online of OneDrive).
Quarantaine	Geeft alle quarantainemails en bestandsarchieven van deze gebruiker weer. U kunt ook een actie gebruiken: E-mails of bestanden in quarantaine Vrijgeven, Downloaden of Verwijderen.

U kunt gebruikers filteren op verschillende criteria. Klik op **Filter toevoegen** en selecteer een filtertype in het vervolgkeuzemenu of voer een tekenreeks in (herhaal dit als u meerdere criteria combineert):

Filter toevoegen	Syntaxis
Beveiligingsstatus	Selecteer de status Beveiligd, Niet-beveiligd, Waarschuwing of In behandeling van een gebruiker.
Automatisch beveiligd	Alleen automatisch beveiligde gebruikers weergeven.
Naam	Typ een geldige gebruikersnaam.
E-mail	Typ een geldig e-mailadres van een gebruiker.
Type	Selecteer het gebruikerstype (Onbekend, Gebruiker, Gekoppeld, Gedeeld postvak, Ruimte, Apparatuur, Overige).

Gebruikers beveiligen

1. Selecteer **Gebruikers** die worden beveiligd en klik op **Beveiligen**.
2. Selecteer de **Licentiepool** die is geladen vanuit ESET Business Account en klik op **OK**. Het standaardbeleid beveiligt nu geselecteerde gebruikers.
3. Geef indien nodig aangepast beleid op voor gebruikers in het gedeelte Beleid.

Beveiliging van gebruikers opheffen

Selecteer **Gebruikers** die niet langer beveiligd hoeven te worden en klik op **Beveiliging opheffen**.

Teams en sites

ESET Cloud Office Security biedt beveiliging aan Teamgroepen en SharePoint-sites.

Schakelen tussen de tabbladen Teamgroepen en SharePoint-sites. Er wordt een lijst met Teamgroepen of SharePoint-sites weergegeven voor elke tenant.

Teamgroepen

geeft objecten weer die van het groepstype Microsoft 365 zijn, inclusief de standaard SharePoint-teamsite en OneDrive:

- naam
- status
- e-mail
- tenant

Als u Teamgroepen wilt beveiligen, moet u ervoor zorgen dat ten minste één lid een gebruiker is die door ESET Cloud Office Security wordt beveiligd. Elke Microsoft 365-groep heeft een standaard SharePoint-teamsite en OneDrive die ook zijn beveiligd.

SharePoint-sites

geeft alle SharePoint-hoofdsites weer die niet zijn gekoppeld aan de Microsoft 365-groep:

- naam
- status
- URL
- tenant

SharePoint-sites worden automatisch beveiligd, ook de subsites ervan (niet weergegeven).

Klik voor meer informatie op een Teamgroep of SharePoint-site om het venster **Details weergeven** te openen dat uit vier onderdelen bestaat:

Actie	Syntaxis
Overzicht	Geeft de benodigde informatie over de Teamgroepen of SharePoint-sites weer die vanuit Microsoft 365 zijn geladen (E-mail, Eigenaar, Leden, Auteur, URL, enz.). Ook de huidige beveiligingsstatus voor Teamgroep of SharePoint-site wordt weergegeven.
Configuratie	Bevat een lijst met Instellingen (alleen-lezen) en toegewezen Beleid. Schakel tussen de tabbladen om de configuratie of een lijst met toegewezen beleidsregels weer te geven. U kunt instellingen niet wijzigen of beleid toewijzen. Ga in plaats hiervan naar het gedeelte Beleid.
Detecties	Alle detecties voor Teamgroep of SharePoint-site weergeven.
Quarantaine	Alle in quarantaine geplaatste bestanden weergeven. U kunt ook een actie gebruiken: Bestanden in quarantaine Vrijgeven, Downloaden of verwijderen.

Klik op **Filter toevoegen** om Teamgroepen of SharePoint-sites te filteren.

Detecties

Hier worden alle detecties van ESET Cloud Office Security weergegeven. Schakel tussen Gmail, Google Drive, Exchange Online, OneDrive, Teamgroepen en SharePoint-sites met de tabbladen. Bekijk informatie over elke detectie. Gedetecteerde bestanden die naar een Teamgroep zijn geüpload, worden bijvoorbeeld weergegeven op het tabblad Teamgroepen.

Klik op het pictogram om een zijbalk te openen met een overzicht van een specifieke logboekrecord (detectie). Klik op het pictogram en selecteer **Details weergeven** voor uitvoerige informatie.

Navigeer binnen de structuur om alleen detecties voor een bepaalde tenant of groep te zien. Klik op **Alles** als u alle detecties in elke tenant en groep wilt zien. Als u het zoeken naar een bepaalde detectie gemakkelijker wilt maken, kunt u filteren op meerdere criteria. Klik op **Filter toevoegen** en selecteer het filtertype in het vervolgkeuzemenu of voer een tekenreeks in (herhaal dit wanneer u criteria combineert):

Filter toevoegen	Syntaxis
Vond plaats van	Geef een bereik voor Datum vanaf op.
Vond plaats tot	Geef een bereik voor Datum tot op.
Onderwerp	Is van toepassing op berichten die een specifieke tekenreeks (of een reguliere expressie) wel of niet in het onderwerp bevatten.
Bericht-id	Filter e-mailberichten op unieke bericht-id bij het zoeken naar een specifiek bericht, vooral in grote logboeken met veel berichten of bij meerdere bezorgingspogingen.
Van	Berichten filteren op een specifieke afzender.
Tot	Berichten filteren op ontvangers.
Postvak	Is van toepassing op berichten die zich in een specifiek postvak bevinden.
Scanresultaat	Selecteer een van de volgende opties: Malware, -malware (gedetecteerd door ESET LiveGuard Advanced), phishing of spam.
Actie	Selecteer een van de beschikbare acties.
Team	Typ de geldige teamnaam.
Site	Typ de geldige sitenaam.
Object	Typ een geldige objectnaam.
Detectie	Typ een geldige detectienaam.
Hash	Typ een geldige detectiehash.

Wanneer u op het pictogram klikt, is de optie **Van witte lijst verwijderen** beschikbaar als u eerder voor dezelfde gebruiker een bestand op de witte lijst hebt geplaatst door dit uit Quarantaine te halen. Gebruik deze optie om een bestand van de witte lijst te verwijderen. Al deze toekomstige bestanden worden in quarantaine geplaatst.

De bewaartermijn voor detecties is 90 dagen. Records ouder dan 90 dagen worden definitief verwijderd.

Vals-positief/vals-negatief melden

U kunt vals-positieve en vals-negatieve detecties voor spam, phishing of malware handmatig melden door een sample ter analyse naar ESET-labs te verzenden. E-mailadressen om de samples naartoe te verzenden:

Spam: stuur een e-mail naar nospam_ecos@eset.com voor e-mails die onjuist zijn gemarkeerd als spam, of naar spam_ecos@eset.com voor niet-gedetecteerde spam met het oorspronkelijke bericht als bijlage in de indeling *.eml* of *.msg*.

Phishing: om vals-positieve of vals-negatieve classificaties van phishing te melden, moet u een nieuw e-mailbericht maken en verzenden naar samples@eset.com met *'phishing email'* op de onderwerpregel en de phishingmail als bijlage in de indeling *.eml* of *.msg* aan het bericht toevoegen.

Malware: om vals-positieve of vals-negatieve classificaties van malware te melden, moet u een nieuw e-mailbericht maken en verzenden naar samples@eset.com met *'False positive'* of *'Suspected infection'* op de onderwerpregel en het bestand of de bestanden gecomprimeerd als bijlage in de indeling *.zip* of *.rar* aan het bericht toevoegen.

Rapporten

Met ESET Cloud Office Security-rapporten wordt u op de hoogte gehouden. U krijgt namelijk een overzicht van de ESET Cloud Office Security-beveiligingsstatistieken. U kunt kiezen uit twee typen rapporten, statistische rapporten of rapporten van E-mailquarantaine.

In statistische rapporten vindt u informatie over de beveiliging van Gmail, Google Drive, Exchange Online, OneDrive, Teamgroepen en SharePoint-sites, en hierin vindt u het aantal gescande e-mails, bestanden, gedetecteerde malware, phishing en spam voor de opgegeven periode. De rapporten kunnen handmatig worden gegenereerd en gedownload als *PDF*- of *CSV*-bestand of worden gepland en als e-mail worden bezorgd bij geselecteerde ontvangers. In een *PDF* worden gegevens als grafiek weergegeven, ziet u het langetermijngemiddelde ter vergelijking en vindt u informatie over het verkeer voor elk beveiligingstype en de belangrijkste ontvangers van malware, phishing en spam.

In het rapport van E-mailquarantaine staat een lijst met objecten die onlangs in quarantaine zijn geplaatst. Het rapport wordt per e-mail naar geselecteerde ontvangers verzonden. De ontvangers kunnen spamberichten vrijgeven (indien ze als veilig of legitiem worden beschouwd) door op de koppeling **Vrijgeven** te klikken. Is alleen van toepassing op spam. Andere typen in quarantaine geplaatste objecten kunnen niet worden vrijgegeven.

U kunt de statistieken per e-mail ontvangen en hoeft zich niet aan te melden bij de ESET Cloud Office Security-console. Stel terugkerende rapporten in en geef e-mailontvangers op. Bovendien kunt u rapportstatistieken genereren, rechtstreeks vanuit de ESET Cloud Office Security-console. Selecteer een bestaand rapport (kan ook een gepland rapport zijn) en klik op **Genereren en downloaden**. Ook kunt u klikken met de rechtermuisknop en de vervolgkeuzelijst gebruiken. U kunt eenvoudig een nieuwe rapportsjabloon met aangepaste instellingen maken.

Nieuw rapport

Klik op Nieuw rapport om een rapportsjabloon te openen en aangepaste instellingen op te geven. Voer een rapportnaam en beschrijving in.

Taal

Kies de gewenste taal in het vervolgkeuzemenu. Het rapport wordt gegenereerd in de geselecteerde taal.

Type

Selecteer welk type u in de statistieken opgenomen wilt hebben.

Statistische rapporten

Maak een gepland rapport of maak er een on-demand met daarin informatie op basis van de opties die u kiest.

E-mailquarantainerapporten

Als u gebruikers wilt informeren over hun onlangs in quarantaine geplaatste e-mailberichten, moet u e-mails met meldingen naar geselecteerde gebruikers sturen. U kunt één of meerdere ontvangers of een groep toewijzen. Kies een interval voor de rapporten en de begindatum en -tijd. Als het een periodiek rapport is, kies dan wanneer deze rapporten moeten eindigen (op een datum, na een bepaald aantal of nooit). Het rapport van E-mailquarantaine wordt alleen geactiveerd als er nieuwe items zijn. De ontvangers van het rapport kunnen spamberichten vrijgeven (als ze als veilig of legitiem worden beschouwd) door op de koppeling Vrijgeven te klikken (er wordt een bevestigingsvenster in een webbrowser geopend). Het vrijgegeven spambericht wordt als bijlage in een

afzonderlijke e-mail bezorgd.

Tenant

Deze optie is beschikbaar in een omgeving met meerdere tenants. U kunt meerdere tenants selecteren om statistieken te genereren. Het rapport wordt voor elke tenant afzonderlijk gegenereerd en wordt in één ESET Cloud Office Security-rapportmail met meerdere bijlagen geleverd.

Tijdsduur

Definieer de periode waarvoor u resultaten weergegeven wilt hebben (laatste 24 uur, week, maand). Wanneer u Aangepast selecteert, kunt u een bereik opgeven (Datum van en Datum tot).

Uitvoer

Selecteer de juiste bestandsindeling. U kunt kiezen uit *PDF* en *CSV*. In de *PDF*-indeling bevinden zich de gegevens die in grafieken worden weergegeven. *CSV* is geschikt voor onbewerkte gegevens. Rapporten worden verzameld op basis van bepaalde opties. Als u zowel gegevens van Gmail, Google Drive, Exchange Online, OneDrive, Teamgroepen als SharePoint-sites hebt geselecteerd, is het uitvoerbestand een archief in ZIP-indeling met daarin *PDF*- of *CSV*-rapportbestanden.

Whitelabel

Als u wilt dat het logo van uw bedrijf in het rapport wordt weergegeven, schakelt u deze functie in. U hebt de mogelijkheid om een co-branded koptekst in het rapport aan te brengen met uw logo samen met dat van ESET, of met alleen uw logo. Upload het logo in *PNG*- of *JPEG*-indeling.

Gepland

Gebruik de planner om de rapporten te laten genereren op een bepaalde datum en tijd. U kunt dit ook als terugkerende gebeurtenis in de planner opnemen. Geplande rapporten worden naar geselecteerde ontvangers verzonden, die ESET Cloud Office Security-rapporten als bijlage(n) in een e-mail ontvangen.

Herhalen

Kies of u wilt dat het rapport eenmaal of herhaaldelijk wordt gegenereerd:

- **Eenmaal**: het rapport wordt slechts één keer uitgevoerd.
- **Dagelijks**: het rapport wordt elke dag herhaaldelijk gegenereerd en geleverd (tenzij u opgeeft dat de herhaling wordt beëindigd na xx gebeurtenissen).
- **Wekelijks**: het rapport wordt herhaaldelijk gegenereerd en op de geselecteerde dag(en) van de week bezorgd.
- **Maandelijks**: het rapport wordt eenmaal per maand gegenereerd en op een geselecteerde dag bezorgd.

Vanaf

Kies de begindatum voor de rapporten.

Eindigt

Selecteer wanneer het herhalingsinterval is afgelopen.

Ontvangers

Geef het e-mailadres van de ontvanger van het rapport op en druk op Enter om uw keuze te bevestigen. Herhaal dit als u meerdere ontvangers wilt toevoegen.

Klik op het pictogram  en selecteer een actie voor meer informatie:

Actie	Syntaxis
Details weergeven	Geeft uitvoerige informatie over een rapport weer.
Genereren en downloaden	Klik op Genereren en downloaden en kies *PDF* of *CSV*. In de *PDF*-indeling bevinden zich de gegevens die in grafieken worden weergegeven. *CSV* is geschikt voor onbewerkte gegevens. Rapporten worden verzameld op basis van bepaalde opties. Als u zowel gegevens van Exchange Online, OneDrive, Teamgroepen als SharePoint-sites hebt geselecteerd, is het uitvoerbestand een archief in *ZIP*-indeling met daarin PDF- of *CSV*-rapportbestanden.
Bewerken	Configuratie van een bestaand rapport bewerken.
Verwijderen	Geselecteerd rapport volledig verwijderen.

Als u rapporten wilt filteren, klikt u op **Filter toevoegen** en selecteert u een filtertype in het vervolgkeuzemenu of voert u een tekenreeks in (herhaal dit als u meerdere criteria combineert):

Filter toevoegen	Syntaxis
Naam	Typ de gedeeltelijke of volledige naam van het rapport.
Gepland	Selecteer Niet gepland, Eenmalig, Dagelijks, Wekelijks of Maandelijks.
Gegevens	Selecteer Exchange Online, OneDrive, Teamgroepen of SharePoint-sites om op gegevens te filteren.

Quarantaine

Eenvoudig beheer van objecten (e-mails en bestanden) die door ESET Cloud Office Security in quarantaine zijn geplaatst. Schakel tussen Gmail, Google Drive, Exchange Online, OneDrive, Teamgroepen en SharePoint-sites via de tabbladen. U ziet belangrijke informatie over elk object.

Klik op het pictogram  om een zijbalk te openen met een overzicht van een specifiek object. Klik op het pictogram  en selecteer **Details weergeven** voor uitvoerige informatie.

Navigeer binnen de structuur om alleen detecties voor een bepaalde tenant of groep te zien. Klik op **Alles** als u alle detecties in elke tenant en groep wilt zien.

Inspecteer in quarantaine geplaatste e-mailberichten of bestanden en voer een actie uit (**Verwijderen** of **Vrijgeven**). U kunt ook het oorspronkelijke bestand of een met een wachtwoord beveiligd bestand in *.zip*-indeling **downloaden**.

Wanneer u een detectie niet als schadelijk beoordeelt (m.a.w. het gaat om een vals-positieve detectie), kunt u het bestand uit quarantaine **vrijgeven**. Een vrijgegeven bestand wordt automatisch op een witte lijst geplaatst, op basis van een hash. Alle toekomstige gebeurtenissen van hetzelfde bestand, voor dezelfde gebruiker, worden niet als verdacht gedetecteerd en worden niet in quarantaine geplaatst. Automatisch op de witte lijst plaatsen vindt per gebruiker plaats. Voor andere gebruikers wordt hetzelfde bestand nog steeds als verdacht gedetecteerd en in quarantaine geplaatst.
Met de optie **Van witte lijst verwijderen** kunt u een bestand van de witte lijst verwijderen in Detecties.

Klik op het pictogram en selecteer een actie:

Actie	Syntaxis
Details weergeven	Geeft uitvoerige informatie weer over het e-mailbericht dat in quarantaine is geplaatst.
Vrijgeven (e-mails of bestanden)	Hiermee geeft u e-mail vrij aan de oorspronkelijke ontvanger(s) in de vorm van een e-mailmelding van Quarantaine met het oorspronkelijke bericht als bijlage. In het geval van een OneDrive-item wordt het bestand geüpload naar de oorspronkelijke locatie in de OneDrive van de gebruiker. Wanneer u een bestand vrijgeeft van een Teamgroep of SharePoint-site, wordt het bestand weer weergegeven op de oorspronkelijke locatie. Een vrijgegeven bestand wordt automatisch op een witte lijst geplaatst, op basis van een hash. Hiermee wordt voorkomen dat het bestand opnieuw in quarantaine wordt geplaatst.
Verwijderen	Verwijdert item uit quarantaine.
Oorspronkelijk bestand downloaden	Niet-beveiligd bestand in de oorspronkelijke vorm downloaden.
Met een wachtwoord beveiligd archief downloaden	Met wachtwoord beveiligd archief downloaden.
Sample verzenden	In het dialoogvenster voor het verzenden van samples kunt u een verdacht bestand of spam ter analyse naar ESET verzenden. Kies een Reden voor verzenden van een sample in het vervolgkeuzemenu.

Als u het zoeken naar een bepaald in quarantaine geplaatst object gemakkelijker wilt maken, kunt u filteren op meerdere criteria. Klik op **Filter toevoegen** en selecteer het filtertype in het vervolgkeuzemenu of voer een tekenreeks in (herhaal dit wanneer u criteria combineert):

Filter toevoegen	Syntaxis
Vond plaats van	Geef een bereik voor Datum vanaf op.
Vond plaats tot	Geef een bereik voor Datum tot op.
Onderwerp	Is van toepassing op berichten die een specifieke tekenreeks (of een reguliere expressie) wel of niet in het onderwerp bevatten.
Bericht-id	Filter e-mailberichten op unieke bericht-id bij het zoeken naar een specifiek bericht, vooral in grote logboeken met veel berichten of bij meerdere bezorgingspogingen.
Van	Berichten filteren op een specifieke afzender.
Tot	Berichten filteren op ontvangers.
Postvak	Is van toepassing op berichten die zich in een specifiek postvak bevinden.
Scanresultaat	Selecteer een van de volgende opties: Malware, -malware (gedetecteerd door ESET LiveGuard Advanced), phishing of spam.
Team	Typ de geldige teamnaam.
Object	Typ een geldige objectnaam.
Site	Typ een geldige sitenaam.

De bewaarperiode voor in quarantaine geplaatste objecten is 30 dagen. Objecten die ouder zijn dan 30 dagen worden definitief uit quarantaine verwijderd.

Scanlogboeken

Geeft alle scanresultaten van ESET Cloud Office Security weer. Logboeken zijn vergelijkbaar met Detecties, maar bovendien kunt u opgeschoonde objecten in de lijst opnemen (activeer in de beleidsregels de instelling Alle objecten in logbestand registreren). Schakel met behulp van de tabbladen tussen Gmail, Google Drive, Exchange Online, OneDrive, Teamgroepen, SharePoint-sites en ingediende bestanden. U kunt een aanzienlijke hoeveelheid informatie zien voor elke detectie. Ingediende bestanden is een lijst met bestanden die ter analyse bij ESET LiveGuard Advanced zijn ingediend.

Klik op het pictogram  om een zijbalk te openen met een overzicht van een specifieke logboekrecord. Klik op het pictogram  en selecteer **Details weergeven** voor uitvoerige informatie.

Navigeer in de structuur om alleen logboekrecords voor een bepaalde tenant of groep te zien. Klik op **Alles** als u alle detecties in elke tenant en groep wilt zien.

> Als een scanresultaat **Niet gescand** is, kan de reden variëren. Zie Beperkingen voor meer informatie.

Wanneer u rechtsboven op het tandwielpictogram  klikt om **Exporteren naar CSV** te openen in het contextmenu, kunt u het tabelraster exporteren in *CSV*-indeling en dit in andere toepassingen gebruiken om met de lijst te werken.

Als u het zoeken naar een bepaalde logboekrecord gemakkelijker wilt maken, kunt u filteren op meerdere criteria. Klik op **Filter toevoegen** en selecteer het filtertype in het vervolgkeuzemenu of voer een tekenreeks in (herhaal dit wanneer u criteria combineert):

Filter toevoegen	Syntaxis
Vond plaats van	Geef een bereik voor Datum vanaf op.
Vond plaats tot	Geef een bereik voor Datum tot op.
Gegevensbron	Selecteer een van de volgende opties: Exchange Online, OneDrive, Teamgroep en SharePoint-site.
Postvak	Is van toepassing op berichten die zich in een specifiek postvak bevinden.
Van	Berichten filteren op een specifieke afzender.
Tot	Berichten filteren op ontvangers.
Onderwerp	Is van toepassing op berichten die al dan niet een specifieke tekenreeks bevatten in het onderwerp.
Bericht-id	Filter e-mailberichten op unieke bericht-id bij het zoeken naar een specifiek bericht, vooral in grote logboeken met veel berichten of bij meerdere bezorgingspogingen.
Scanresultaat	Selecteer een van de volgende opties: Malware, -malware (beveiligd door ESET LiveGuard Advanced), phishing, spam, schoon, niet gescand, fout of uitgeschakeld.
Actie	Selecteer een van de beschikbare acties.
Eigenaren	Typ de geldige naam van de eigenaar.
Object	Typ een geldige objectnaam.
Detectie	Typ een geldige detectienaam.
Hash	Typ een geldige detectiehash.
Team	Typ een geldige teamnaam.
Site	Typ een geldige sitenaam.

Er is een retentieperiode van 90 dagen voor logboekrecords. Records ouder dan 90 dagen worden definitief verwijderd. Als u beleid hanteert dat **alle objecten registreert**, worden logboekrecords met het scanresultaat **Schoon** 3 dagen bewaard. Schone scanresultaten ouder dan 3 dagen worden definitief verwijderd.

Beleid

Grote organisaties hebben doorgaans meerdere afdelingen en willen per organisatie-eenheid verschillende beveiligingsinstellingen kunnen configureren. ESET Cloud Office Security biedt op beleid gebaseerde beveiligingsinstellingen die u kunt aanpassen aan uw behoeften en die u kunt toewijzen aan geselecteerde gebruikers en gebruikersgroepen, tenants, teamgroepen en SharePoint-sites.

Als u filtercriteria wilt toevoegen, klikt u op **Filter toevoegen**, selecteert u de toepasselijke **itemnaam** en typt u een geldige beleidsnaam. In de structuur van Beleid worden Tenants en hun groepen, Teamgroepen of SharePoint-sites weergegeven, waaronder een groep genaamd **Niet toegewezen** met aangepaste beleidsregels die aan geen enkel doel zijn toegewezen.

U kunt nieuw beleid toevoegen, of bestaand beleid en bijbehorende instellingen wijzigen:

1. Klik op **Beleid** > **Nieuw beleid**.

2. Typ **Naam** en **Beschrijving** voor een nieuw beleid.

3. Selecteer een doel en configureer beleid voor:

   • **Tenants** – Gmail, Google Drive, Exchange Online, OneDrive, SharePoint-sites en teamgroepbeveiliging instellen en toewijzen aan geselecteerde tenants

   • **Gebruikers** – Gmail, Google Drive, Exchange Online- en OneDrive-beveiliging en toewijzen aan geselecteerde gebruikers of een of meer gebruikersgroepen

   • **Teamgroepen** – Beveiliging van teamgroepen instellen en toewijzen aan geselecteerde teamgroepen

   • **SharePoint-sites** – Beveiliging van SharePoint-sites instellen en toewijzen aan geselecteerde sites

4. Pas de **Instellingen** van de beveiliging aan voor Exchange Online, Gmail, OneDrive, Google Drive, Teamgroepen, SharePoint-sites of ESET LiveGuard Advanced en klik op **Volgende**.

5. Klik op **Toewijzen** en kies een doel waaraan u het beleid wilt toewijzen.

6. Klik op **Wijzigingen opslaan** om de beleidsinstelling op te slaan.

Beleidsbeginselen

Standaardbeleid
- Van toepassing op alle gebruikers (beveiligd en niet beveiligd)
- Kan niet worden gewijzigd of verwijderd

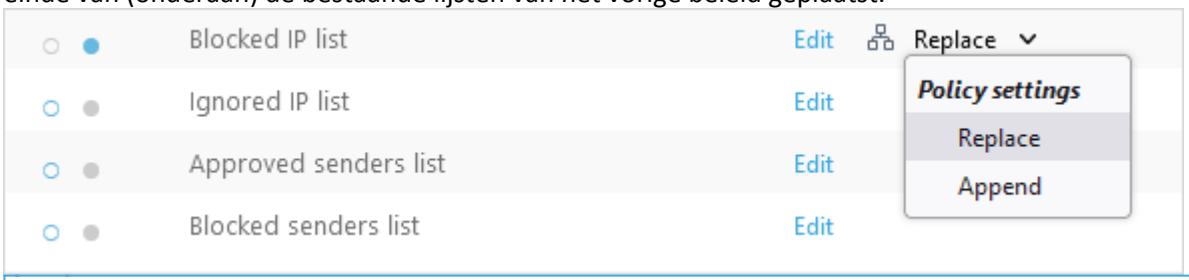
Aangepast beleid kan worden toegewezen aan:
- **Gebruikers** — is van toepassing op handmatig geselecteerde individuele gebruikers
- **Groepen** – beleid dat van toepassing is op alle leden van de gebruikersgroep
- **Tenants** — beleid dat van toepassing is op alle entiteiten binnen de tenant
- **Teamgroepen** – beleid dat van toepassing is op een teamgroep
- **SharePoint-sites** – is van toepassing op een SharePoint-site

Aangepast beleid dat aan een **tenant** of **groep** is toegewezen, wordt samengevoegd met het standaardbeleid
Aangepast **Tenantbeleid**, **Groepsbeleid**, **Teamgroepbeleid** of **SharePoint-sitesbeleid** heeft voorrang op het standaardbeleid
Aangepast beleid dat aan een **Gebruiker** is toegewezen, wordt samengevoegd met het beleid voor **Tenant**, **Groep**, **Teamgroepen**, **SharePoint-sites** en het standaardbeleid
Een aangepast **gebruikersbeleid** heeft voorrang op een tenant- of groepsbeleid en een standaardbeleid.
Wanneer een gebruiker echter een bestand uploadt naar Teamgroep of een SharePoint-site, wordt het beleid voor de Teamgroep of SharePoint-site toegepast.

Aan gebruikers en tenants kunnen meerdere **aangepaste beleidsregels** worden toegewezen, maar het effectieve beleid wordt berekend op basis van de prioriteit (volgorde).

Instelling voor antispamlijsten bij het samenvoegen van beleid

De samenvoegoptie is van toepassing op de instellingen voor Antispamlijsten en Beheerder op de hoogte stellen (adressen voor e-mails met meldingen van anti-malware en anti-phishing).
Wanneer u meerdere beleidsregels hebt met antispamlijsten (goedgekeurde, geblokkeerde en genegeerde lijsten met IP-adressen, domeinen of e-mailadressen) of anti-malware- en anti-phishing-beheerdersadressen voor e-mails met meldingen, kiest u de volgende samenvoegstrategie:
Vervangen: bewaar alleen de nieuwe lijstvermeldingen (standaardoptie). Alle lijsten uit het vorige beleid worden vervangen door de nieuwe lijstvermeldingen van het huidige beleid.
Toevoegen: breid lijsten van het vorige beleid uit door nieuwe vermeldingen toe te voegen. Voeg lijsten uit het vorige beleid samen met nieuwe vermeldingen van het huidige beleid. De nieuwe vermeldingen worden aan het einde van (onderaan) de bestaande lijsten van het vorige beleid geplaatst.



Het standaardgedrag was **Vervangen**, maar u kunt nu ook kiezen voor de samenvoegoptie. Als u al beleid met specifieke antispamlijsten hebt, kunt u de standaardoptie **Vervangen** blijven gebruiken of deze wijzigen in **Toevoegen**.

Maak een nieuw beleid met een gedefinieerde antispamlijst en selecteer de samenvoegoptie (indien er bestaand beleid met antispamlijsten is).
1. Klik op **Beleid** > **Nieuw beleid**.
2. Typ een **Naam** en **Beschrijving** voor het nieuwe beleid, selecteer **Tenants** als doel en klik op **Volgende**.
3. Vouw **Exchange Online Anti-Spam** uit en klik op **Bewerken** naast de lijst met geblokkeerde IP-adressen.
4. Klik op **Toevoegen**, typ het IP-adres, druk op **Enter** om de actie te voltooien (u kunt de lijst ook uit een bestand importeren) en klik op **Wijzigingen opslaan**.
5. Kies **Toevoegen** als samenvoegoptie in het vervolgkeuzemenu en klik op **Volgende**.
6. Klik op **Toewijzen**, kies **Toewijzen aan tenants** in het vervolgkeuzemenu, schakel het selectievakje naast de tenant in en klik op **OK**.
7. Klik op **Wijzigingen opslaan** om het proces te voltooien.

Als u de prioriteit van beleid wilt wijzigen, klikt u op **Volgorde wijzigen**. Selecteer beleid of meerdere beleidsregels en klik op **Eerder toepassen** of **Later toepassen** om de prioriteit ervan te wijzigen. Beleidsregels worden over het algemeen (ongeacht toewijzing – tenant, groep of gebruiker) in een bepaalde volgorde van boven naar beneden toegepast. Het standaardbeleid wordt altijd als eerste toegepast.

Als u de volgende acties wilt uitvoeren, selecteert u het beleid en klikt u op het pictogram :

Actie	Syntaxis
Details weergeven	Geef gedetailleerde informatie weer over een gemaakt beleid, instellingen en de personen aan wie het beleid is toegewezen.
Bewerken	De configuratie van bestaand beleid aanpassen.
Toewijzen	Selecteer Gebruikers, Tenants, Teamgroepen of SharePoint-sites waarop het beleid van toepassing is.
Duplicaat	Maak nieuw beleid op basis van de geselecteerde sjabloon. Er is een nieuwe naam vereist voor het dubbele beleid.
Verwijderen	Verwijder het geselecteerde beleid volledig.

Maak een aangepast tenantbeleid om alle scanresultaten (waaronder schone resultaten) te bekijken in Scanlogboeken. Tenantbeleid is van toepassing op alle gebruikers (beveiligd en niet beveiligd).
1. Klik op **Beleid** > **Nieuw beleid**.
2. Typ een **Naam** en **Beschrijving** voor het nieuwe beleid, selecteer **Tenants** als doel en klik op **Volgende**.
3. Vouw **Exchange Online Algemeen** uit en klik op de schakelaar als u **Alle objecten in logbestand registreren** wilt inschakelen.
4. Vouw **OneDrive Algemeen** uit en klik op de schakelaar als u **Alle objecten in logbestand registreren** wilt inschakelen.
5. Vouw **Teamgroepen Algemeen** uit en klik op de schakelaar als u **Alle objecten in logbestand registreren** wilt inschakelen.
6. Vouw **SharePoint-sites Algemeen** uit en klik op de schakelaar als u **Alle objecten in logbestand registreren** wilt inschakelen. Klik vervolgens op **Volgende**.
7. Klik op **Toewijzen**, schakel het selectievakje naast de tenant in en klik vervolgens op **OK**.
8. Klik op **Wijzigingen opslaan** om het proces te voltooien.

Maak aangepast beleid voor specifieke gebruikers met geavanceerde instellingen die van invloed zijn op de manier waarop malware, spam en phishing worden verwerkt. Met dit beleid worden e-mailbijlagen verwijderd waarin malware is verborgen, worden spamberichten verplaatst naar de map met ongewenste e-mail van de gebruiker, wordt bij phishingmails een tag aan het onderwerp toegevoegd en worden ze in quarantaine geplaatst, en wordt de inhoud van malwarebestanden op OneDrive vervangen door platte tekst om schade te voorkomen.

1. Klik op **Beleid** > **Nieuw beleid**.
2. Typ een **Naam** en **Beschrijving** voor het nieuwe beleid, selecteer **Gebruikers** als doel en klik op **Volgende**.
3. Vouw **Exchange Online Anti-Malware** uit en gebruik het vervolgkeuzemenu naast **Wanneer items worden gedetecteerd** om **Bijlage verwijderen** te selecteren.
4. Vouw **Exchange Online Anti-Spam** uit en gebruik het vervolgkeuzemenu naast **Wanneer items worden gerapporteerd** om **Verplaatsen naar Ongewenste e-mail** te selecteren.
5. Vouw **Exchange Online Anti-Phishing** uit en klik op de schakelaar als u **Onderwerp taggen** wilt inschakelen. U kunt **Onderwerptekst taggen** ook wijzigen als u deze optie wilt aanpassen.
6. Vouw **OneDrive Online Anti-Malware** uit, gebruik het vervolgkeuzemenu naast **Wanneer items worden gerapporteerd** om **Vervangen** te selecteren en klik op **Volgende**.
7. Klik op **Toewijzen**, schakel selectievakjes in naast de gebruikers waarop u het beleid wilt toepassen en klik op **OK**. Als een gebruiker bestaand aangepast beleid heeft toegepast, wordt dat overschreven door het nieuwe beleid.
8. Klik op **Wijzigingen opslaan** om het proces te voltooien.

Beveiligingsinstellingen voor Exchange Online

In dit gedeelte vindt u informatie over het wijzigen van instellingen en opties voor Exchange Online Algemeen, Anti-Malware, Anti-Spam of Anti-Phishing.

Exchange Online Algemeen

ESET LiveGrid®Feedback voor
Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Lees meer over ESET LiveGrid® in de woordenlijst .
Alle objecten in logbestand registreren
Als deze optie is geselecteerd, worden alle scanresultaten (waaronder schone resultaten) weergegeven in Scanlogboeken. Het bewaarbeleid voor schone scanresultaten is drie dagen. Scanresultaten ouder dan drie dagen worden definitief verwijderd.

Exchange Online Anti-Malware

Exchange Online Anti-Malware inschakelen
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Rapportage en beveiliging door zelflerende systemen
Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees het volgende voordat u een drempelwaarde (of niveau) voor categorie rapportage.
Wanneer items worden gerapporteerd
- **Geen actie**: er wordt geen actie ondernomen en de e-mail wordt bij de beoogde ontvanger bezorgd
- **Verplaatsen naar Ongewenste e-mail**: de e-mail wordt verplaatst naar de map Ongewenste e-mail.
- **Verplaatsen naar Prullenbak**: de e-mail wordt verplaatst naar map Prullenbak.
- **Bericht verwijderen**: de e-mail wordt verwijderd
- **Bericht in quarantaine plaatsen**: de oorspronkelijke e-mail wordt verwijderd en een kopie van de e-mail wordt opgeslagen in quarantaine. Als u besluit de e-mail in quarantaine vrij te geven, wordt deze als bijlage in een nieuwe e-mail verzonden en bij de ontvanger bezorgd.
- **Bijlage verwijderen**: de bijlage wordt verwijderd en het bericht wordt zonder bijlage bezorgd bij de ontvanger.
- **Bijlage vervangen**: de bijlage wordt vervangen door een tekstbestand met uitvoerige informatie over de actie die is ondernomen.
- **Bijlage in quarantaine plaatsen** — De bijlage wordt uit de e-mail verwijderd en in bestandsquarantaine geplaatst.

Vervangende tekst voor bijlagen
Vervangt de bijlage door een tekstbestand met uitvoerige informatie over een actie die is ondernomen.
Onderwerp taggen
Indien ingeschakeld, kunt u sjablonen wijzigen die zijn toegevoegd aan het onderwerp van geïnfecteerde berichten.
Onderwerptekst taggen
U kunt een aangepaste tag toevoegen aan de onderwerpen van de desbetreffende berichten.
Eigenaar van postvak op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Taal
Kies de gewenste taal in het vervolgkeuzemenu. De eigenaar van het postvak ontvangt e-mails met meldingen in de geselecteerde taal wanneer een object wordt vrijgegeven uit de quarantaine van Exchange Online. Deze optie negeert de standaardtaal voor de tenant in Instellingen.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Exchange Online Anti-Spam

Exchange Online Anti-Spam inschakelen
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Wanneer items worden gerapporteerd
- **Geen actie**: er wordt geen actie ondernomen en de e-mail wordt bij de beoogde ontvanger bezorgd
- **Verplaatsen naar Ongewenste e-mail**: de e-mail wordt verplaatst naar de map Ongewenste e-mail.
- **Verplaatsen naar Prullenbak**: de e-mail wordt verplaatst naar map Prullenbak.
- **Bericht verwijderen**: de e-mail wordt verwijderd
- **Bericht in quarantaine plaatsen**: de oorspronkelijke e-mail wordt verwijderd en een kopie van de e-mail wordt opgeslagen in quarantaine. Als u besluit de e-mail in quarantaine vrij te geven, wordt deze als bijlage in een nieuwe e-mail verzonden en bij de ontvanger bezorgd.

Onderwerp taggen
Indien ingeschakeld, kunt u sjablonen wijzigen die zijn toegevoegd aan het onderwerp van geïnfecteerde berichten.
Onderwerptekst taggen
U kunt een aangepaste tag toevoegen aan de onderwerpen van de desbetreffende berichten.
U kunt de lijsten **Goedgekeurd**, **Geblokkeerd** en **Genegeerd** configureren door criteria op te geven, zoals IP-adres of bereik, domeinnaam, enz. Klik op **Bewerken** voor de lijst die u wilt beheren als u criteria wilt toevoegen, aanpassen of verwijderen. U kunt uw aangepaste lijst ook importeren vanuit een bestand in plaats van elke vermelding handmatig toe te voegen. Klik hiertoe op **Importeren** en blader naar het bestand (*.txt*) dat de vermeldingen bevat die u aan de lijst wilt toevoegen. Als u uw bestaande lijst naar een bestand (*.txt*) wilt exporteren, gaat u op soortgelijke wijze te werk, maar selecteert u **Exporteren** in het contextmenu.

Lijst met goedgekeurde IP-adressen	Plaatst e-mails die afkomstig zijn van opgegeven IP-adressen automatisch op de witte lijst. E-mailinhoud wordt niet gecontroleerd.
Lijst met geblokkeerde IP-adressen	Blokkeert automatisch e-mails die afkomstig zijn van opgegeven IP-adressen.
Lijst met genegeerde IP-adressen	Lijst met IP-adressen die tijdens classificatie worden genegeerd. E-mailinhoud wordt gecontroleerd.
Lijst met goedgekeurde afzenders	Plaatst e-mailadres van een bepaalde afzender of domein op de witte lijst. Er wordt slechts één afzenderadres of een heel domein gebruikt voor verificatie op basis van de volgende prioriteit: 1.SMTP 'MAIL FROM'-adres 2."Return-Path:" e-mailkopveld 3."X-Env-Sender:" e-mailkopveld 4."Van:" e-mailkopveld 5."Afzender:" e-mailkopveld 6."X-Apparently-From:" e-mailkopveld
Lijst met geblokkeerde afzenders	Blokkeert e-mailadres van een bepaalde afzender of een be[aald domein. Alle geïdentificeerde afzenderadressen of hele domeinen worden gebruikt voor verificatie: SMTP 'MAIL FROM'-adres "Return-Path:" e-mailkopveld "X-Env-Sender:" e-mailkopveld "Van:" e-mailkopveld "Afzender:" e-mailkopveld "X-Apparently-From:" e-mailkopveld

Exchange Online Anti-Phishing

Exchange Online Anti-Phishing inschakelen
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Wanneer items worden gerapporteerd
• **Geen actie** — Er wordt geen actie ondernomen en e-mails met schadelijke bijlagen worden bij de ontvanger bezorgd.
• **Verplaatsen naar Ongewenste e-mail**: de e-mail wordt verplaatst naar de map Ongewenste e-mail.
• **Verplaatsen naar Prullenbak**: de e-mail wordt verplaatst naar map Prullenbak.
• **Bericht verwijderen**: de e-mail wordt verwijderd
• **Bericht in quarantaine plaatsen**: de oorspronkelijke e-mail wordt verwijderd en een kopie van de e-mail wordt opgeslagen in quarantaine. Als u besluit de e-mail in quarantaine vrij te geven, wordt deze als bijlage in een nieuwe e-mail verzonden en bij de ontvanger bezorgd.
Onderwerp taggen
Indien ingeschakeld, kunt u sjablonen wijzigen die zijn toegevoegd aan het onderwerp van geïnfecteerde berichten.
Onderwerptekst taggen
U kunt een aangepaste tag toevoegen aan de onderwerpen van de desbetreffende berichten.
Eigenaar van postvak op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Beheerder op de hoogte stellen
Geef het e-mailadres op (druk op Enter om meerdere adressen toe te voegen) waarop e-mails met meldingen moeten worden ontvangen wanneer er een detectie wordt gevonden voor een Exchange Online-gebruiker.

Beveiligingsinstellingen voor Gmail

In dit gedeelte vindt u informatie over het wijzigen van instellingen en opties voor Gmail Algemeen, Anti-Malware, Anti-Spam of Anti-Phishing.

Gmail Algemeen

ESET LiveGrid®Feedback voor
Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Lees meer over ESET LiveGrid® in de woordenlijst .
Alle objecten in logbestand registreren
Als deze optie is geselecteerd, worden alle scanresultaten (waaronder schone resultaten) weergegeven in Scanlogboeken. Het bewaarbeleid voor schone scanresultaten is drie dagen. Scanresultaten ouder dan drie dagen worden definitief verwijderd.

Gmail Anti-Malware

Gmail Anti-Malware inschakelen
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Rapportage en beveiliging door zelflerende systemen
Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees het volgende voordat u een drempelwaarde (of niveau) voor categorie rapportage.
Wanneer items worden gerapporteerd
- **Geen actie**: er wordt geen actie ondernomen en de e-mail wordt bij de beoogde ontvanger bezorgd
- **Verplaatsen naar Ongewenste e-mail**: de e-mail wordt verplaatst naar de map Ongewenste e-mail.
- **Verplaatsen naar Prullenbak**: de e-mail wordt verplaatst naar map Prullenbak.
- **Bericht verwijderen**: de e-mail wordt verwijderd
- **Bericht in quarantaine plaatsen**: de oorspronkelijke e-mail wordt verwijderd en een kopie van de e-mail wordt opgeslagen in quarantaine. Als u besluit de e-mail in quarantaine vrij te geven, wordt deze als bijlage in een nieuwe e-mail verzonden en bij de ontvanger bezorgd.
- **Bijlage verwijderen**: de bijlage wordt verwijderd en het bericht wordt zonder bijlage bezorgd bij de ontvanger.
- **Bijlage vervangen**: de bijlage wordt vervangen door een tekstbestand met uitvoerige informatie over de actie die is ondernomen.
- **Bijlage in quarantaine plaatsen** — De bijlage wordt uit de e-mail verwijderd en in bestandsquarantaine geplaatst.

Vervangende tekst voor bijlagen
Vervangt de bijlage door een tekstbestand met uitvoerige informatie over een actie die is ondernomen.
Onderwerp taggen
Indien ingeschakeld, kunt u sjablonen wijzigen die zijn toegevoegd aan het onderwerp van geïnfecteerde berichten.
Onderwerptekst taggen
U kunt een aangepaste tag toevoegen aan de onderwerpen van de desbetreffende berichten.
Eigenaar van postvak op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Taal
Kies de gewenste taal in het vervolgkeuzemenu. De eigenaar van het postvak ontvangt e-mails met meldingen in de geselecteerde taal wanneer een object wordt vrijgegeven uit de quarantaine. Deze optie negeert de standaardtaal voor de tenant in Instellingen.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Gmail Anti-Spam

Gmail Anti-Spam inschakelen
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Wanneer items worden gerapporteerd
- **Geen actie**: er wordt geen actie ondernomen en de e-mail wordt bij de beoogde ontvanger bezorgd
- **Verplaatsen naar Ongewenste e-mail**: de e-mail wordt verplaatst naar de map Ongewenste e-mail.
- **Verplaatsen naar Prullenbak**: de e-mail wordt verplaatst naar map Prullenbak.
- **Bericht verwijderen**: de e-mail wordt verwijderd
- **Bericht in quarantaine plaatsen**: de oorspronkelijke e-mail wordt verwijderd en een kopie van de e-mail wordt opgeslagen in quarantaine. Als u besluit de e-mail in quarantaine vrij te geven, wordt deze als bijlage in een nieuwe e-mail verzonden en bij de ontvanger bezorgd.

Onderwerp taggen
Indien ingeschakeld, kunt u sjablonen wijzigen die zijn toegevoegd aan het onderwerp van geïnfecteerde berichten.
Onderwerptekst taggen
U kunt een aangepaste tag toevoegen aan de onderwerpen van de desbetreffende berichten.
U kunt de lijsten **Goedgekeurd**, **Geblokkeerd** en **Genegeerd** configureren door criteria op te geven, zoals IP-adres of bereik, domeinnaam, enz. Klik op **Bewerken** voor de lijst die u wilt beheren als u criteria wilt toevoegen, aanpassen of verwijderen. U kunt uw aangepaste lijst ook importeren vanuit een bestand in plaats van elke vermelding handmatig toe te voegen. Klik hiertoe op **Importeren** en blader naar het bestand (*.txt*) dat de vermeldingen bevat die u aan de lijst wilt toevoegen. Als u uw bestaande lijst naar een bestand (*.txt*) wilt exporteren, gaat u op soortgelijke wijze te werk, maar selecteert u **Exporteren** in het contextmenu.

Lijst met goedgekeurde IP-adressen	Plaatst e-mails die afkomstig zijn van opgegeven IP-adressen automatisch op de witte lijst. E-mailinhoud wordt niet gecontroleerd.
Lijst met geblokkeerde IP-adressen	Blokkeert automatisch e-mails die afkomstig zijn van opgegeven IP-adressen.
Lijst met genegeerde IP-adressen	Lijst met IP-adressen die tijdens classificatie worden genegeerd. E-mailinhoud wordt gecontroleerd.
Lijst met goedgekeurde afzenders	Plaatst e-mailadres van een bepaalde afzender of domein op de witte lijst. Er wordt slechts één afzenderadres of een heel domein gebruikt voor verificatie op basis van de volgende prioriteit: 1.SMTP 'MAIL FROM'-adres 2."Return-Path:" e-mailkopveld 3."X-Env-Sender:" e-mailkopveld 4."Van:" e-mailkopveld 5."Afzender:" e-mailkopveld 6."X-Apparently-From:" e-mailkopveld
Lijst met geblokkeerde afzenders	Blokkeert e-mailadres van een bepaalde afzender of een be[aald domein. Alle geïdentificeerde afzenderadressen of hele domeinen worden gebruikt voor verificatie: SMTP 'MAIL FROM'-adres "Return-Path:" e-mailkopveld "X-Env-Sender:" e-mailkopveld "Van:" e-mailkopveld "Afzender:" e-mailkopveld "X-Apparently-From:" e-mailkopveld

Gmail Anti-Phishing

Gmail Anti-Phishing inschakelen
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Wanneer items worden gerapporteerd
• **Geen actie** — Er wordt geen actie ondernomen en e-mails met schadelijke bijlagen worden bij de ontvanger bezorgd.
• **Verplaatsen naar Ongewenste e-mail**: de e-mail wordt verplaatst naar de map Ongewenste e-mail.
• **Verplaatsen naar Prullenbak**: de e-mail wordt verplaatst naar map Prullenbak.
• **Bericht verwijderen**: de e-mail wordt verwijderd
• **Bericht in quarantaine plaatsen**: de oorspronkelijke e-mail wordt verwijderd en een kopie van de e-mail wordt opgeslagen in quarantaine. Als u besluit de e-mail in quarantaine vrij te geven, wordt deze als bijlage in een nieuwe e-mail verzonden en bij de ontvanger bezorgd.
Onderwerp taggen
Indien ingeschakeld, kunt u sjablonen wijzigen die zijn toegevoegd aan het onderwerp van geïnfecteerde berichten.
Onderwerptekst taggen
U kunt een aangepaste tag toevoegen aan de onderwerpen van de desbetreffende berichten.
Eigenaar van postvak op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Beveiligingsinstellingen voor OneDrive

In dit gedeelte vindt u informatie over het wijzigen van instellingen en opties voor OneDrive Algemeen of OneDrive Anti-Malware.

OneDrive Algemeen

ESET LiveGrid®Feedback voor
Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Zie de woordenlijst voor meer informatie over deze toepassingen.
Alle objecten in logbestand registreren
Als deze optie is geselecteerd, worden alle scanresultaten (waaronder schone resultaten) weergegeven in Scanlogboeken. Het bewaarbeleid voor schone scanresultaten is drie dagen. Scanresultaten ouder dan drie dagen worden definitief verwijderd.

OneDrive Anti-Malware

OneDrive Anti-Malware
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Rapportage en beveiliging door zelflerende systemen
Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees het volgende voordat u een drempelwaarde (of niveau) voor categorie rapportage.
Wanneer items worden gerapporteerd
- **Geen actie**: er wordt geen actie uitgevoerd en het bestand blijft op OneDrive staan
- **Verplaatsen naar Prullenbak**: het bestand wordt verplaatst naar de Prullenbak.
- **Vervangen**: de inhoud van het oorspronkelijke bestand wordt vervangen door tekst die hieronder is gedefinieerd in het veld Vervangende tekst voor bestanden.
- **Quarantaine**: het oorspronkelijke bestand wordt verplaatst naar de Prullenbak en gekopieerd naar quarantaine. Wanneer het bestand wordt vrijgegeven, blijft het eerder verwijderde bestand in de Prullenbak staan en wordt er een nieuwe kopie naar de oorspronkelijke OneDrive-map geüpload.

Vervangende tekst voor bestanden
Vervangt de bijlage door een tekstbestand met uitvoerige informatie over een actie die is ondernomen.
Eigenaar op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Beveiligingsinstellingen voor Google Drive

In dit gedeelte vindt u informatie over het wijzigen van instellingen en opties voor Google Drive Algemeen of Google Drive Anti-Malware.

Google Drive Algemeen

ESET LiveGrid®Feedback voor
Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Zie de woordenlijst voor meer informatie over deze toepassingen.
Alle objecten in logbestand registreren
Als deze optie is geselecteerd, worden alle scanresultaten (waaronder schone resultaten) weergegeven in Scanlogboeken. Het bewaarbeleid voor schone scanresultaten is drie dagen. Scanresultaten ouder dan drie dagen worden definitief verwijderd.

Google Drive Anti-Malware

Google Drive Anti-Malware
Wanneer deze functie is ingeschakeld, kunt u gedetailleerde opties configureren.
Rapportage en beveiliging door zelflerende systemen
Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees het volgende voordat u een drempelwaarde (of niveau) voor categorie rapportage.
Wanneer items worden gerapporteerd
- **Geen actie**: er wordt geen actie uitgevoerd en het bestand blijft op Google Drive staan
- **Verplaatsen naar Prullenbak**: het bestand wordt verplaatst naar de Prullenbak.
- **Vervangen**: de inhoud van het oorspronkelijke bestand wordt vervangen door tekst die hieronder is gedefinieerd in het veld Vervangende tekst voor bestanden.
- **Quarantaine**: het oorspronkelijke bestand wordt verplaatst naar de Prullenbak en gekopieerd naar quarantaine.
- **Verwijderen**: het oorspronkelijke bestand wordt permanent verwijderd uit Google Drive.

Vervangende tekst voor bestanden
Vervangt de bijlage door een tekstbestand met uitvoerige informatie over een actie die is ondernomen.
Eigenaar op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Beveiligingsinstellingen voor Teamgroepen

In dit gedeelte vindt u informatie over het wijzigen van instellingen en opties voor Teamgroepen Algemeen of Teamgroepen Anti-Malware.

Teamgroepen Algemeen

ESET LiveGrid®Feedback voor
Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Zie de woordenlijst voor meer informatie over deze typen toepassingen.
Alle objecten in logbestand registreren
Als deze optie is geselecteerd, worden alle scanresultaten (waaronder schone resultaten) weergegeven in Scanlogboeken. Het bewaarbeleid voor schone scanresultaten is drie dagen. Scanresultaten ouder dan drie dagen worden definitief verwijderd.

Teamgroepen Anti-Malware

Teamgroepen Anti-Malware
Indien deze functie is ingeschakeld, is deze functie actief en kunt u gedetailleerde opties configureren.
Rapportage en beveiliging door zelflerende systemen
Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees het volgende voordat u een drempelwaarde (of niveau) voor categorie rapportage.
Wanneer items worden gerapporteerd
- **Geen actie** — Er wordt geen actie uitgevoerd. Het bestand blijft onveranderd.
- **Verplaatsen naar Prullenbak** — Het bestand wordt verplaatst naar de Prullenbak van Teams.
- **Vervangen** — inhoud van het oorspronkelijke bestand wordt vervangen door tekst die hieronder is gedefinieerd in het veld Vervangende tekst voor bestanden.
- **Quarantaine** — Het oorspronkelijke bestand wordt verplaatst naar de Prullenbak van Teams en gekopieerd naar Quarantaine. Wanneer het bestand wordt vrijgegeven, blijft het eerder verwijderde bestand in de Prullenbak staan en wordt er een nieuwe kopie op de oorspronkelijke locatie teruggeplaatst.

Vervangende tekst voor bestanden
Vervangt de bijlage door een tekstbestand met uitvoerige informatie over een actie die is ondernomen.
Eigenaar op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Beveiligingsinstellingen voor SharePoint-sites

In dit gedeelte vindt u informatie over het wijzigen van instellingen en opties voor SharePoint-sites Algemeen of SharePoint-sites Anti-Malware.

SharePoint-sites Algemeen

ESET LiveGrid®Feedback voor
Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Zie de woordenlijst voor meer informatie over deze typen toepassingen.
Alle objecten in logbestand registreren
Als deze optie is geselecteerd, worden alle scanresultaten (waaronder schone resultaten) weergegeven in Scanlogboeken. Het bewaarbeleid voor schone scanresultaten is drie dagen. Scanresultaten ouder dan drie dagen worden definitief verwijderd.

SharePoint-sites Anti-Malware

SharePoint-sites Anti-Malware
Indien deze functie is ingeschakeld, is deze functie actief en kunt u gedetailleerde opties configureren.
Rapportage en beveiliging door zelflerende systemen
Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees het volgende voordat u een drempelwaarde (of niveau) voor categorie rapportage.
Wanneer items worden gerapporteerd
• **Geen actie** — Er wordt geen actie uitgevoerd. Het bestand blijft onveranderd.
• **Verplaatsen naar Prullenbak** — Het bestand wordt verplaatst naar de Prullenbak van SharePoint.
• **Vervangen** — inhoud van het oorspronkelijke bestand wordt vervangen door tekst die hieronder is gedefinieerd in het veld Vervangende tekst voor bestanden.
• **Quarantaine** — Het oorspronkelijke bestand wordt verplaatst naar de Prullenbak van SharePoint en gekopieerd naar Quarantaine. Wanneer het bestand wordt vrijgegeven, blijft het eerder verwijderde bestand in de Prullenbak staan en wordt er een nieuwe kopie op de oorspronkelijke locatie teruggeplaatst.
Vervangende tekst voor bestanden
Vervangt de bijlage door een tekstbestand met uitvoerige informatie over een actie die is ondernomen.
Eigenaar op de hoogte stellen
Indien ingeschakeld, ontvangt de gebruiker een e-mail met een melding wanneer er een detectie wordt gevonden.
Beheerder op de hoogte stellen
Geef een e-mailadres op waar u e-mails met meldingen wilt ontvangen in het geval van een detectie (druk op Enter als u meerdere adressen wilt toevoegen).

Beveiligingsinstellingen voor ESET LiveGuard Advanced

Als u de ESET LiveGuard Advanced-functie wilt gebruiken, moet u beleid configureren waarmee ESET LiveGuard Advanced-analyse mogelijk is. Gebruikers of groepen die aan dit beleid zijn toegewezen, worden extra beveiligd. Bestanden die ter analyse bij ESET LiveGuard Advanced worden ingediend, worden weergegeven op het tabblad Ingediende bestanden. Dit geldt voor onbekende (nooit eerder geziene) verdachte samples. Bekende schadelijke bestanden (op basis van hash) worden niet voor ESET LiveGuard Advanced-analyse verzonden.

U ziet de ESET LiveGuard Advanced-resultaten in de Scanlogboeken (Exchange Online, OneDrive, Teamgroepen of SharePoint-sites) en deze zijn gemarkeerd als malware.

ESET LiveGuard Advanced

Indien deze functie is ingeschakeld, is deze functie actief en kunt u gedetailleerde opties configureren.

ESET LiveGuard Advanced schakelt ESET LiveGrid®-feedback automatisch in. Gegevens worden voor verdere analyse naar het ESET Research Lab verzonden. Lees meer over ESET LiveGrid® in de woordenlijst .

Drempel voor detectie

Resultaten met een geselecteerd drempelniveau en hoger worden als bedreigingen beschouwd.

Verdachte samples automatisch indienen (vervolgkeuzemenu)

Deze instelling is verwant aan ESET LiveGrid® en maakt de volgende acties mogelijk: Alles, Alles behalve documenten, Geen.

Verdachte samples automatisch indienen (schuifregelaars)

Kies welke bestandstypen moeten worden ingediend bij ESET LiveGuard Advanced als ze verdachte code bevatten

die op een bedreiging lijkt of als ze ongebruikelijke kenmerken hebben of ongebruikelijk gedrag vertonen:

- **Uitvoerbare bestanden** – .exe, .dll, .sys
- **Archieven** – .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Scripts** – .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Anders** – .jar, .reg, .msi, .swf, .lnk

Verdachte samples van ESET-servers verwijderen

Kies wanneer u samples wilt verwijderen die ter analyse zijn ingediend. Verwijder samples uit de ESET LiveGuard Advanced-cloud: Nooit, Na 30 dagen, Onmiddellijk na analyse.

Documenten

Gebruik de schuifregelaar om toe te staan dat Microsoft Office-documenten, PDF's en andere documenttypen ter analyse naar ESET LiveGuard Advanced verzendt.

Documenten verwijderen van de servers van ESET

Samples van documentbestandsindelingen uit de ESET LiveGuard Advanced-cloud verwijderen: Nooit, Na 30 dagen, Onmiddellijk na analyse.

Rapportage en beveiliging door zelflerende systemen

Detectie-engine beschermt tegen schadelijke systeemaanvallen door bestanden, e-mails en netwerkcommunicatie te scannen. Als er een object wordt gedetecteerd dat als malware is geclassificeerd, wordt herstel ervan gestart. Detectie-engine kan het probleem oplossen door de detectie eerst te blokkeren en vervolgens actie te ondernemen, zoals opschonen, verwijderen of naar quarantaine verplaatsen.

Real-timebeveiliging en beveiliging door zelflerende systemen

Geavanceerde zelflerende systemen maken nu deel uit van de detectie-engine als een geavanceerde beveiligingslaag, waardoor de detectie verbetert. Lees meer over dit type beveiliging in de woordenlijst. U kunt Rapportageniveaus configureren in de volgende categorieën:

Malware

Een computervirus is een stuk schadelijke code dat aan het begin of einde van bestaande bestanden op uw computer wordt toegevoegd. Het woord 'virus' wordt echter vaak verkeerd gebruikt. 'Malware' (schadelijke software) is een nauwkeuriger woord. De detectie-enginemodule voert in combinatie met het onderdeel van het zelflerende systeem malwaredetectie uit. Zie de woordenlijst voor meer informatie over deze typen toepassingen.

Potentieel ongewenste toepassingen

Een potentieel ongewenste toepassing is software waarvan niet geheel duidelijk is of deze schadelijk is. Maar er kan mogelijk wel ongewenste software mee worden geïnstalleerd, het gedrag van een digitaal apparaat worden gewijzigd, activiteiten worden uitgevoerd die niet de goedkeuring van de gebruiker hebben of die de gebruiker niet verwacht of die onduidelijke doelstellingen hebben.

Tot deze categorie behoren: software waarmee reclame wordt weergegeven, wrappers worden gedownload, diverse browsertaakbalken worden gedownload, software met misleidend gedrag, bundelware, trackware.
Zie de woordenlijst voor meer informatie over deze typen toepassingen.

Potentieel verdachte toepassingen

Dit is software die door een merkgebonden compressie- en/of versleutelingsmethode van een inpakprogramma is gecomprimeerd. Inpakprogramma's worden vaak gebruikt om reverse engineering te verhinderen of de inhoud van het uitvoerbare bestand te verbergen (bijvoorbeeld om de aanwezigheid van malware te verbergen).
Deze categorie bestaat uit: alle onbekende toepassingen die zijn gecomprimeerd met een inpakprogramma, dat vaak wordt gebruikt om malware te comprimeren.

Potentieel onveilige toepassingen

Deze classificatie wordt gegeven voor commerciële, legitieme software die voor schadelijke doeleinden kan worden misbruikt. Potentieel onveilige toepassingen is een term die verwijst naar legitieme commerciële software die voor schadelijke doelen kan worden misbruikt.
Deze categorie omvat: hulpprogramma's om software te kraken, licentiecodes te genereren, hacken, op afstand toegang te krijgen of de controle over te nemen, toepassingen om wachtwoorden te kraken en keyloggers (programma's die elke toetsenbordaanslag van een gebruiker vastleggen). Deze optie is standaard uitgeschakeld.
Zie de woordenlijst voor meer informatie over deze typen toepassingen.

Rapportage

Rapportage wordt uitgevoerd door het onderdeel van de detectie-engine en het onderdeel van het zelflerende systeem. U kunt een rapportagedrempel instellen die beter past bij uw omgeving en behoeften. Er is geen enkele configuratie die beter is dan een andere. Daarom raden we aan het gedrag binnen uw omgeving te controleren en daarna te beslissen of een andere rapportage-instelling geschikter is.

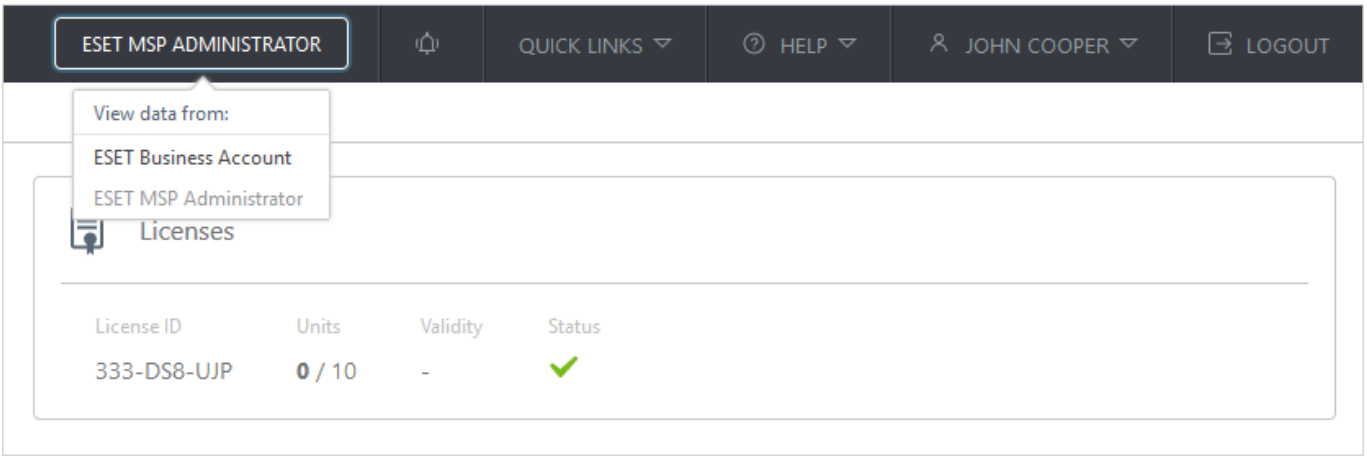
Rapportage onderneemt geen actie op objecten. Er wordt alleen informatie doorgegeven aan een desbetreffende beveiligingslaag en de beveiligingslaag zorgt voor de juiste actie.

Aggressief	**Rapportage die is geconfigureerd voor maximale gevoeligheid. Er worden meer detecties gemeld. Hoewel de instelling Agressief de veiligste lijkt te zijn, kan deze vaak te gevoelig zijn, wat daardoor zelfs contraproductief is.** De instelling Agressief kan objecten ten onrechte als schadelijk identificeren, waardoor er actie op dergelijke objecten wordt ondernomen (afhankelijk van de beveiligingsinstellingen).
Evenwichtig	Deze instelling is een optimale balans tussen prestaties en nauwkeurigheid qua detectiepercentages en het aantal ten onrechte gerapporteerde objecten.
Voorzichtig	Rapportage die is geconfigureerd om het risico van onjuist geïdentificeerde objecten te minimaliseren met behoud van een voldoende beveiligingsniveau. Objecten worden alleen gerapporteerd wanneer het hoogstwaarschijnlijk om malware gaat en het gedrag overeenkomt met het gedrag daarvan.
Uit	Rapportage is niet actief. Detecties worden niet gevonden, gerapporteerd of opgeschoond. Malwarerapportage kan niet worden gedeactiveerd; Daarom is de instelling Uit niet beschikbaar voor malware.

Licentiebeheer

In het hoofdvenster ziet u een overzicht van de licenties die uit ESET Business Account of ESET MSP Administrator zijn verwijderd. U kunt alle licentiepools, sites of bedrijven zien die beschikbaar zijn in de ESET Business Account-portal of ESET MSP Administrator-portal. Met Licentiebeheer kunt u gebruikers beveiligen of de beveiliging opheffen.

Als u hetzelfde e-mailadres hebt geregistreerd in zowel ESET MSP Administrator als ESET Business Account (eenmalige aanmelding), kunt u schakelen tussen de ESET Business Account- en ESET MSP Administrator-weergave (hybride licentieaccount).



Als u een licentie hebt voor ESET Cloud Office Security, kunt u de ESET LiveGuard Advanced-functie zonder extra kosten gebruiken. U vindt het ELG-label naast de licentie-id.

Licentiebeheer met ESET Business Account

Geeft licentiegegevens en -gebruik weer (naam van licentiepool, licentie-ID, eenheden, geldigheid en status.). De licenties en licentiepools worden vanuit ESET Business Account geladen. Licentiepools zijn alleen beschikbaar als u bestaande sites in ESET Business Account hebt (sites zijn handig voor categoriseringsdoeleinden). Eén eenheid staat voor ESET Cloud Office Security-beveiliging van één gebruiker voor Exchange Online en OneDrive.

> Voor elke beveiligde gebruiker wordt één licentie-eenheid gebruikt. Dit is ongeacht welke Microsoft 365-services worden gebruikt. Een gebruiker met Exchange Online of OneDrive (of beide) gebruikt altijd één licentie-eenheid. Voor teamgroepen of SharePoint-sites wordt geen licentie-eenheid gebruikt.

Elke nieuwe gebruiker wordt in het gedeelte Gebruikers als Onbeveiligd weergegeven. Als u automatische beveiliging per tenant of groep gebruikt, worden nieuwe gebruikers automatisch beveiligd en worden deze als Beveiligd weergegeven.

Wanneer u gebruikers beveiligt, hebt u twee mogelijkheden:

- **Automatische beveiliging per tenant of groep (aanbevolen)**: elke nieuw toegevoegde gebruiker die deel uitmaakt van een Azure AD-groep of van een tenant, wordt automatisch beveiligd. U hoeft verder niets te doen. Zie voor meer informatie.
- **Individuele gebruikersbeveiliging**: dit is een beheerde optie, dat wil zeggen dat elke nieuwe gebruiker handmatig moet worden beveiligd.

Gebruikers beveiligen (zonder Licentiepool)

1. Klik op **Beveiligen**.
2. Selecteer Tenant of Groep voor automatische beveiliging van de gebruiker en klik op **Beveiligen**. Selecteer voor individuele gebruikersbeveiliging de gebruikers die u wilt beveiligen en klik op **Beveiligen**. Het standaardbeleid beveiligt gebruikers nu.
3. Geef indien vereist aangepast beleid op voor de gebruikers in het gedeelte Beleid.

Gebruikers beveiligen (met Licentiepool)

1. Selecteer Licentiepool en klik op het pictogram met de drie stippen > **Details weergeven** naast de licentiepool.
2. Klik op **Beveiligen**.
3. Selecteer Tenant of Groep voor automatische beveiliging van de gebruiker en klik op **Beveiligen**. Selecteer voor individuele gebruikersbeveiliging de gebruikers die u wilt beveiligen en klik op **Beveiligen**. Het standaardbeleid beveiligt gebruikers nu.
4. Geef indien vereist aangepast beleid op voor de gebruikers in het gedeelte Beleid.

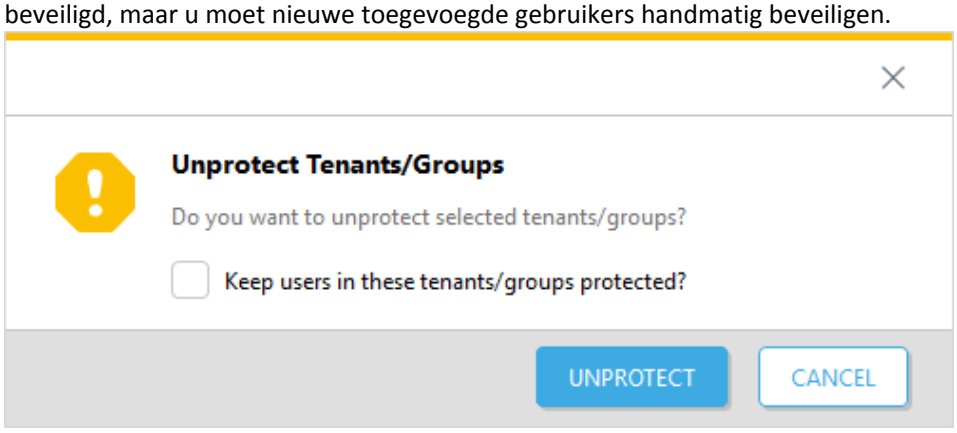
> Controleer of u voldoende licentie-eenheden hebt, vooral als automatische beveiliging is ingeschakeld en het aantal gebruikers toeneemt. Wanneer alle licentie-eenheden in gebruik zijn, worden nieuwe gebruikers binnen een tenant of groep niet beveiligd. De beveiliging van bestaande gebruikers blijft ongewijzigd.
> Als u tijdelijk een tekort aan licentie-eenheden hebt en gebruikers wilt opgeven die u toch wilt beveiligen, kunt u gebruikmaken van onbeveiligde groepen (dus geen automatische beveiliging) en de gebruikers handmatig beveiligen. Zodra u licentiepools met meer eenheden hebt uitgebreid, kunt u terugkeren naar automatische beveiliging zodat het beheer eenvoudiger wordt.

Verplaatsen

Als u gebruikers wilt verplaatsen tussen licentiepools en voor meer geavanceerde bewerkingen met licenties, klikt u op ESET Business Account openen .

Beveiliging opheffen

1. Selecteer individuele gebruikers, een tenant of een groep en klik op **Beveiliging opheffen**.
2. Wanneer u de automatische beveiliging van een tenant of groep verwijdert, wordt u gevraagd: **Gebruikers in deze tenants/groepen blijven beveiligen?**. Als u ervoor kiest deze optie niet te gebruiken, wordt de beveiliging van de gebruikers opgeheven. Als u het selectievakje inschakelt, wordt de automatische beveiliging van de tenant of groep gedeactiveerd en wordt deze gewijzigd in individuele gebruikersbeveiliging. Bestaande gebruikers zijn nog steeds beveiligd, maar u moet nieuwe toegevoegde gebruikers handmatig beveiligen.



Geeft licentiegegevens en -gebruik weer (klantbedrijf, licentie-ID, eenheden en status).

> Voor elke beveiligde gebruiker wordt één licentie-eenheid gebruikt. Dit is ongeacht welke Microsoft 365-services worden gebruikt. Een gebruiker met Exchange Online of OneDrive (of beide) gebruikt altijd één licentie-eenheid.
> Voor teamgroepen of SharePoint-sites wordt geen licentie-eenheid gebruikt.

Elke nieuwe gebruiker wordt in het gedeelte Gebruikers als **Onbeveiligd** weergegeven. Als u automatische beveiliging per tenant of groep gebruikt, worden nieuwe gebruikers automatisch beveiligd en worden deze als **Beveiligd** weergegeven.
Wanneer u gebruikers beveiligt, hebt u twee mogelijkheden:
• **Automatische beveiliging door tenant of groep (aanbevolen)** - onderhoudsvrij, elke nieuw toegevoegde gebruiker die lid is van de Azure AD-groep of deel uitmaakt van een tenant, wordt automatisch beveiligd. Zie voor meer informatie.
• **Individuele gebruikersbeveiliging**: dit is een beheerde optie, dat wil zeggen dat elke nieuwe gebruiker handmatig moet worden beveiligd.

Gebruikers beveiligen

1. Klik op **Beveiligen**.
2. Selecteer Tenant of Groep voor automatische beveiliging van de gebruiker en klik op **Beveiligen**. Selecteer voor individuele gebruikersbeveiliging de gebruikers die u wilt beveiligen en klik op **Beveiligen**. Het standaardbeleid beveiligt gebruikers nu.
3. Geef indien vereist aangepast beleid op voor de gebruikers in het gedeelte Beleid.

> Controleer of u voldoende licentie-eenheden hebt, vooral als automatische beveiliging is ingeschakeld en het aantal gebruikers toeneemt. Wanneer alle licentie-eenheden in gebruik zijn, worden nieuwe gebruikers binnen een tenant of groep niet beveiligd. De beveiliging van bestaande gebruikers blijft ongewijzigd.
> Als u tijdelijk een tekort aan licentie-eenheden hebt en gebruikers wilt opgeven die u toch wilt beveiligen, kunt u gebruikmaken van onbeveiligde groepen (dus geen automatische beveiliging) en de gebruikers handmatig beveiligen. Zodra u licentiepools met meer eenheden hebt uitgebreid, kunt u terugkeren naar automatische beveiliging zodat het beheer eenvoudiger wordt.

Beveiliging opheffen

1. Selecteer individuele gebruikers, een tenant of een groep en klik op **Beveiliging opheffen**.
2. Wanneer u de automatische beveiliging van een tenant of groep verwijdert, wordt u gevraagd: **Gebruikers in deze tenants/groepen blijven beveiligen?**. Als u ervoor kiest deze optie niet te gebruiken, wordt de beveiliging van de gebruikers opgeheven. Als u het selectievakje inschakelt, wordt de automatische beveiliging van de tenant of groep gedeactiveerd en wordt deze gewijzigd in individuele gebruikersbeveiliging. Bestaande gebruikers zijn nog steeds beveiligd, maar u moet nieuwe toegevoegde gebruikers handmatig beveiligen.

ESET Cloud Office Security-gebruikerstoegang voor een specifiek bedrijf

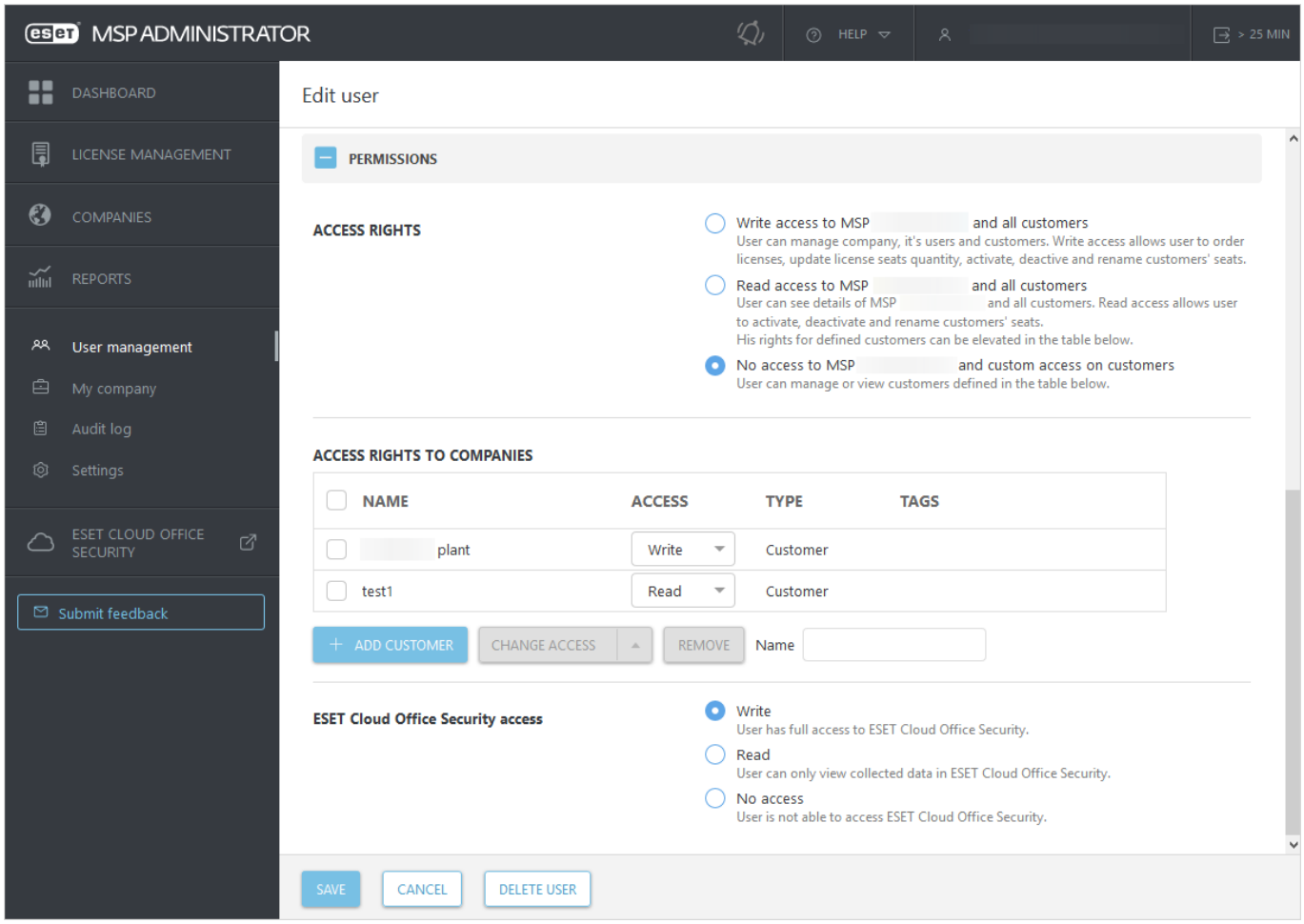
In een omgeving met meerdere tenants kunt u een gebruiker toegang geven tot ESET Cloud Office Security waardoor de gebruiker alleen een specifiek bedrijf kan zien (met lees- of schrijfmachtigingen). Dit is vooral nuttig voor MSP's.

U kunt toegangsrechten voor gebruikers configureren in ESET MSP Administrator door een bedrijf met **Schrijfmachtiging** en **Schrijftoegang** toe te wijzen aan ESET Cloud Office Security:

1. Log in bij ESET MSP Administrator als beheerder.

2. Bewerk een gebruiker en configureer **Toegangsrechten voor bedrijven** onder Machtigingen en selecteer **Schrijftoegang**. De gebruiker kan alleen het toegewezen bedrijf met de licentiepool zien.

3. Stel **Schrijftoegang** voor ESET Cloud Office Security in zodat de gebruiker een bedrijf kan beveiligen door een tenant toe te voegen. Een gebruiker met Leestoegang kan geen tenant toevoegen of verwijderen.



Slechts één toegangstype voor ESET Cloud Office Security kan als een globale instelling worden geconfigureerd en is van toepassing op alle bedrijven (als aan een gebruiker meerdere bedrijven zijn toegewezen).

Controlelogboek

Houdt wijzigingen bij in de configuratie of beveiliging van ESET Cloud Office Security. De records in controlelogboeken zijn bewijs van de activiteiten en tonen de volgorde waarin deze activiteiten plaatsvonden. In controlelogboeken wordt informatie over de specifieke bewerking of gebeurtenis geregistreerd. Controlelogboeken worden gemaakt wanneer een ESET Cloud Office Security-object (licentiepool, gebruiker, beleid, rapport, quarantaine-item zoals een bijlage) wordt gemaakt of gewijzigd.

Wanneer u rechtsboven op het tandwielpictogram klikt om **Exporteren naar CSV** te openen in het contextmenu, kunt u het tabelraster exporteren in *CSV*-indeling en dit in andere toepassingen.

Klik op het pictogram om een zijbalk te openen met een overzicht van een specifieke Controlelogboekrecord. Klik op het pictogram en selecteer **Details weergeven** voor uitvoerige informatie.

Tegel	Details
Basisinformatie	Toont algemene controlelogboekgegevens (Plaatsgevonden, Actie, Ernst, Resultaat, Sectie).
Gebruiker	Toont informatie over de gebruiker die actie heeft ondernomen of een wijziging heeft aangebracht, waaronder het e-mailadres en IP-adres van de gebruiker.

Tegel	Details
Wijzigingen	Details over de aangebrachte wijzigingen.
Oude instellingen	Hier worden eerdere beleidsinstellingen weergegeven.
Nieuwe instellingen	Hier worden de huidige beleidsinstellingen weergegeven.
Objecten	Geeft een overzicht van objecten die door de wijziging of actie worden beïnvloed (gebruiker, beleid, bijlage, enz.).

U kunt gebruikers filteren op verschillende criteria. Klik op **Filter toevoegen** en selecteer een filtertype in het vervolgkeuzemenu of voer een tekenreeks in (herhaal dit als u meerdere criteria combineert):

Filter toevoegen	Syntaxis
Actie	Selecteer een van de beschikbare acties.
Object	Typ een geldige objectnaam.
Status	Selecteer een van de volgende opties: Gelukt, Mislukt, Gestart of Gedeeltelijk gelukt
Gebruiker	Typ de gebruiker die wijzigingen heeft aangebracht.
Ernst	Selecteer het ernstniveau: Laag, Gemiddeld of Hoog
Vond plaats van / Vond plaats tot	Filteren op het moment van optreden. Gebruik Vond plaats van en klik op de datum om alleen records weer te geven die nieuwer zijn dan de opgegeven datum. Gebruik Vond plaats tot voor eerdere records, of gebruik ze allebei voor het gewenste tijdsbereik.
Door systeem geïnitieerd	Filteren records die door het systeem zijn gemaakt.

Feedback verzenden

Als u uw feedback wilt verzenden in de ESET Cloud Office Security-console: ga naar de werkbalk in de rechterbovenhoek, plaats de muisaanwijzer op **Help**, klik op **Feedback verzenden** en kies **Laat ons weten wat u ervan vindt** (om ideeën en ervaringen te delen) of **Meld een probleem of bug**.

Technische ondersteuning

Gebruik de volgende koppelingen met ondersteuningsinformatie om u te helpen eventuele problemen op te lossen:

Zoeken in ESET-kennisbank

ESET-kennisbank: bevat antwoorden op veelgestelde vragen en aanbevolen oplossingen voor verschillende problemen. De kennisbank wordt regelmatig bijgewerkt door de technisch specialisten van ESET en vormt zo een krachtig hulpmiddel voor het oplossen van een breed scala aan problemen.

Het ESET Security-forum raadplegen

Supportforum: het ESET-forum is handig voor ESET-gebruikers die hulp willen krijgen of anderen willen helpen. U kunt hier elk probleem of elke vraag met betrekking tot uw ESET-producten posten.

Neem contact op met Technische ondersteuning

ESET-formulier voor technische ondersteuning: vul het formulier in om uw gegevens op te geven, inclusief de beschrijving van het probleem.

Contact opnemen met uw lokale ESET-partner voor ondersteuning

Neem contact op met uw lokale ESET-ondersteuning Zoek de contactgegevens voor ESET-ondersteuning in uw regio, zoals vermeld in de e-mail over uw ESET-licentie.

Feedback verzenden

Feedback verzenden: kies Laat ons weten wat u ervan vindt (ideeën en ervaringen delen) of Meld een probleem of bug.

Suggesties voor verbetering van de Online-Help

U kunt uw beoordeling plaatsen en feedback geven over een specifiek onderwerp in de Online-Help door te klikken op de koppeling **Was deze informatie nuttig?** onder de Help-pagina. Laat ons weten of de inhoud heeft geholpen of hoe Technical Writer deze volgens u kan verbeteren.

Beschikbaarheid van de service

De ESET Status Portal geeft de huidige status van ESET-cloudservices, geplande uitval en eerdere incidenten weer. Als u een probleem ondervindt met een ondersteunde ESET-service en deze niet wordt vermeld in de Status Portal, neemt u contact op met de technische ondersteuning van ESET.

Controleteams verifiëren potentiële problemen intern en bevestigde incidenten worden handmatig gepost en bijgewerkt om de geloofwaardigheid en nauwkeurigheid te waarborgen. Daarom verschijnen ze met een kleine vertraging in de Status Portal. Het is mogelijk dat korte incidenten niet worden gepost als ze zijn opgelost voordat ze handmatig zijn bevestigd.

Security for ESET Cloud Office Security

Inleiding

In dit document vindt u een samenvatting van de beveiligingspraktijken en beveiligingscontroles die binnen ESET Cloud Office Security worden toegepast. Beveiligingspraktijken en -controles zijn ontworpen om de vertrouwelijkheid, integriteit en beschikbaarheid van klantgegevens te beschermen. Houd er rekening mee dat beveiligingspraktijken en -controles kunnen veranderen.

Reikwijdte

In dit document vindt u een samenvatting van de beveiligingspraktijken en beveiligingscontroles voor de infrastructuur, de organisatie, het personeel en de operationele processen van ESET Cloud Office Security, ESET Business Account (hierna "EBA" genoemd), ESET Data Framework, ESET LiveGrid, Update, AntiSpam en ESET Dynamic Threat Defense. Beveiligingspraktijken en -controles bestaan uit:

1. Informatiebeveiligingsbeleid
2. Organisatie van informatiebeveiliging
3. Beveiliging van human resources
4. Beheer van activa
5. Toegangsbeheer
6. Cryptografie

7. Fysieke beveiliging en beveiliging van de omgeving
8. Operationele beveiliging
9. Beveiliging van de communicatie
10. Systeemacquisitie, -ontwikkeling en -onderhoud
11. Relatie met leverancier
12. Beheer van IT-incidenten
13. IT-aspecten van bedrijfscontinuïteitsbeheer
14. Naleving

Beveiligingsconcept

ESET s.r.o. bedrijf is ISO 27001: 2013 gecertificeerd met een reikwijdte van het geïntegreerd beheersysteem van ESET Cloud Office Security, EBA en andere diensten.

Bij het concept van informatiebeveiliging wordt gebruik gemaakt van het ISO 27001-raamwerk om een gelaagde verdediging als beveiligingsstrategie te implementeren bij het toepassen van beveiligingscontroles bij de laag van het netwerk, de besturingssystemen, databases, toepassingen, het personeel en de bedrijfsprocessen. Toegepaste beveiligingspraktijken en beveiligingscontroles zijn bedoeld om elkaar te overlappen en aan te vullen.

Beveiligingspraktijken en -controles

1. Informatiebeveiligingsbeleid

ESET hanteert informatiebeveiligingsbeleid om alle aspecten van de ISO 27001-standaard te dekken, waaronder informatiebeveiligingsbeheer en beveiligingscontroles en -praktijken. Beleid wordt na belangrijke wijzigingen jaarlijks herzien en bijgewerkt om ervoor te zorgen dat het nog steeds geschikt, adequaat en effectief is.

ESET voert een jaarlijkse beoordeling van dit beleid en interne beveiligingscontroles uit om consistentie met dit beleid te waarborgen. Niet-naleving van het informatiebeveiligingsbeleid is onderworpen aan disciplinaire maatregelen voor ESET-werknemers of contractuele sancties, tot en met beëindiging van het contract met leveranciers.

2. Organisatie van informatiebeveiliging

De organisatie van informatiebeveiliging voor ESET Cloud Office Security bestaat uit meerdere teams en personen die betrokken zijn bij informatiebeveiliging en IT, waaronder:

- uitvoerend management van ESET
- interne beveiligingsteams van ESET
- IT-teams voor bedrijfstoepassingen
- Andere ondersteunende teams

IT-beveiligingsverantwoordelijkheden worden toegewezen in overeenstemming met het geldende IT-beveiligingsbeleid. Interne processen worden geïdentificeerd en beoordeeld op elk risico van ongeautoriseerde of onbedoelde wijziging of misbruik van ESET-activa. Risicovolle of gevoelige activiteiten van interne processen hanteren het principe van 'functiescheiding' om risico's te beperken.

Het juridische team van ESET is verantwoordelijk voor de contacten met overheidsinstanties, waaronder Slowaakse toezichthouders op het gebied van cyberbeveiliging en de bescherming van persoonsgegevens. Het interne beveiligingsteam van ESET is verantwoordelijk voor contact met speciale belangengroepen zoals ISACA. Het onderzoekslaboratorium van ESET is verantwoordelijk voor de communicatie met andere beveiligingsbedrijven en de grotere cyberbeveiligingsgemeenschap.

Informatiebeveiliging maakt dankzij het toegepaste projectmanagementkader deel uit van projectmanagement, van concept tot oplevering van projecten.

Werken op afstand en telewerken vallen onder beleid dat is geïmplementeerd op mobiele apparaten, waaronder het gebruik van sterke cryptografische gegevensbescherming op mobiele apparaten tijdens de overdracht naar niet-vertrouwde netwerken. Beveiligingscontroles op mobiele apparaten zijn ontworpen om onafhankelijk van de interne netwerken en interne systemen van ESET te werken.

3. Beveiliging van human resources

ESET hanteert standaard humanresourcepraktijken, waaronder beleidsregels die zijn ontworpen om de informatiebeveiliging te handhaven. Deze praktijken bestrijken de hele levenscyclus van medewerkers en zijn van toepassing op alle teams die toegang tot de ESET Cloud Office Security-omgeving hebben.

4. Beheer van activa

De ESET Cloud Office Security-infrastructuur is opgenomen in ESET-activa-inventarissen met strikte eigendom en regels die worden toegepast op basis van het type en de gevoeligheid van de activa. ESET hanteert een intern classificatieschema. Alle ESET Cloud Office Security-gegevens en configuraties worden als vertrouwelijk geclassificeerd.

5. Toegangsbeheer

Het toegangsbeheerbeleid van ESET regelt alle toegang in ESET Cloud Office Security. Toegangsbeheer wordt ingesteld op het niveau van de infrastructuur, netwerkservices, het besturingssysteem, de database en de toepassing. Volledig gebruikerstoegangsbeheer op toepassingsniveau vindt autonoom plaats. Eenmalige aanmelding bij ESET Cloud Office Security en ESET Business Account wordt beheerd door een centrale identiteitsprovider die ervoor zorgt dat een gebruiker alleen toegang tot de geautoriseerde tenant heeft. De toepassing maakt gebruik van standaardmachtigingen van ESET Cloud Office Security om op rollen gebaseerd toegangsbeheer voor de tenant af te dwingen.

ESET-backend-toegang is strikt beperkt tot geautoriseerde personen en rollen. Er worden standaard-ESET-processen voor gebruikersregistratie, (de)provisioning, beheer van bevoegdheden en beoordeling van gebruikerstoegangsrechten gehanteerd om de toegang van ESET-medewerkers tot de infrastructuur en netwerken van ESET Cloud Office Security te beheren.

Er is sterke verificatie aanwezig om de toegang tot alle ESET Cloud Office Security-gegevens te beveiligen.

6. Cryptografie

Om de ESET Cloud Office Security-gegevens te beveiligen, wordt sterke cryptografie gebruikt om gegevens in rust en tijdens overdracht te versleutelen. Er wordt een algemeen vertrouwde certificeringsinstantie gebruikt om certificaten voor openbare diensten uit te geven. Er wordt een interne openbare-sleutelinfrastructuur van ESET gebruikt om sleutels binnen de infrastructuur van ESET Cloud Office Security te beheren. Gegevens die in de database zijn opgeslagen, worden beveiligd met versleutelingssleutels die in de cloud worden gegenereerd. Alle back-upgegevens worden beveiligd met door ESET beheerde sleutels.

7. Fysieke beveiliging en beveiliging van de omgeving

Omdat ESET Cloud Office Security en ESET Business Account gebaseerd zijn op de cloud, vertrouwen we op Microsoft Azure voor de fysieke beveiliging en beveiliging van de omgeving. Microsoft Azure maakt gebruik van gecertificeerde datacenters met robuuste fysieke beveiligingsmaatregelen. De fysieke locatie van het datacenter

is afhankelijk van de keuze die voor de klantregio wordt gemaakt.

8. Operationele beveiliging

De ESET Cloud Office Security-service wordt uitgevoerd via geautomatiseerde middelen op basis van strikte operationele procedures en configuratiesjablonen. Alle wijzigingen, waaronder configuratiewijzigingen en de implementatie van nieuwe pakketten, worden goedgekeurd en getest in een speciale testomgeving voordat deze in productie worden genomen. Ontwikkelings-, test- en productieomgevingen zijn van elkaar gescheiden. ESET Cloud Office Security-gegevens bevinden zich alleen in de productieomgeving.

De ESET Cloud Office Security-omgeving wordt bewaakt met behulp van operationele monitoring om problemen snel te identificeren en alle services op netwerk- en hostniveau voldoende capaciteit te bieden.

Alle configuratiegegevens worden opgeslagen in opslagplaatsen waarvan regelmatig back-ups worden gemaakt om geautomatiseerd herstel van de configuratie van een omgeving mogelijk te maken. Gegevensback-ups van ESET Cloud Office Security worden zowel onsite als offsite opgeslagen.

Back-ups worden als onderdeel van het testen van de bedrijfscontinuïteit versleuteld en regelmatig getest op herstelbaarheid.

Audits op systemen worden uitgevoerd volgens interne normen en richtlijnen. Logboeken en gebeurtenissen in de infrastructuur, het besturingssysteem, de database, toepassingsservers en beveiligingscontroles worden continu verzameld. De logboeken worden verder verwerkt door IT- en interne beveiligingsteams om operationele afwijkingen, beveiligingsafwijkingen en informatiebeveiligingsincidenten te identificeren.

ESET gebruikt een algemeen technisch proces voor het beheer van beveiligingsproblemen om het optreden van beveiligingsproblemen in de ESET-infrastructuur, waaronder ESET Cloud Office Security en andere ESET-producten, aan te pakken. Dit proces bestaat uit proactieve scans op beveiligingsproblemen en herhaalde penetratietests van de infrastructuur, producten en toepassingen.

ESET hanteert interne richtlijnen voor de beveiliging van interne infrastructuur, netwerken, besturingssystemen, databases, toepassingsservers en toepassingen. Deze richtlijnen worden gecontroleerd met behulp van technische monitoring op de naleving en ons interne auditprogramma voor informatiebeveiliging.

9. Beveiliging van de communicatie

De ESET Cloud Office Security-omgeving is gesegmenteerd op basis van native cloudsegmentatie met netwerktoegang die beperkt is tot noodzakelijke services tussen netwerksegmenten. De beschikbaarheid van netwerkservices wordt gerealiseerd op basis van native cloudbesturingselementen zoals beschikbaarheidszones, load-balancing en redundantie. Er worden speciale load-balancing-componenten geïmplementeerd om specifieke endpoints mogelijk te maken, bijvoorbeeld voor ESET Cloud Office Security-routering die autorisatie van verkeer en load-balancing afdwingt. Het netwerkverkeer wordt continu bewaakt op afwijkingen in de werking en beveiliging. Potentiële aanvallen kunnen worden opgelost met behulp van native cloudcontroles of geïmplementeerde beveiligingsoplossingen. Alle netwerkcommunicatie wordt versleuteld via algemeen beschikbare technieken, waaronder IPsec en TLS.

10. Systeemacquisitie, -ontwikkeling en -onderhoud

De ontwikkeling van ESET Cloud Office Security-systemen wordt uitgevoerd in overeenstemming met het ESET-beleid voor de ontwikkeling van veilige software. Interne beveiligingsteams worden vanaf de beginfase in het ESET Cloud Office Security-ontwikkelingsproject opgenomen en houden toezicht op alle ontwikkelings- en onderhoudsactiviteiten. Het interne beveiligingsteam definieert en controleert de naleving van beveiligingsvereisten tijdens verschillende stadia van de ontwikkeling van de software. De beveiliging van alle

services, waaronder nieuw ontwikkelde services, wordt na release continu getest.

11. Relatie met leverancier

Een relevante relatie met de leverancier is gebaseerd op geldende ESET-richtlijnen, die betrekking hebben op volledig relatiebeheer en contractuele vereisten vanuit het oogpunt van informatiebeveiliging en privacy. De kwaliteit en veiligheid van de dienstverlening van de kritische dienstverlener worden regelmatig beoordeeld.

12. Informatiebeveiligingsbeheer

Informatiebeveiligingsbeheer in ESET Cloud Office Security wordt op dezelfde manier uitgevoerd als in andere ESET-infrastructuren en is afhankelijk van gedefinieerde procedures voor incidentrespons. Rollen binnen incidentrespons worden gedefinieerd en toegewezen aan meerdere teams, waaronder IT, beveiliging, juridisch, human resources, public relations en uitvoerend management. Het incidentresponseteam voor incidenten wordt samengesteld op basis van de triage van incidenten door het interne beveiligingsteam. Dat team zorgt voor verdere coördinatie van andere teams die het incident afhandelen. Het interne beveiligingsteam is ook verantwoordelijk voor het verzamelen van bewijsmateriaal en het leren van lessen om soortgelijke incidenten in de toekomst te voorkomen. Incident en oplossing worden naar de betrokken partijen gecommuniceerd. Het juridische team van ESET is volgens de Algemene Verordening Gegevensbescherming (AVG) en de Cybersecurity Act Transposing Network and Information Security Directive (NIS) verantwoordelijk voor het indien nodig op de hoogte stellen van regelgevende instanties.

13. Informatiebeveiligingsaspecten ten aanzien van bedrijfscontinuïteitsbeheer

De bedrijfscontinuïteit van de ESET Cloud Office Security-service ligt besloten in de robuuste architectuur die wordt gehanteerd om de beschikbaarheid van de geleverde services te maximaliseren. Voor ESET Cloud Office Security-componenten of de ESET Cloud Office Security is volledig herstel van offsite back-up- en configuratiegegevens mogelijk na een catastrofale storing van alle redundante knooppunten -service. Het herstelproces wordt regelmatig getest.

14. Naleving

Naleving van de reglementaire en contractuele vereisten van ESET Cloud Office Security wordt regelmatig bekeken en beoordeeld, net als andere infrastructuur en processen van ESET, en de nodige stappen worden genomen om naleving ervan op een continue basis te waarborgen. ESET is geregistreerd als digitale serviceprovider voor digitale cloudcomputingservices voor meerdere ESET-services, waaronder ESET Cloud Office Security. Houd er rekening mee dat ESET-nalevingsactiviteiten niet noodzakelijkerwijs betekent dat als zodanig aan de algemene nalevingsvereisten van klanten wordt voldaan.

Gebruiksvoorwaarden

Van kracht per 23 oktober 2023 | Een eerdere versie van de Gebruiksvoorwaarden bekijken | Wijzigingen vergelijken

Deze ESET Cloud Office Security Overeenkomst (hierna aangeduid als "Voorwaarden") vormt een speciale overeenkomst tussen ESET, spol. s r. o., kantoorhoudende te Einsteinova 24, 85101 Bratislava, Slovak Republic, ingeschreven in het handelsregister dat wordt beheerd door de rechtbank van Bratislava I, sectie Sro, volgnr. 3586/B, bedrijfsregistratienummer: 31333532 ("ESET" of "Provider") en u, een natuurlijke persoon of rechtspersoon ("U" of "Gebruiker") die toegang krijgt tot een account voor administratie, ESET Cloud Office Security en tot een webportal die eigendom is van en beheerd wordt door ESET ("Account"), teneinde ESET Cloud Office Security te kunnen gebruiken. Als u het Account en ESET Cloud Office Security (hierna gezamenlijk

aangeduid als "Product") namens een organisatie gebruikt, gaat u namens die organisatie akkoord met deze Voorwaarden en garandeert u dat u de bevoegdheid hebt om die organisatie tot deze Voorwaarden te verplichten. In dat geval verwijzen U en Gebruiker naar die organisatie. Lees deze Voorwaarden zorgvuldig door, aangezien deze ook betrekking hebben op door ESET geleverde services via of in verband met het Product. De specifieke voorwaarden voor het gebruik van individuele services buiten deze Voorwaarden worden bij elke service vermeld, en de aanvaarding ervan maakt deel uit van het serviceactiveringsproces. De bijgevoegde bijlagen vormen een aanvulling op deze Voorwaarden.

Beveiliging en gegevensbescherming

Account biedt toegang tot services die door ESET worden geleverd. Gebruikersgegevens zoals volledige naam, bedrijfsnaam, land, geldig e-mailadres, telefoonnummer, licentiegegevens en statistieken zijn vereist voor de registratie en het gebruik van het Account en voor de inrichting en het onderhoud van de services die via het Account worden gebruikt. U gaat er hierbij mee akkoord dat de gegevens worden verzameld en overdragen naar de servers van de Provider of die van zijn partners, met als doel de functionaliteit van en autorisatie voor het gebruik van de Software te garanderen en de rechten van de Provider te beschermen. Na sluiting van deze Voorwaarden heeft de Provider of zijn partners het recht essentiële gegevens waarmee U kunt worden geïdentificeerd, over te dragen, te verwerken en op te slaan, voor ondersteuningsdoeleinden en voor de uitvoering van deze Voorwaarden. U bent uitsluitend gemachtigd het Account te gebruiken voor de doeleinden en manier waarop het in het kader van deze Voorwaarden, individuele servicevoorwaarden en documentatie is bedoeld.

U bent verantwoordelijk voor de beveiliging van uw Account en de aanmeldingsgegevens om toegang te krijgen. ESET zal niet aansprakelijk worden gesteld voor enig verlies of enige schade die het gevolg is van niet-naleving van deze verplichting om de veiligheid te handhaven. De Gebruiker is ook verantwoordelijk voor alle activiteit met betrekking tot het gebruik van het Account, of deze nu geautoriseerd is of niet. Als er inbreuk is gemaakt op het Account, dient u de Provider direct hiervan op de hoogte te stellen.

Voor het aanbieden van de administratieservice voor het Account is het verzamelen van gegevens met betrekking tot beheerde apparaten vereist in combinatie met administratiegegevens (hierna aangeduid als "”Gegevens""). Gegevens worden uitsluitend door ESET aan U geleverd met als doel het inrichten van de administratieservice van het Account. Gegevens worden verwerkt en opgeslagen in overeenstemming met het beveiligingsbeleid en -richtlijnen van ESET evenals in overeenstemming met het Privacybeleid.

Details over privacy, bescherming van persoonlijke gegevens en uw rechten als gegevensonderwerp vindt u in het Privacybeleid.

Beleid inzake aanvaardbaar gebruik

U bent verplicht zich te houden aan technische beperkingen die in de documentatie zijn vastgelegd. U stemt ermee in dat U het Account 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 Gebruikers te beperken, om het gebruik van de services door een zo hoog mogelijk aantal Gebruikers te kunnen waarborgen. Beperking van de reikwijdte van de services betekent ook volledige beëindiging van de mogelijkheid om gebruik te maken van de functies van het Account en van verwijdering van gegevens en informatie.

Details over technische beperkingen zijn te vinden in Beperkingen.

Locatie

Provider kan u toestaan te kiezen uit beschikbare hostinglocaties voor Account, waaronder een aanbevolen locatie die wordt gekozen door de Provider. U erkent dat een keuze voor een andere dan de aanbevolen locatie gevolgen kan hebben voor uw gebruikerservaring. Op basis van de gekozen locatie kunnen de in bijlage nr. 2 van deze overeenkomst opgenomen gegevensbeschermingsovereenkomst en de in bijlage nr. 3 van deze overeenkomst opgenomen modelcontractbepalingen van toepassing zijn. ESET behoudt zich het recht voor om op elk moment en zonder voorafgaande kennisgeving een specifieke locatie te wijzigen met het oog op de verbetering van de services die door ESET worden geleverd in overeenstemming met de voorkeuren van uw locatie (bijvoorbeeld de Europese Unie).

Software

ESET of zijn respectieve leveranciers bezitten het auteursrecht op alle software die beschikbaar is als onderdeel van het Product, of kunnen dit recht uitoefenen (hierna aangeduid als "Software"). De Software mag alleen worden gebruikt in overeenstemming met de in Bijlage 1 van deze Overeenkomst opgenomen Licentieovereenkomst voor eindgebruikers (hierna aangeduid als "EULA"). Overige informatie met betrekking tot licenties, auteursrecht, documentatie en handelsmerken zijn uiteengezet in het juridische informatie.

Beperkingen

U mag geen componenten kopiëren, verspreiden of uitnemen, of afgeleide producten van het Account maken. Bij gebruik van het Account bent U verplicht te voldoen aan de volgende beperkingen:

(a) U mag het Account niet gebruiken, wijzigen, vertalen of reproduceren of gebruiksrechten voor het Account of onderdelen ervan overdragen op een andere wijze dan in deze Voorwaarden wordt beschreven.

(b) U mag het Account niet verkopen, onder sublicentie geven, leasen of huren of lenen, of het Account gebruiken voor het verrichten van commerciële diensten.

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

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

Disclaimers

ALS DE GEBRUIKER ERKENT U HIERBIJ DAT HET ACCOUNT EN DE SERVICES IN DE 'OORSPRONKELIJKE STAAT' ZIJN GELEVERD, ZONDER EXPLICIETE OF IMPLICIETE GARANTIE VAN WELKE AARD DAN OOK EN VOOR ZOVER DAT VOLGENS 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 HET ACCOUNT OF DE SERVICES GEEN INBREUK MAKEN OP OCTROOIEN, AUTEURSRECHT, HANDELSMERKEN OF ANDERE RECHTEN VAN DERDEN. DE PROVIDER OF WELKE ANDERE PARTIJ DAN OOK GEVEN GEEN GARANTIE DAT HET ACCOUNT OF DE SERVICES VOLDOEN AAN UW VEREISTEN OF DAT DE WERKING VAN HET ACCOUNT OF DE SERVICES ONONDERBROKEN EN VRIJ VAN FOUTEN ZAL ZIJN. U AANVAARDT ALLE VERANTWOORDELIJKHEID EN HET RISICO VOOR DE SELECTIE EN HET GEBRUIK VAN HET ACCOUNT OF DE SERVICES OM DE DOOR U BEOOGDE RESULTATEN

TE BEHALEN EN VOOR DE RESULTATEN DIE HIERMEE WORDEN VERKREGEN.

Deze Voorwaarden creëren geen verplichtingen voor de Provider en zijn licentiegevers, anders dan specifiek is uiteengezet in deze Voorwaarden.

Beperking van aansprakelijkheid

VOOR ZOVER IS TOEGESTAAN VOLGENS DE TOEPASSELIJKE WETTEN, ZULLEN DE PROVIDER, ZIJN WERKNEMERS OF CONTRACTANTEN 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 HET ACCOUNT, ZELFS ALS DE PROVIDER, ZIJN CONTRACTANTEN OF GELIEERDE ONDERNEMINGEN 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 CONTRACTANTEN OF GELIEERDE BEDRIJVEN BEPERKT TOT HET BEDRAG DAT U VOOR DE DESBETREFFENDE SERVICE OF HET DESBETREFFENDE ACCOUNT HEBT BETAALD.

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 ('Gelieerde ondernemingen') 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 deze Voorwaarden moeten worden uitgevoerd, of waarin het ESET of een van aan haar Gelieerde ondernemingen is gevestigd of werkzaam is en

ii. elke economische, financiële, handels- of andere sanctie, beperking, embargo, import- of exportverbod, verbod op de overdracht van fondsen of activa of op het verrichten van diensten, of 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 deze Voorwaarden moeten worden uitgevoerd, of waarin ESET of een van haar gelieerde ondernemingen zijn gevestigd of werkzaam zijn (rechtshandelingen zoals bedoeld in punt i en ii hierboven samen als "Handelscontrolewetten").

(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 bepaalt dat, naar haar redelijke mening, de Gebruiker de bepaling van sectie (a) van deze 'Naleving van handelscontroles'-clausule van deze Voorwaarden heeft geschonden of waarschijnlijk zal schenden; 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 deze Voorwaarden ertoe kan leiden dat ESET of aan haar Gelieerde ondernemingen de Handelscontrolewetten schendt of onderworpen wordt aan negatieve gevolgen.

(c) Niets in deze Voorwaarden 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.

Toepasselijk recht en taal

Met betrekking tot deze Voorwaarden en de interpretatie ervan geldt het Slowaakse recht als toepasselijk recht. De Eindgebruiker en de Provider gaan ermee akkoord dat conflictbepalingen van het toepasselijke recht en het Weens koopverdrag niet van toepassing zijn. Als U een consument bent met een gewone verblijfplaats in de EU, krijgt u ook extra bescherming die U wordt verleend door dwingende wettelijke bepalingen die van toepassing zijn in uw land van verblijf.

U stemt er uitdrukkelijk mee in dat de rechtbank van Bratislava I., Slowakije, de exclusieve jurisdictie heeft over vorderingen of geschillen die U hebt met de Provider of die op enige wijze verband houden met uw gebruik van de Software, het Account of de Services of voortvloeiend uit deze Voorwaarden of Bijzondere voorwaarden (indien van toepassing) en U gaat ook akkoord en stemt uitdrukkelijk in met de uitoefening van de persoonlijke jurisdictie in de districtsrechtbank van Bratislava I, in verband met enige vordering of enig geschil. Als U een consument bent en uw gewoonlijke verblijfplaats in de EU hebt, kunt U ook een claim indienen om uw consumentenrechten af te dwingen in de plaats van exclusieve jurisdictie of in het EU-land waarin U woont. Bovendien kunt U ook gebruikmaken van een onlineplatform voor geschillenbeslechting, dat hier toegankelijk is: https://ec.europa.eu/consumers/odr/. Overweeg echter eerst contact met ons op te nemen voordat U officieel een claim indient.

Als er verschillen zijn tussen de taalversies van deze Voorwaarden, prevaleert altijd de Engelstalige versie die hier beschikbaar is.

Algemene bepalingen

ESET behoudt zich het recht voor deze Voorwaarden of onderdelen ervan op enig moment zonder voorafgaande kennisgeving te wijzigen door dit document bij te werken, zodat het overeenkomt met wijzigingen in de wetgeving of met wijzigingen in het Account. U ontvangt bericht als deze Voorwaarden voor Accounts worden gewijzigd. Als u niet akkoord gaat met de wijzigingen van deze Voorwaarden, kunt u uw Account annuleren. Tenzij U uw Account annuleert, bent U gebonden aan de amendementen of wijzigingen van deze Voorwaarden. Wij raden u aan regelmatig deze pagina te bezoeken om de huidige Voorwaarden te lezen die van toepassing zijn op uw gebruik van het Account.

Kennisgevingen

Alle kennisgevingen moeten worden verzonden naar: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Bijlagenr. 1

Licentieovereenkomst voor eindgebruikers

Bijlagenr. 2

Gegevensverwerkingsovereenkomst

Bijlagenr. 3

Modelcontractbepalingen

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, 851 01 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 ga akkoord' of 'Ik ga akkoord...' 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, en informatie over de bewerkingen en functionaliteit van de Software (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.

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, 851 01 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: BUS-ECOS-20-01

Data Processing Agreement

Overeenkomstig de vereisten van Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (hierna de 'AVG' genoemd) gaan de Aanbieder (hierna 'Verwerker' genoemd) en U (hierna 'Verwerkingsverantwoordelijke' genoemd) de gegevensverwerkingsovereenkomst aan om de voorwaarden en bepalingen voor de verwerking van persoonsgegevens en de wijze van bescherming daarvan vast te leggen en om andere rechten en plichten van beide partijen bij de verwerking van persoonsgegevens van betrokkenen in opdracht van de Verwerker in het kader van de uitvoering van het voorwerp van deze Voorwaarden als hoofdovereenkomst te definiëren.

1. **Verwerking van persoonsgegevens.** De services die in overeenstemming met deze Voorwaarden worden geleverd, kunnen de verwerking van informatie omvatten met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon die wordt vermeld in het Privacybeleid (hierna 'Persoonsgegevens' genoemd).

2. **Autorisatie.** De Verwerkingsverantwoordelijke machtigt de Verwerker om Persoonsgegevens te verwerken, met inbegrip van de volgende instructies:

(i) Doel van de verwerking: het verlenen van services in overeenstemming met deze Voorwaarden, De Verwerker mag alleen Persoonsgegevens verwerken namens de Verwerkingsverantwoordelijke met betrekking tot de levering van de door de Verwerkingsverantwoordelijke gevraagde services. Alle informatie die voor aanvullende doeleinden wordt verzameld, wordt verwerkt buiten de contractuele relatie tussen Verwerkingsverantwoordelijke en Verwerker.

(ii) Verwerkingsperiode: periode vanaf het aangaan van de wederzijdse samenwerking op grond van deze Voorwaarden tot de beëindiging van de services,

(iii) Reikwijdte en categorieën van Persoonsgegevens. De Services zijn uitsluitend bedoeld voor de verwerking van algemene persoonsgegevens. De Verwerkingsverantwoordelijke is er echter als enige verantwoordelijk voor om de reikwijdte van de persoonsgegevens te bepalen.

(iv) Betrokkene: een natuurlijke persoon als gemachtigde gebruiker van de apparaten van de Verantwoordelijke voor de verwerking,

v) Verwerkingsactiviteiten: alle handelingen die voor de verwerking noodzakelijk zijn,

(vi) Gedocumenteerde instructies: instructies die in deze Voorwaarden, de Bijlagen, het Privacybeleid en de documentatie van de serviceverlening worden beschreven. De Verwerkingsverantwoordelijke is verantwoordelijk voor de wettelijke toelaatbaarheid van de verwerking van Persoonsgegevens door de Verwerker met betrekking tot de respectievelijk toepasselijke bepalingen van de wetgeving inzake gegevensbescherming.

3. **Verplichtingen van Verwerker**. De Verwerker verplicht zich tot het volgende:

(i) Persoonsgegevens alleen verwerken op basis van Gedocumenteerde instructies en voor het doel dat is

gedefinieerd in de Voorwaarden, de Bijlagen, het Privacybeleid en de documentatie van de serviceverlening,

(ii) instructies geven aan de personen die gemachtigd zijn om de Persoonsgegevens te verwerken (hierna 'Geautoriseerde personen' genoemd), in verband met hun rechten en plichten volgens de AVG en over hun aansprakelijkheid in geval van inbreuk, en waarborgen dat Geautoriseerde personen zich hebben verplicht tot vertrouwelijkheid en naleving van de Gedocumenteerde instructies,

(iii) de maatregelen implementeren en volgen die worden beschreven in de Voorwaarden, de Bijlagen, het Privacybeleid en de documentatie van de serviceverlening,

(iv) de Verwerkingsverantwoordelijke helpen om te reageren op verzoeken van Betrokkenen met betrekking tot hun rechten. De Verwerker zal de verwerking van Persoonsgegevens niet corrigeren, verwijderen of beperken zonder de instructie van de Verwerkingsverantwoordelijke. Alle verzoeken van Betrokkenen met betrekking tot Persoonsgegevens die namens de Verwerkingsverantwoordelijke worden verwerkt, worden onverwijld doorgestuurd naar de Verwerkingsverantwoordelijke.

(v) de Verwerkingsverantwoordelijke bijstaan bij de melding van een inbreuk op persoonsgegevens aan de toezichthoudende autoriteit en de Betrokkene. De Verwerker zal Verwerkingsverantwoordelijke onmiddellijk na ontdekking op de hoogte stellen van een inbreuk op de verwerking van persoonsgegevens of de beveiliging van persoonsgegevens. De Verwerker zal in redelijke mate meewerken aan een onderzoek naar en verhelpen van een dergelijke inbreuk, en redelijke maatregelen nemen om verdere negatieve gevolgen te beperken.

(vi) naar keuze van de Verwerkingsverantwoordelijke, alle Persoonsgegevens verwijderen of teruggeven aan de Verwerkingsverantwoordelijke na het einde van de Verwerkingsperiode. De Verwerkingsverantwoordelijke verbindt zich ertoe de Verwerker binnen tien (10) dagen na het einde van de Verwerkingsperiode op de hoogte te stellen van de keuze. Deze bepaling doet geen afbreuk aan het recht van de Verwerker om de Persoonsgegevens te bewaren voor zover nodig voor archiveringsdoeleinden in het algemeen belang, wetenschappelijk onderzoek, statistische doeleinden of voor het instellen, uitoefenen of verdedigen van juridische claims.

(vii) een register bijhouden van alle categorieën Verwerkingsactiviteiten die zijn uitgevoerd namens de Verwerkingsverantwoordelijke,

(viii) alle informatie die nodig is om naleving aan te tonen als onderdeel van de Voorwaarden, de Bijlagen, het Privacybeleid en de documentatie van de serviceverlening, beschikbaar stellen aan de Verwerkingsverantwoordelijke. In geval van audit of controle van de verwerking van Persoonsgegevens door Verwerkingsverantwoordelijke is de Verwerkingsverantwoordelijke verplicht de Verwerker hiervan minimaal tien (30) dagen vóór de geplande audit of controle schriftelijk op de hoogte te stellen.

4. **Een andere Verwerker inschakelen.** De Verwerker heeft het recht om een andere verwerker in te schakelen voor de uitvoering van specifieke verwerkingsactiviteiten, zoals het aanbieden van cloudopslag en infrastructuur voor de service in overeenstemming met de Voorwaarden, de Bijlagen, het Privacybeleid en de documentatie van de serviceverlening. Microsoft biedt momenteel cloudopslag en infrastructuur als onderdeel van Azure-cloudservice. In dat geval blijft de Verwerker het enige aanspreekpunt en de partij die verantwoordelijk is voor naleving. De Verwerker verbindt zich er hierbij toe de Verwerkingsverantwoordelijke te informeren over elke toevoeging of vervanging van een andere verwerker om de mogelijkheid te bieden om tegen een dergelijke wijziging bezwaar te maken.

5. **Gebied van Verwerking.** De Verwerker zorgt ervoor dat de verwerking plaatsvindt in de Europese Economische Ruimte of in een land dat bij besluit van de Europese Commissie op basis van het besluit van de Verwerkingsverantwoordelijke als veilig is aangemerkt. Modelcontractbepalingen zijn van toepassing in geval van doorgifte en verwerking buiten de Europese Economische Ruimte of een land dat bij besluit van de Europese Commissie op verzoek van de Verwerkingsverantwoordelijke als veilig is aangemerkt.

6. **Beveiliging.** De Verwerker is ISO 27001:2013-gecertificeerd en gebruikt het ISO 27001-raamwerk om een gelaagde verdediging als beveiligingsstrategie te implementeren bij het toepassen van beveiligingscontroles bij de laag van het netwerk, de besturingssystemen, databases, toepassingen, het personeel en de bedrijfsprocessen. Naleving van de reglementaire en contractuele vereisten wordt regelmatig beoordeeld en geëvalueerd, net als andere infrastructuur en bewerkingen van Verwerker, en de nodige stappen worden genomen om naleving ervan op een continue basis te waarborgen. De Verwerker heeft de beveiliging van de gegevens georganiseerd met behulp van ISMS op basis van ISO 27001. De beveiligingsdocumentatie omvat voornamelijk beleidsdocumenten voor informatiebeveiliging, fysieke veiligheid, beveiliging van apparatuur, incidentmanagement, behandeling van datalekken en veiligheidsincidenten, enz.

7. **Technische en organisatorische maatregelen**. Verwerker zal de Persoonsgegevens beschermen tegen onopzettelijke en onrechtmatige beschadiging en vernietiging, onopzettelijk verlies, wijziging, ongeoorloofde toegang en openbaarmaking. Hiertoe neemt de Verwerker passende technische en organisatorische maatregelen die overeenkomen met de wijze van verwerking en het risico dat de verwerking vormt voor de rechten van de Betrokkenen, in overeenstemming met de vereisten van de AVG. Een uitgebreide beschrijving van de technische en organisatorische maatregelen is te vinden in het Beveiligingsbeleid.

8. **Contactinformatie van Verwerker.** Alle kennisgevingen, verzoeken, eisen en andere mededelingen betreffende de bescherming van persoonlijke gegevens moeten worden gericht aan ESET, spol. s.r.o., ter attentie van: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal

remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer

and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including

measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely

identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data

(hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be

onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to

do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Privacybeleid

Per 21 maart 2023 | Een eerdere versie van het Privacybeleid bekijken | Wijzigingen vergelijken

De bescherming van persoonsgegevens is van bijzonder belang voor ESET, spol. s r. o., kantoorhoudende te Einsteinova 24, 851 01 Bratislava, Slovak Republic, ingeschreven in het handelsregister dat wordt beheerd door de rechtbank Bratislava I District Court, sectie Sro, volgnr. 3586/B, bedrijfsregistratienummer: 31333532 als verwerkingsverantwoordelijke ("ESET" of "Wij"). We willen voldoen aan de transparantievereiste zoals wettelijk gestandaardiseerd onder de Algemene Verordening Gegevensbescherming van de EU ("AVG"). Om dit doel te verwezenlijken publiceren Wij dit Privacybeleid met als enige doel om onze klant ("Eindgebruiker" of "U") als betrokkene over de volgende onderwerpen over bescherming van persoonsgegevens te informeren:

- Rechtsgrondslag van verwerking van persoonsgegevens,
- Gegevens delen en vertrouwelijkheid,
- Gegevensbeveiliging,
- Uw rechten als betrokkene,
- Verwerking van uw persoonsgegevens
- Contactinformatie.

Rechtsgrondslag van verwerking van persoonsgegevens

Er zijn slechts enkele rechtsgrondslagen voor de verwerking van gegevens die Wij hanteren overeenkomstig het toepasselijke wetgevingskader inzake de bescherming van persoonsgegevens. De verwerking van persoonsgegevens bij ESET is vooral noodzakelijk voor de uitvoering van de Gebruiksvoorwaarden Licentieovereenkomst voor eindgebruikers („Voorwaarden") met eindgebruiker (artikel 6, lid 1, onder b) AVG), die van toepassing is op de levering van ESET-producten of -services, tenzij uitdrukkelijk anders vermeld, bijvoorbeeld:

- Legitieme belangen (artikel 6, lid 1, onder f) AVG), een rechtsgrondslag op basis waarvan wij gegevens kunnen verwerken over hoe onze klanten onze Services gebruiken en hun instemming om onze gebruikers de beste beveiliging, ondersteuning en ervaring te kunnen geven die wij hun kunnen bieden. Zelfs marketing wordt door toepasselijke wetgeving erkend als een rechtmatig belang, en daarom vertrouwen wij hier doorgaans op voor de marketingcommunicatie met onze klanten.
- Toestemming (artikel 6, lid 1, onder a) AVG), die wij u kunnen vragen in specifieke situaties waarin wij deze rechtsgrondslag het geschiktst achten of indien de wet dit vereist.
- Naleving van een wettelijke verplichting (artikel 6, lid 1, onder c) AVG), bijvoorbeeld eisen inzake elektronische communicatie, het bewaren voor facturering of factureringsdocumenten.

Gegevens delen en vertrouwelijkheid

Wij delen uw gegevens niet met derden. ESET is echter een bedrijf dat als onderdeel van ons verkoop-, service- en ondersteuningsnetwerk wereldwijd actief is via gelieerde ondernemingen of partners. Informatie over licenties, facturering en technische ondersteuning die door ESET wordt verwerkt, kan worden overgedragen naar en van gelieerde entiteiten of partners om uitvoering te geven aan de Licentieovereenkomst voor eindgebruikers, zoals de levering van services of ondersteuning.

ESET verwerkt haar gegevens bij voorkeur in de Europese Unie (EU). Afhankelijk van uw locatie (gebruik van onze producten en/of services buiten de EU) en/of de service die u kiest, kan het echter nodig zijn om uw gegevens over te dragen naar een land buiten de EU. We gebruiken bijvoorbeeld services van derden in verband met cloud computing. In deze gevallen selecteren we onze serviceproviders zorgvuldig en zorgen we voor een passend niveau van gegevensbescherming door middel van zowel contractuele als technische en organisatorische

maatregelen. In de regel komen we de EU-modelcontractbepalingen overeen, indien nodig met aanvullende contractuele voorschriften.

Voor sommige landen buiten de EU, zoals het Verenigd Koninkrijk en Zwitserland, heeft de EU al een vergelijkbaar niveau van gegevensbescherming vastgesteld. Vanwege het vergelijkbare niveau van gegevensbescherming vereist de overdracht van gegevens naar deze landen geen speciale toestemming of overeenkomst.

We vertrouwen op services van derden voor wat betreft cloudcomputing. Deze worden geleverd door Microsoft, die onze cloudserviceprovider is.

Gegevensbeveiliging

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 relevante toezichthoudende autoriteit alsmede betreffende eindgebruikers als betrokkenen hiervan op de hoogte stellen.

Rechten van degene van wie de gegevens afkomstig zijn.

De rechten van elke Eindgebruiker zijn belangrijk en We willen u informeren dat alle Eindgebruikers (uit een EU of een niet-EU-land) de volgende rechten hebben die bij ESET worden gegarandeerd. Om de rechten van uw betrokkene uit te oefenen kunt u contact met ons opnemen via het ondersteuningsformulier of per e-mail op dpo@eset.sk. Voor identificatiedoeleinden vragen wij u om de volgende informatie: naam, e-mailadres en - indien beschikbaar - licentiecode of klantnummer en bedrijfsaffiliatie. Stuur ons geen andere persoonsgegevens, zoals geboortedatum. Wij willen u erop wijzen dat wij uw persoonsgegevens zullen verwerken om uw verzoek te kunnen verwerken, evenals voor identificatiedoeleinden.

Recht om de toestemming in te trekken. Het recht om de toestemming in te trekken is alleen van toepassing in geval van verwerking op basis van toestemming. Als Wij uw persoonsgegevens verwerken op basis van uw toestemming, hebt U het recht om de toestemming te allen tijde zonder opgaaf van redenen in te trekken. De intrekking van uw toestemming is alleen effectief voor de toekomst en heeft geen invloed op de rechtmatigheid van de gegevens die vóór de intrekking zijn verwerkt.

Recht van bezwaar. Het recht om bezwaar te maken tegen verwerking is alleen van toepassing in geval van verwerking op basis van het legitieme belang van ESET of derde partijen. Als Wij uw persoonsgegevens verwerken om een legitiem belang te beschermen, hebt U als betrokkene het recht om te allen tijde bezwaar te maken tegen het door ons genoemde legitieme belang en de verwerking van uw persoonsgegevens. Uw bezwaar is alleen effectief voor de toekomst en heeft geen invloed op de rechtmatigheid van de gegevens die vóór het bezwaar zijn verwerkt. Als wij uw persoonsgegevens verwerken voor direct marketing-doeleinden, is het niet nodig om uw bezwaar te motiveren. Dit geldt ook voor profilering, voor zover deze verband houdt met dergelijke direct marketing. In alle andere gevallen vragen wij u om ons kort te informeren over uw klachten tegen het legitieme belang van ESET om uw persoonsgegevens te verwerken.

Houd er rekening mee dat we in sommige gevallen, ondanks het intrekken van uw toestemming, het recht hebben om uw persoonsgegevens verder te verwerken op basis van een andere rechtsgrondslag, bijvoorbeeld voor de uitvoering van een contract.

Recht op inzage. Als betrokkene hebt U te allen tijde het recht om gratis informatie te verkrijgen over uw gegevens die door ESET zijn opgeslagen.

Recht op rectificatie. Indien wij per ongeluk onjuiste persoonsgegevens over U verwerken, hebt U het recht om dit te laten corrigeren.

Recht op gegevenswissing en recht op beperking van de verwerking. Als betrokkene hebt U het recht te vragen om de verwerking van uw persoonsgegevens te beperken of om uw persoonsgegevens te verwijderen. Als wij uw persoonsgegevens verwerken, bijvoorbeeld met uw toestemming, en U deze intrekt en er geen andere rechtsgrond is, bijvoorbeeld een contract, verwijderen we uw persoonsgegevens onmiddellijk. Uw persoonsgegevens worden ook verwijderd zodra ze niet langer nodig zijn voor de doeleinden die hiervoor zijn vermeld aan het einde van onze bewaartermijn.

Als we uw persoonsgegevens uitsluitend gebruiken voor direct marketing en u uw toestemming hebt ingetrokken of bezwaar hebt gemaakt tegen het onderliggende legitieme belang van ESET, zullen we de verwerking van uw persoonsgegevens beperken voor zover we uw contactgegevens opnemen in onze interne zwarte lijst om ongevraagd contact te voorkomen. Anders worden uw persoonsgegevens verwijderd.

Houd er rekening mee dat We mogelijk verplicht zijn om uw gegevens op te slaan tot het verstrijken van de bewaarverplichtingen en -termijnen die zijn uitgegeven door de wetgever of toezichthoudende autoriteiten. Bewaarverplichtingen en -termijnen kunnen ook voortvloeien uit de Slowaakse wetgeving. Daarna worden de bijbehorende gegevens routinematig verwijderd.

Het recht op overzetbaarheid van gegevens. Wij verstrekken aan U als betrokkene graag de persoonsgegevens die ESET verwerkt in het xls-formaat.

Het recht om een klacht in te dienen. Als betrokkene hebt U het recht om te allen tijde een klacht in te dienen bij een toezichthoudende autoriteit. ESET is onderworpen aan regelgeving van Slowaakse wetten en Wij zijn gebonden aan gegevensbeschermingswetgeving van de Europese Unie. De relevante toezichthoudende autoriteit voor gegevens is het Bureau voor de bescherming van persoonsgegevens van de Slowaakse Republiek, gevestigd op Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Verwerking van uw persoonsgegevens

Services geleverd door ESET en geïmplementeerd in ons op het web gebaseerd product worden geleverd volgens de voorwaarden van de Gebruiksvoorwaarden, maar bepaalde voorwaarden hebben mogelijk wat extra aandacht nodig. Wij willen u graag meer informatie geven over het verwerken van gegevens in verband met de levering van onze producten en services. Wij verzorgen verschillende services die zijn beschreven in de voorwaarden en het product documentatie. Om dit te kunnen doen, moeten wij de volgende informatie verzamelen:

Licentie- en factureringsgegevens. De naam, het e-mailadres, de licentiecode en (indien van toepassing) het adres, de bedrijfsaffiliatie en betalingsgegevens worden door ESET verzameld en verwerkt om de activering van de licentie, de levering van de licentiecode, herinneringen bij het verlopen, ondersteuningsverzoeken, verificatie van de echtheid van licenties, levering van onze services en andere meldingen waaronder marketingberichten, in overeenstemming met de toepasselijke wetgeving of uw toestemming, te vergemakkelijken. ESET is wettelijk verplicht om de factuurgegevens gedurende de periode van 10 jaar te bewaren, maar de licentie-informatie wordt uiterlijk 12 maanden na het verstrijken van de licentie geanonimiseerd.

Update en andere statistieken. De verwerkte informatie omvat 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 wordt verwerkt voor de levering van update- en upgradeservices en ten behoeve van het onderhoud, de beveiliging en de verbetering van onze back-end infrastructuur.

Deze informatie wordt gescheiden gehouden van de identificatie-informatie die vereist is voor de licentie- en factureringsdoeleinden, omdat hiervoor geen identificatie van de eindgebruiker is vereist. De bewaartermijn is maximaal 4 jaar.

ESET LiveGrid®-reputatiesysteem. Eénrichtings-hashes met betrekking tot infiltratie worden verwerkt ten behoeve van het ESET LiveGrid®-reputatiesysteem, dat de efficiëntie verbetert 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. De Eindgebruiker wordt tijdens dit proces niet geïdentificeerd.

ESET LiveGrid® Feedbacksysteem. 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 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.

Alle informatie die wordt verkregen en verwerkt via het ESET LiveGrid®-feedbacksysteem, is bedoeld om te worden gebruikt zonder de identificatie van de Eindgebruiker.

Technische ondersteuning. De contact- en licentiegegevens 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. De gegevens die worden verwerkt voor technische ondersteuning worden 4 jaar bewaard.

Let op: als de persoon die onze producten en services gebruikt, niet de Eindgebruiker is die het product of de service heeft gekocht en de Voorwaarden met ons heeft gesloten (bijv. een werknemer van de Eindgebruiker, een familielid of een persoon die anderszins gemachtigd is om het product of de service te gebruiken door de Eindgebruiker in overeenstemming met de Voorwaarden), wordt de verwerking van de gegevens uitgevoerd in het legitieme belang van ESET in de zin van artikel 6, lid 1, onder f) AVG om de door de Eindgebruiker geautoriseerde gebruiker in staat te stellen de door Ons geleverde producten en services te gebruiken in overeenstemming met de Voorwaarden.

Contactinformatie

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