ESET Cloud Office Security

Guia do Usuário

Clique aqui para exibir a versão da Ajuda deste documento

Digital Security
Progress. Protected.

ESET Cloud Office Security foi desenvolvido por ESET, spol. s r.o.

Para obter mais informações, visite https://www.eset.com.

Suporte técnico: https://support.eset.com

REV. 30-04-2024

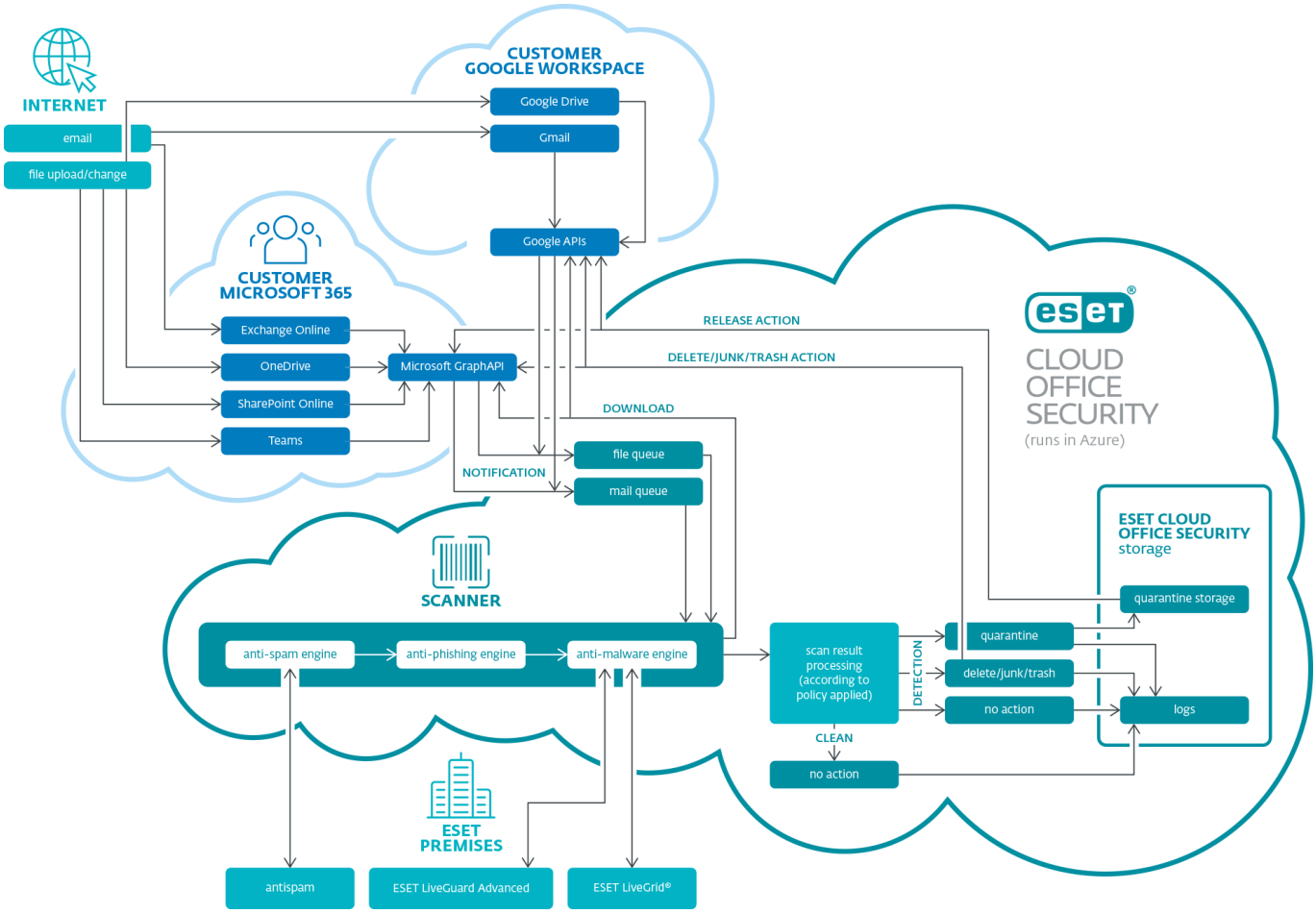
Visão geral

O ESET Cloud Office Security é um serviço em nuvem multilocatário e escalável no Microsoft Azure. O ESET Cloud Office Security é oferecido como um produto Software-as-a-Service (SaaS) que funciona totalmente na nuvem sem a necessidade de qualquer hardware. É a melhor combinação de filtragem de spam, escaneamento antimalware e proteção antiphishing que ajuda a proteger a comunicação da sua empresa contra malware, minimiza os efeitos adversos das mensagens não solicitadas na produtividade diária e impede que e-mails externos recebidos sejam usados como um canal para ataques direcionados.

Os serviços de segurança ESET Cloud Office Security abrangem os principais provedores de plataformas de nuvem e oferecem proteção abrangente de e-mail com mecanismos antimalware de ponta e ESET LiveGuard Advanced. Essa solução oferece defesa avançada contra ameaças por meio de sandbox baseado em nuvem, analisando amostras suspeitas em um ambiente isolado.

A arquitetura do ESET Cloud Office Security permite que você inicie a proteção rapidamente conectando-se à sua plataforma de nuvem do Microsoft 365 e do Google Workspace. Ele oferece o poder de gerenciar a proteção por meio de um console baseado na web acessível de qualquer lugar.

O ESET Cloud Office Security fornece proteção preventiva avançada para proteger os aplicativos Microsoft 365 da sua empresa - Exchange Online, OneDrive, SharePoint Online e Teams. A mesma proteção é fornecida aos aplicativos do Google Workspace: Gmail e Google Drive.



O ESET Cloud Office Security protege o OneDrive e a Caixa de entrada de usuários licenciados, assim como grupos de equipe e sites do SharePoint. Cada loja desses aplicativos Microsoft 365 está protegida, independentemente de quem carregou um arquivo ou quem enviou um e-mail. O conteúdo em si é protegido independentemente de quem seja o autor. O autor também pode ser um usuário convidado para garantir a melhor proteção possível.

Recursos chave

A tabela a seguir oferece uma lista de recursos disponíveis no ESET Cloud Office Security.

Vários locatários	Você pode proteger e gerenciar vários locatários do Microsoft 365 e do Google Workspace de um console ESET Cloud Office Security. O Azure Active Directory (Azure AD) organiza objetos como usuários e aplicativos em grupos chamados de locatários. Os locatários permitem que você defina políticas para usuários e aplicativos dentro da sua empresa para cumprir as políticas operacionais e de segurança.

Antispam	O Antispam é um componente essencial de qualquer servidor de e-mail. O ESET Cloud Office Security usa um mecanismo antispam com tecnologia de ponta que impede as tentativas de spam e phishing com taxas de sucesso muito altas. O ESET Cloud Office Security foi campeão consecutivamente de testes de filtragem de spam realizados pela Virus Bulletin, uma autoridade líder em testes de segurança, e recebeu a certificação VBSpam+ por vários anos. O mecanismo Antispam alcançou 99,99% da taxa de detecção de spam com zero falso positivos, fazendo dele uma tecnologia líder na indústria de proteção contra spam. O ESET Cloud Office Security Antispam é baseado na nuvem e a maioria dos banco de dados da nuvem estão localizados nos centros de dados da ESET. Os serviços de nuvem do Antispam permitem atualizações de dados imediatas, que fornecem um tempo de reação mais rápido quando surge um spam.
Proteção antiphishing	Esse recurso impede os usuários de acessarem páginas da web conhecidas por phishing. Mensagens de e-mail podem conter links que levam a páginas da web de phishing e o ESET Cloud Office Security usa um pareador sofisticado que pesquisa no corpo da mensagem e no assunto de mensagens de e-mail recebidas para identificar esse tipo de link (URLs). Os links são comparados contra um banco de dados de phishing que é atualizado continuamente.
Proteção Antimalware	Uma defesa premiada e inovadora contra malware, essa tecnologia de ponta impede ataques. Elimina todos os tipos de ameaças, inclusive vírus, ransomware, rootkits, worms e spyware com escaneamento ativado por nuvem para taxas de detecção ainda melhores. Sua pegada pequena não pesa nos recursos do sistema e não compromete o desempenho. A detecção Antimalware usa um modelo de segurança em camadas. Cada camada, ou fase, tem várias tecnologias principais. A fase Pré-execução inclui as tecnologias a seguir: Escaneador UEFI (Unified Extensible Firmware Interface), Proteção de ataque a rede, Reputação e Cache, Sandbox no produto, Detecções de DNA. As tecnologias da fase de Execução são o Bloqueio de Exploit, Escudo Anti-ransomware, Escaneador de memória avançado e Escaneador de script (AMSI). A fase Pós-execução usa a Proteção contra botnet, Sistema de proteção contra malware em nuvem e Área de segurança. Este conjunto avançado de recursos de tecnologias centrais fornece um nível de proteção inigualável.
Políticas	Empresas maiores geralmente têm vários departamentos e querem configurar diferentes configurações de proteção para cada unidade organizacional. O ESET Cloud Office Security fornece configurações de proteção baseadas em políticas que podem ser atribuídas a Locatários, Usuários, Grupos de equipe ou sites SharePoint selecionados. Você pode personalizar cada política de acordo com suas necessidades.
Gerente de quarentena	Inspecione os objetos em quarentena e execute uma ação adequada (fazer download, remover ou liberar). Este recurso oferece o gerenciamento simples de mensagens de e-mail, anexos, e também arquivos do Exchange Online / OneDrive / Grupos de equipe / sites SharePoint que foram colocados em quarentena pelo ESET Cloud Office Security. Fazer download dá a você a opção de analisar objetos em quarentena com ferramentas de terceiros, se necessário, o que pode ajudar a decidir a ação a ser tomada.
Painel com estatísticas de detecção	Obtenha uma visão geral rápida das atividades de segurança dentro do Microsoft 365. O painel fornece informações essenciais em cada uma de suas guias de visão geral (Exchange Online/OneDrive/Grupos de equipe/sites do SharePoint). Visão geral do usuário mostra o número de Locatários e uso de Licença, bem como estatísticas por cada Locatário – Número de usuários, Principais destinatários de spam/phishing/malware e Principais contas suspeitas do OneDrive, Principais grupos de Equipe suspeitos e sites SharePoint. Você pode escolher exibir as estatísticas de um período de tempo e um Locatário. Outras estatísticas de detecção e gráficos estão visíveis nas guias de visão geral do Exchange Online, OneDrive, Grupos de equipe e sites do SharePoint. Essas são estatísticas, como o número de e-mails e arquivos escaneados, e o número de spam/phishing/malware detectados. Os gráficos mostram o tráfego para cada tipo de detecção: spam, malware e phishing.
Detecções com opções de filtragem	Este recurso contém todos os registros sobre detecções. Os registros incluem relatórios de cada detecção por escaneamento de e-mail na guia Exchange Online e escaneamento de arquivo nas guias OneDrive/Grupos de equipe/Sites SharePoint. Isso possibilita filtrar e encontrar de maneira eficaz o que você está procurando usando informações adicionais sobre a detecção específica (por exemplo, um nome da infiltração, o hash do arquivo).

Usuários	A entidade central que o ESET Cloud Office Security protege é a conta do usuário. Encontre informações úteis abrindo os Detalhes de um usuário, como Visão geral, Configurações definidas por Políticas, lista de Políticas atribuídas ao usuário e Detecções para o Exchange Online e OneDrive. Esse recurso ajuda quando você precisa investigar detecções relacionadas a um usuário específico. Você também pode escolher quais usuários proteger. Os usuários são organizados em grupos. Os usuários são classificados em grupos, cada grupo é um locatário do Microsoft 365 contendo seus usuários. Usa vários critérios de filtragem para que seja mais fácil pesquisar um usuário específico dentro de um grupo.
Proteção de relatórios e aprendizado de máquina	O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção com base no aprendizado de máquina. Leia mais sobre esse tipo de proteção no glossário. Você pode configurar os Níveis de relatório para as categorias a seguir: Malware, Aplicativos potencialmente indesejados (PUAs), Aplicativos potencialmente suspeitos e Aplicativos potencialmente não seguros.
Relatórios (Quarentena estatística e de e-mail)	Receba dados estatísticos para a proteção do Exchange Online, OneDrive, grupos de equipe e sites do SharePoint por e-mail, ou gere e faça download de um relatório para um período de tempo escolhido. Você pode agendar relatórios a serem gerados e distribuídos a destinatários de e-mail especificados regularmente. Escolha PDF ou CSV como um formato de saída. Os relatórios contêm dados como o número de e-mails escaneados, malware detectado, phishing e spam. O formato PDF inclui dados mostrados em gráficos. E-mails escaneados, tráfego de malware, tráfego de phishing e tráfego de spam – há um gráfico para cada. Também existem estatísticas separadas para os principais destinatários de cada categoria: malware, phishing e spam. Há várias opções disponíveis para gerar relatórios. Além disso, você pode ter um Relatório de quarentena de e-mail — uma lista de mensagens de e-mail em quarentena — entregue aos destinatários selecionados. O relatório de Quarentena de e-mail é enviado na data e hora especificadas, mas apenas se houver novos itens a serem reportados.
Equipes e sites	O ESET Cloud Office Security fornece proteção para Grupos de equipe ou sites do SharePoint. Isso amplia a proteção para soluções de colaboração da Microsoft 365 ao proteger o SharePoint e as Equipes, permitindo o compartilhamento de arquivos protegido. Se você estiver usando o ESET Cloud Office Security, pode ser solicitado que você atualize o consentimento antes de usar o Equipes e sites.
ESET LiveGuard Advanced	Uma camada adicional de proteção contra ameaças avançadas de dia zero. O ESET LiveGuard Advanced é uma solução de sandbox baseada em nuvem que analisa os arquivos enviados ao executar um código suspeito em um ambiente isolado para avaliar seu comportamento. O ESET Cloud Office Security envia anexos de e-mail suspeitos e arquivos do Exchange Online, OneDrive, Grupos de equipe e sites do SharePoint para análise pelo ESET LiveGuard Advanced. Ativar e configurar o recurso ESET LiveGuard Advanced usando as políticas. Os resultados da análise são mostrados em Relatórios do escaneamento.
Relatório de auditoria	O Relatório de auditoria permite ao Administrador inspecionar as atividades realizadas no ESET Cloud Office Security. Este recurso pode ser útil, especialmente quando você tem vários usuários do console ESET Cloud Office Security. Os registros de Relatório de auditoria não fazem parte das atividades e mostram a sequência na qual ocorreram. Os relatórios de auditoria armazenam informações sobre a operação ou evento específico. Os relatórios de auditoria são criados sempre que um objeto ESET Cloud Office Security (pool de licenças, usuário, política, relatório, item de quarentena como anexo) é criado ou modificado.
Google Workspace (proteção para o Gmail e Google Drive)	O ESET Cloud Office Security expande a cobertura de serviços de segurança para outro provedor líder de e-mail na nuvem, o Google Workspace. O ESET Cloud Office Security fornece proteção abrangente aos usuários do Gmail e do Google Drive, utilizando todos os seus recursos. Ele mantém os usuários do Google Workspace protegidos contra malware, phishing e spam.

O que há de novo

Informações sobre novos recursos e melhorias implementadas em cada versão ESET Cloud Office Security:

Portal versão 353 lançado em 23 de novembro de 2023

- Integração com o Google Workspace adicionada.
- Navegador de produto para acessar rapidamente o ESET Business Account (mais consoles a seguir nos próximos meses).
- *Outras correções de bugs e melhorias de backend.*

Portal versão 342.3 lançado em 24 de outubro de 2023

- Adicionada a verificação de conta de administrador do Google Workspace.
- Tipo de coluna Usuário adicionada.
- *Outras correções de bugs e melhorias de backend.*

Portal versão 311.2 lançado em 31 de julho de 2023

- Google Workspace Adicionado (proteção do Gmail e Google Drive) – acesse os Recursos de visualização nos Links rápidos.
- Tema Modo escuro adicionado.
- Navegador de produto adicionado para usuários de acesso antecipado do ESET HUB.
- *Outras correções de bugs e melhorias de backend.*

Portal versão 293.7 lançado em 13 de julho de 2023

- Associação de locatários adicionada aos sites da ESET Business Account (EBA). Essa alteração garante a compatibilidade com o futuro portal do cliente ESET PROTECT HUB, que substituirá o ESET MSP Administrator (EMA) e o ESET Business Account (EBA). Isso afeta apenas alguns clientes que usam licenças de vários sites para proteger um único locatário. Se esse for o seu caso, você será solicitado a associar seus locatários aos sites da EBA.
- Outras pequenas melhorias e correções de bugs.

Portal versão 251.1 lançado em 21 de março de 2023

- Melhorias no carregamento lento de telas para melhor suporte a locatários com dezenas de milhares de usuários.
- Alterações no assistente para adicionar locatário.
- Atualizações na página Sobre.
- Atualizações dos Termos de Uso e Política de Privacidade (Política de retenção de dados e limitações).

Portal versão 205 lançado em 9 de novembro de 2022

- Foi adicionada uma nova janela que deve aparecer quando você entrar pela primeira vez no console ESET Cloud Office Security, descrevendo os recursos adicionados recentemente.
- Opção para exportar Relatórios do escaneamento e Relatório de auditoria para o arquivo CSV.
- Nova configuração adicionada à Mesclar políticas com listas e e-mails de notificação.

Portal versão 180.2 lançado em 27 de julho de 2022

- O novo recurso Relatório de auditoria.
- Relatórios de alteração para Relatórios do escaneamento.

Portal versão 156.2 lançado em 26 de abril de 2022

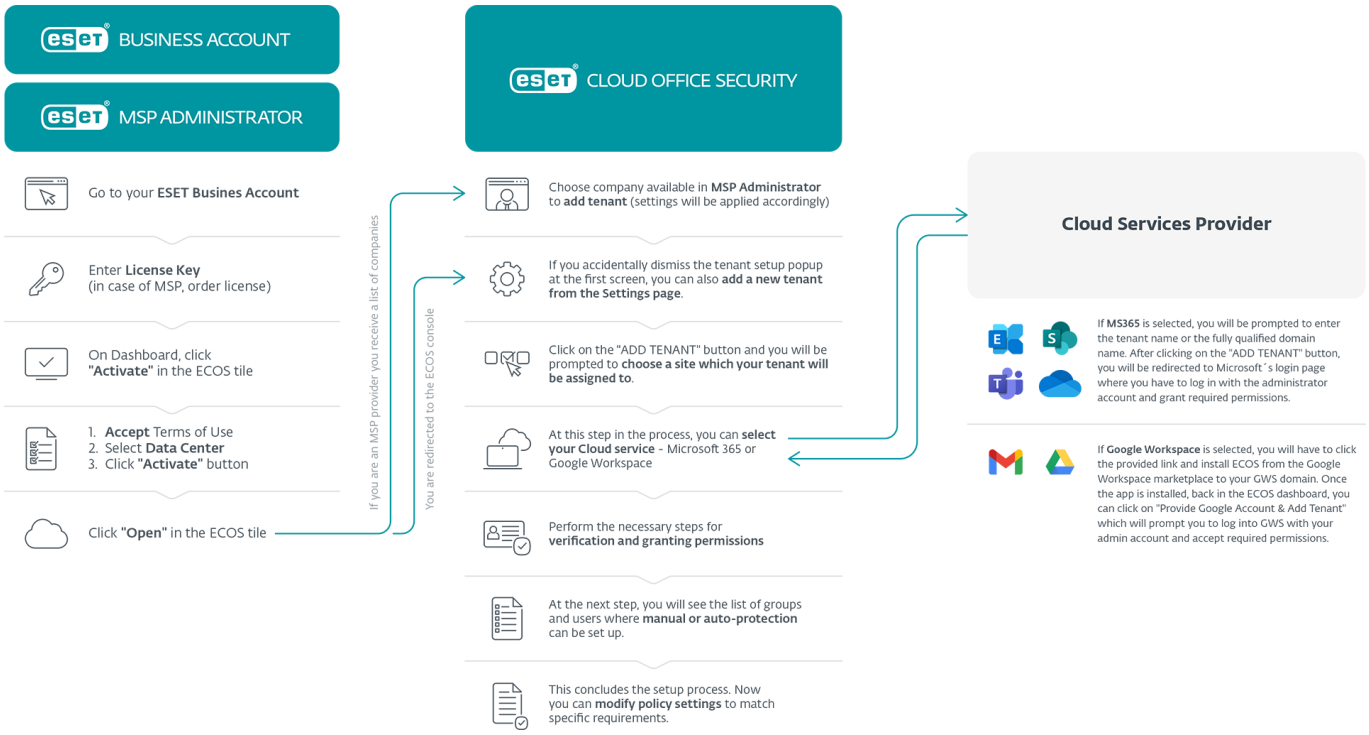
- O Dynamic Threat Defense foi renomeado para ESET LiveGuard Advanced.
- Envio de amostras falso positivo/falso negativo para análise.
- Importar/exportar listas aprovadas, bloqueadas e ignoradas nas Políticas.
- O Painel exibe a contagem de usuários desprotegidos na guia Visão geral.
- Corrigido um bug que estava colocando e-mails de notificação na quarentena.

Portal versão 140.6 lançado em 9 de fevereiro de 2022

- Habilidade de dar whitelabel aos relatórios (apenas co-branding ou logotipo personalizado).
- Opção para definir o idioma preferido para o e-mail de notificação (notificações do proprietário da caixa de entrada).
- Opção para definir o idioma preferido para notificações por e-mail para membros locatários.
- Filtrar e-mails por ID de mensagem.

Integração

O fluxo de integração do ESET Cloud Office Security com seu provedor de serviços em nuvem:



Especificações

Especificações técnicas de referência para ESET Cloud Office Security:

- Requisitos
- Planos da Microsoft 365 compatíveis
- Planos compatíveis do Google Workspace
- Navegadores da Web compatíveis

- Limitações e Política de retenção de dados

Requisitos

Para aproveitar o serviço ESET Cloud Office Security protegendo seu Microsoft 365, o seguinte é necessário:

- Plano de assinatura Microsoft 365 compatível
- Acesso do Administrador para o Azure Active Directory (Azure AD)
- Azure Cloud Services – Exchange | OneDrive
- Uma conta no portal ESET Business Account ou ESET MSP Administrator

Planos da Microsoft 365 compatíveis

o ESET Cloud Office Security é compatível com os seguintes planos do Microsoft 365, Exchange Online e OneDrive.

Planos enterprise da Microsoft 365:

- 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

Planos empresariais da Microsoft 365:

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

Planos de educação da Microsoft 365:

- Microsoft 365 A3
- Microsoft 365 A5

Planos do Exchange Online:

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

Planos do OneDrive:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Planos compatíveis do Google Workspace

O ESET Cloud Office Security é compatível com os seguintes planos do Google Workspace.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Navegadores da Web compatíveis

> Para uma melhor experiência com o console web ESET Cloud Office Security, recomendamos manter seus navegadores web atualizados.

Você pode usar o console ESET Cloud Office Security com os seguintes navegadores da web:

- Mozilla Firefox 69 e versões mais recentes
- Microsoft Edge 44 e versões mais recentes
- Google Chrome 77 e versões mais recentes
- Opera 63 e versões mais recentes
- Safari 13.x e versões mais recentes

> Não é compatível com o Microsoft Internet Explorer.

Limitações e Política de retenção de dados

Em certas circunstâncias, existem ESET Cloud Office Security limitações de escaneamento. Um arquivo não é escaneado e será exibido em Relatórios do escaneamento como **Não escaneado** se o seguinte acontecer:

- O tamanho do arquivo for de mais de 200 MB
- O escaneamento levar mais de 2 minutos e expirar
- O arquivo tem um nível de compactação de 10 ou mais (geralmente um arquivo que é conhecido como bomba de arquivo ou bomba de zip)
- O arquivo é protegido por senha
- O arquivo está danificado

Limites de quarentena (quando liberado da quarentena):

- 15 MB para um anexo de e-mail
- 150 MB para toda a mensagem de e-mail, incluindo anexos

Política de retenção de dados:

Entidade	Período de retenção	Comentário
Objetos em quarentena	30 dias	Objetos com mais de 30 dias serão removidos permanentemente.
Detecções	90 dias	Registros anteriores a 90 dias serão removidos permanentemente.
Registros de relatórios do escaneamento	90 dias	Registros anteriores a 90 dias serão removidos permanentemente.
Registros de relatórios do escaneamento com resultado de Escaneamento limpo	3 dias	Se você tiver uma política que usa Registrar todos os objetos, resultados de escaneamento limpos com mais de 3 dias serão removidos permanentemente.
Backup do banco de dados do ESET Cloud Office Security	90 dias	Backups anteriores a 90 dias serão removidos permanentemente.
Relatórios de auditoria	90 dias	Registros anteriores a 90 dias serão removidos permanentemente.
Relatórios de insights do aplicativo	90 dias	Registros anteriores a 90 dias serão removidos permanentemente.

Locatário removido do console ESET Cloud Office Security

Quando você remove um locatário do console ESET Cloud Office Security, o período de retenção para dados do locatário é de 30 dias (Quarentena, Relatórios do escaneamento e Estatísticas são removidos depois de 30 dias). Se você adicionar o locatário novamente dentro de 30 dias, todos os dados serão restaurados. Outros objetos (locatários, usuários, grupos, sites, relatórios, políticas) são removidos permanentemente depois de 90 dias.

ESET Cloud Office Security desativado no ESET Business Account ou ESET MSP Administrator

Se você desativar o ESET Cloud Office Security no ESET Business Account ou ESET MSP Administrator, esse processo também removerá os locatários do ESET Cloud Office Security. A remoção do ESET Cloud Office Security é permanente e os dados excluídos não podem ser restaurados.

Escaneamento antispam:

O ESET Cloud Office Security escaneia as mensagens de e-mail armazenadas nas caixas de entrada em busca de spam. Por isso, o ESET Cloud Office Security não consegue impedir que um usuário envie uma mensagem de spam para um endereço de e-mail externo. Em um cenário improvável, quando as credenciais de usuário do Office 365 são roubadas, as credenciais podem ser usadas por um spam para enviar mensagens spam em massa (tráfego de e-mail de saída).

Licenciamento para o ESET Cloud Office Security

Gerenciar licenças ESET Cloud Office Security via ESET Business Account ou ESET MSP Administrator. Experimente o ESET Cloud Office Security com uma licença de avaliação de 30 dias.

- Consulte ESET Business Account para criar uma conta, adicionar uma licença ou gerenciar uma licença.
- Veja ESET MSP Administrator se você for um MSP.

ESET Business Account e ESET MSP Administrator (conta de licenciamento híbrido)

Se você tiver o mesmo endereço de e-mail registrado no ESET MSP Administrator e no ESET Business Account (login único), você pode alternar entre a visualização do ESET Business Account e a do ESET MSP Administrator. Proteja os usuários ou as empresas usando o Gerenciamento de licenças para o ESET Cloud Office Security.

Período de carência para licença expirando em ESET Business Account

Quando sua licença estiver perto de expirar, um alerta será exibido na interface ESET Business Account. Se a data de expiração passar e você não renovar sua licença ou ativar uma nova licença, o alerta de licença expirada será exibido em ESET Business Account. Se não houver uma licença elegível uma notificação de que sua licença será suspensa em 14 dias será exibida no ESET Business Account e você receberá um e-mail no endereço especificado na sua conta de administrador.

Você tem um período de carência de 14 dias para renovar depois que sua licença expirar. Você será notificado no ESET Business Account e por e-mail no meio do período de carência. Depois de 14 dias o uso do seu ESET Cloud Office Security será suspenso. A conta ficará inacessível e não funcional. Uma conta ESET Cloud Office Security suspensa será armazenada e acessada novamente adicionando uma nova licença ESET Cloud Office Security ao ESET Business Account. Sua instância ESET Cloud Office Security pode permanecer suspensa por até 30 dias, depois desse período ela será removida permanentemente.

Se sua conta entrar em um estado suspenso você será notificado no ESET Business Account e por e-mail 14 dias antes de sua instância ser removida. Você deve ativar uma nova licença elegível ESET Cloud Office Security para restaurar o acesso a sua conta ESET Cloud Office Security.

> **i** Os usuários continuam a estar totalmente protegidos durante o período de carência. Quando o período de carência acabar, os usuários vão ficar desprotegidos.

Licença suspensa

Se não houver uma licença ESET Cloud Office Security válida presente no ESET Business Account, sua instância ESET Cloud Office Security será suspensa. A instância vai se tornar inacessível e não-funcional. Sua instância ESET Cloud Office Security pode permanecer suspensa por até 30, depois desse período ela será removida permanentemente. Você deve ativar uma nova licença elegível ESET Cloud Office Security para restaurar o acesso a sua instância ESET Cloud Office Security.

ESET Business Account

O ESET Business Account funciona como um ponto de acesso unificado para o ESET Business Account e o ESET Cloud Office Security. Use a página de login ESET Cloud Office Security ou ESET Business Account para acessar seu ESET Cloud Office Security. Ambas as páginas redirecionam você por meio da autenticação ESET Business Account para verificar seu login.

- Crie uma nova conta se você não tiver uma conta registrada no ESET Business Account.
- Se você tiver uma conta ESET Business Account, adicione sua licença ESET Cloud Office Security.
- Gerenciar ESET Business Account.

Criar uma nova conta ESET Business Account

1. Abra a página de login ESET Business Account e clique em **Registre gratuitamente**. Preencha o formulário cuidadosamente para se registrar. O endereço de e-mail inserido será usado como seu nome de login.

2. A senha deve ter no mínimo 10 caracteres. Preencha seu **Nome** e **Detalhes da empresa** e clique em **Continuar**. Leia e confirme se você concorda com os **Termos de uso da ESET**. Complete o formulário reCAPTCHA e clique em **Registrar**.

3. Você receberá um e-mail de confirmação depois do registro bem sucedido (isso pode levar até 15 minutos). Clique no link no e-mail de configuração para abrir uma nova janela **Ativar conta**.

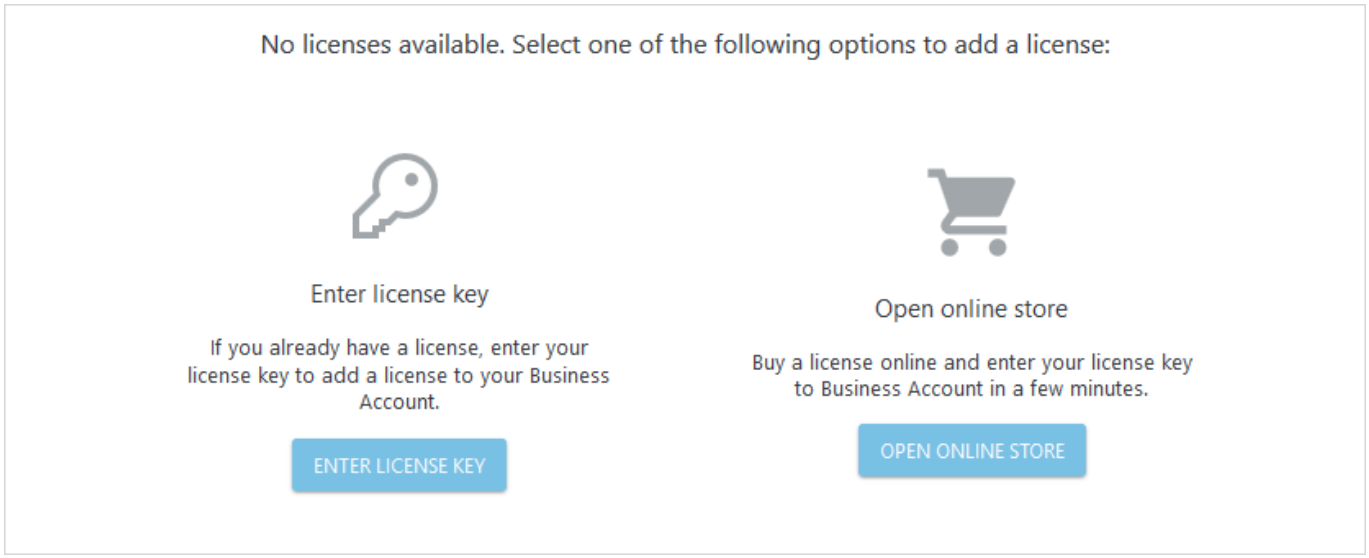
4. Digite sua senha e clique em **Ativar** para ativar sua ESET Business Account. Você receberá outro e-mail verificando que sua conta ESET Business Account foi criada com sucesso. Agora você está pronto para entrar na sua ESET Business Account.

Depois de ativar o ESET Business Account, adicione sua licença ESET Cloud Office Security.

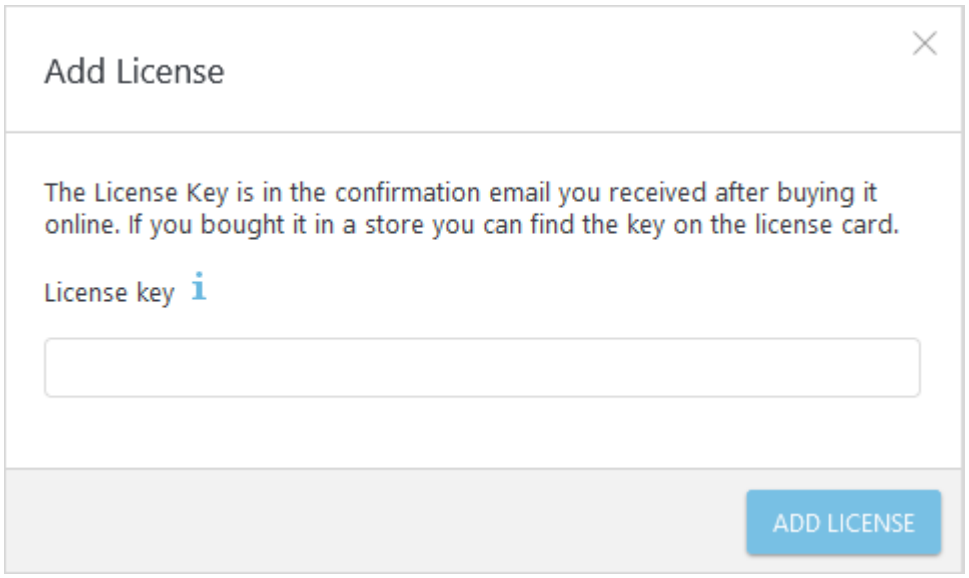
Adicionar licença ESET Cloud Office Security em ESET Business Account

Depois de um login bem-sucedido na ESET Business Account, você verá uma tela de boas-vindas para o ESET Business Account se essa for sua primeira vez como usuário.

1. Clique em **Adicionar licença** para abrir a janela de licenças. Se você for um usuário ESET Business Account regular, vá para a guia **Licença** e clique em **Adicionar licença**.



2. Insira sua **Chave de licença** e clique em **Adicionar licença**.



3. Você receberá um e-mail com um link de verificação. Clique no link e digite suas credenciais de login no portal ESET Business Account quando solicitado. Para obter mais informações sobre o gerenciamento de licenças, usuários e sites consulte o guia ESET Business Account .

Gerenciar ESET Business Account

Atividades comuns relacionadas ao licenciamento:

Sites e pool de licença

As licenças e os pools de licença são carregados do ESET Business Account. Pools de licença estão disponíveis apenas se você tiver sites existentes no ESET Business Account.

Criar um novo usuário no ESET Business Account

Você pode criar um usuário para ajudá-lo a gerenciar um compartilhamento de suas licenças.

1. Abra o ESET Business Account e entre.

2. Selecione **Gerenciamento de usuários**, clique em **Novo usuário** e digite as informações necessárias.

3. Selecionar ESET Cloud Office Security **Direitos de acesso** para um usuário:

   • **Leitura** – o usuário tem um acesso ao ESET Cloud Office Security, consegue ver usuários, relatórios, detecções, mas não pode gerenciar políticas, proteger os usuários ou liberar da quarentena.

   • **Gravação** – o usuário tem um acesso completo ao ESET Cloud Office Security, consegue ver e gerenciar usuários, colocar em quarentena ou criar uma política.

   • **Sem acesso** – O usuário não pode acessar o ESET Cloud Office Security

4. Defina um idioma nas **Preferências** do usuário para o console ESET Cloud Office Security.

5. Clique em **Criar** e o usuário será criado.

Criar um novo Site no ESET Business Account

Os sites permitem que você divida ou mescle suas licenças em pools de licença. Sites são grupos individuais com sua própria localização e administradores.

1. Abra o ESET Business Account e entre.

2. Selecione **Detalhes**, clique em **Criar site** e digite as informações pessoais necessárias.

3. Clique em **Adicionar usuário**, selecione o usuário e clique em **Confirmar**.

4. No pool de licenças, clique em **Adicionar unidades** e selecione a licença ESET Cloud Office Security. Você pode alterar as **Subunidades** e clicar em **Confirmar.**

5. Clique em **Criar** e o site será criado.

ESET MSP Administrator

ESET MSP Administrator é um sistema de gerenciamento de licenças que permite ao usuário MSP criar vários Clientes MSP e gerar licenças específicas com uma contagem de licenças. O portal de licenciamento ESET MSP Administrator oferece suporte a preços por volume e faturamento com base em um número exato de dias de licença comprados.

O ESET Cloud Office Security está disponível para todos os MSP Managers, MSPs e managed MSPs. O usuário ESET MSP Administrator com acesso de gravação é elegível para ativar o ESET Cloud Office Security. O ESET Cloud Office Security pode ser acessado por usuários com direitos de acesso de Gravação, Leitura ou Personalizado.

• Criar um novo cliente MSP (o endereço de e-mail do Cliente é necessário para ativação do console ESET Cloud Office Security).

• Ative o ESET Cloud Office Security do ESET MSP Administrator.

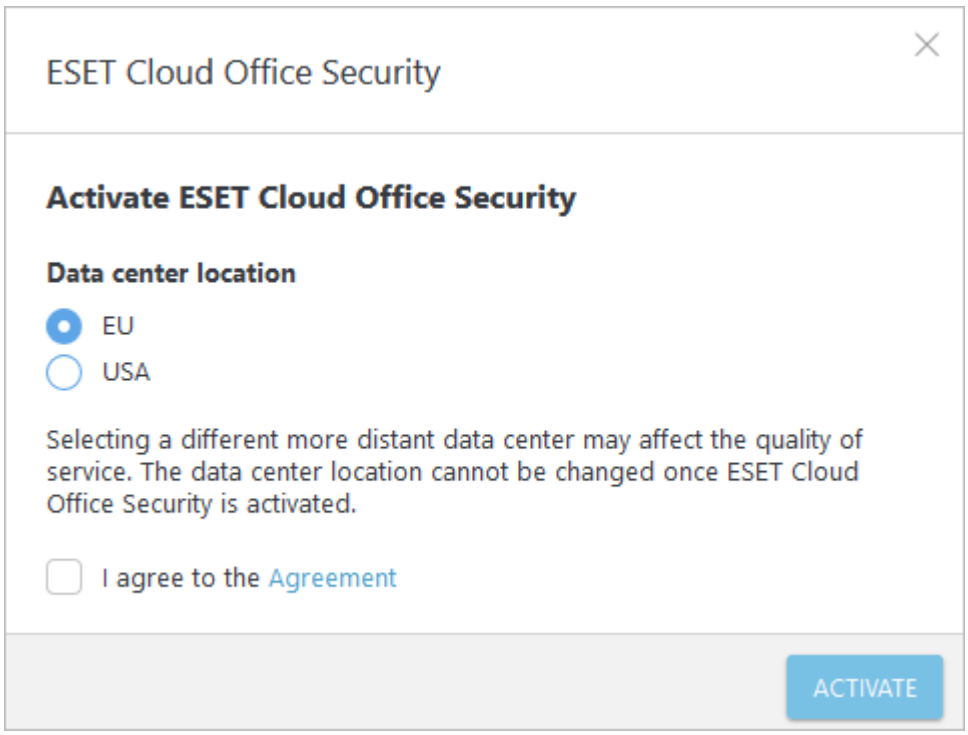
Ativar ESET Cloud Office Security

1. Entre no ESET Business Account ou ESET MSP Administrator e localize o bloco ESET Cloud Office Security no **Painel**.

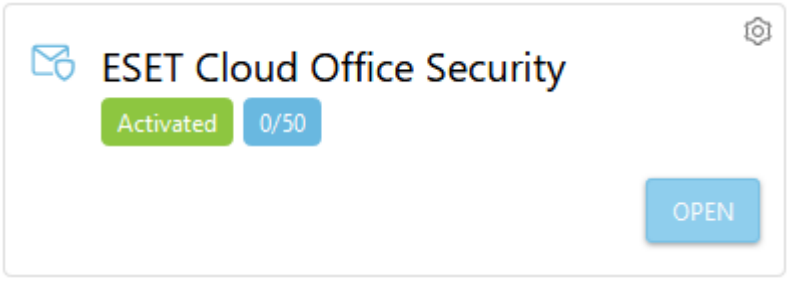
2. Clique em **Ativar** no canto inferior direito do bloco ESET Cloud Office Security.

3. O assistente de ativação consultará os Termos de uso ESET Cloud Office Security e exibirá o local ideal do centro de dados com base em sua localização atual. Selecione **Concordo com os Termos de uso** e clique em **Ativar**. Não recomendamos alterar o local do centro de dados. Porém, você poderá fazer sua seleção se precisar usar outro local.

Os centros de dados são completamente separados. Assim que você selecionar o local do centro de dados, ele não poderá ser alterado e não será possível migrar para outro local. Para alterar o centro de dados, inicie o processo de ativação do início.

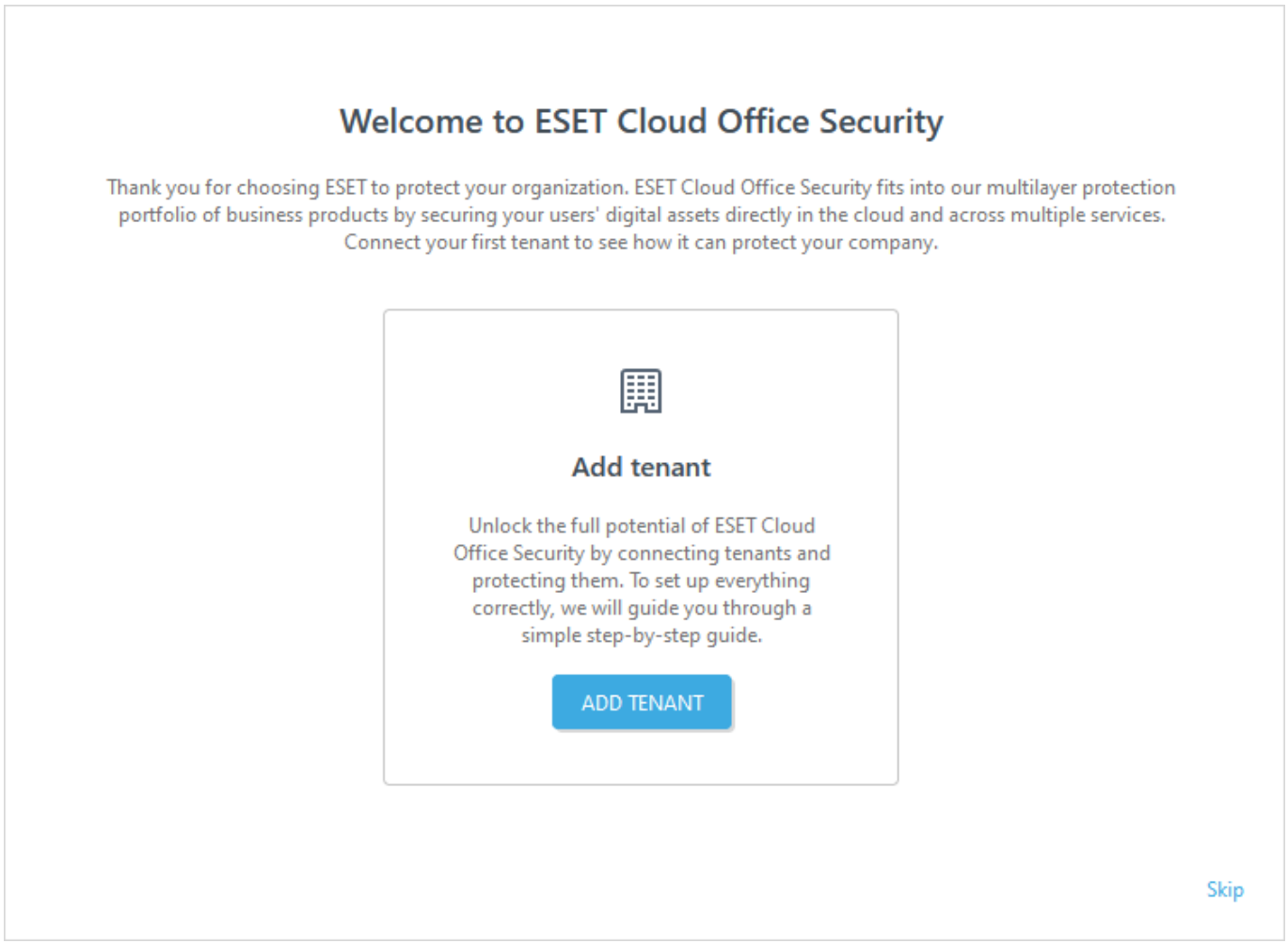


4. Clique em **abrir** no bloco ESET Cloud Office Security. O Painel ESET Cloud Office Security será aberto em uma nova guia do navegador.

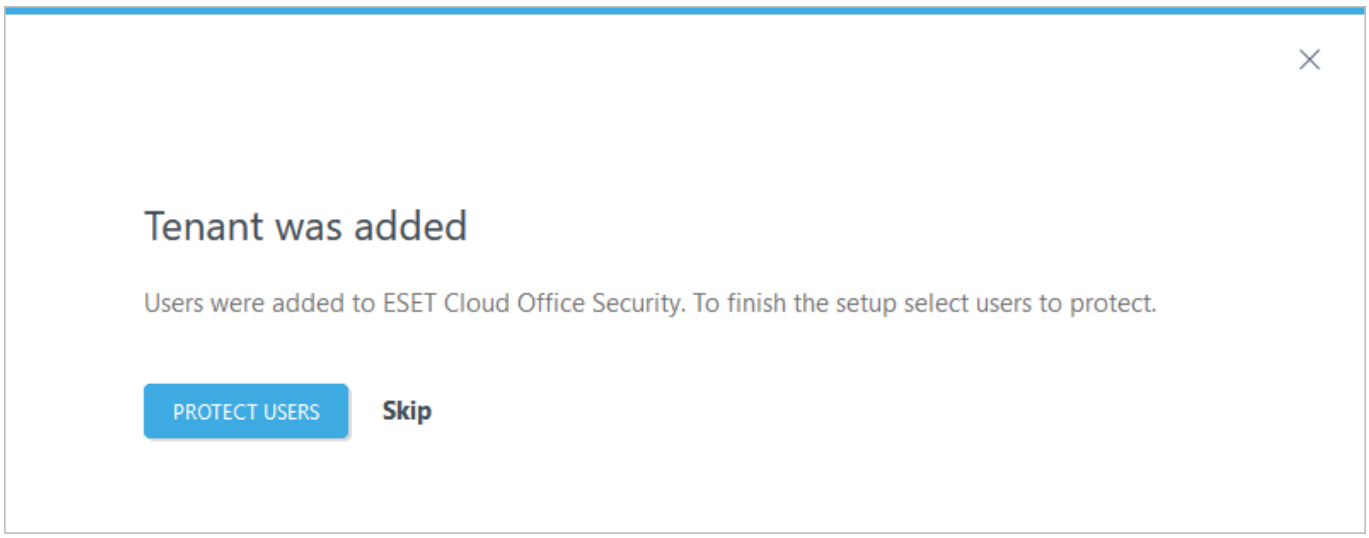


Ao entrar no ESET Cloud Office Security pela primeira vez, um **Assistente de inicialização** aparecerá. Este assistente conduzirá você pelo processo de implantação inicial.

1. Adicione seu locatário (Microsoft 365 ou Google Workspace).



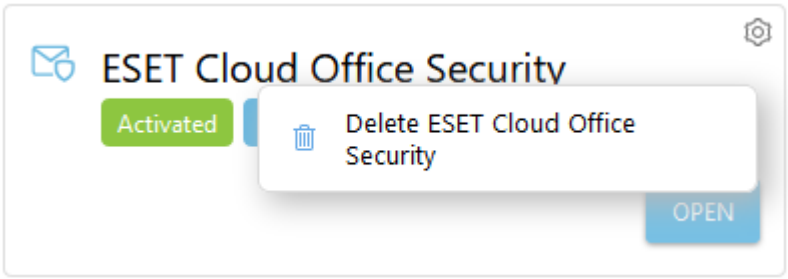
2. Proteger usuários Se você **Ignorar**, você pode proteger o usuário ou as empresas mais tarde usando o Gerenciamento de licenças para o ESET Cloud Office Security.



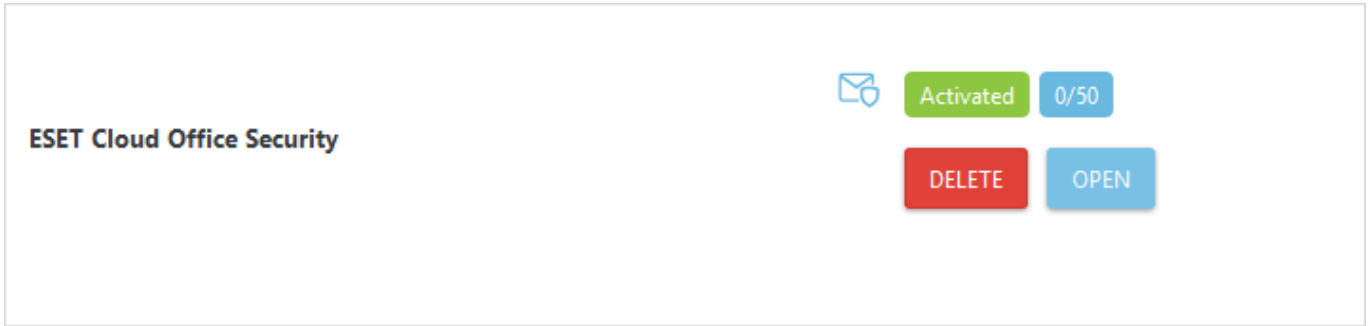
Desativar ESET Cloud Office Security

1. Entre no ESET Business Account ou ESET MSP Administrator e localize o bloco ESET Cloud Office Security no **Painel**.

2. Clique no ícone de engrenagem no canto superior direito do bloco ESET Cloud Office Security e selecione **Remover ESET Cloud Office Security**.

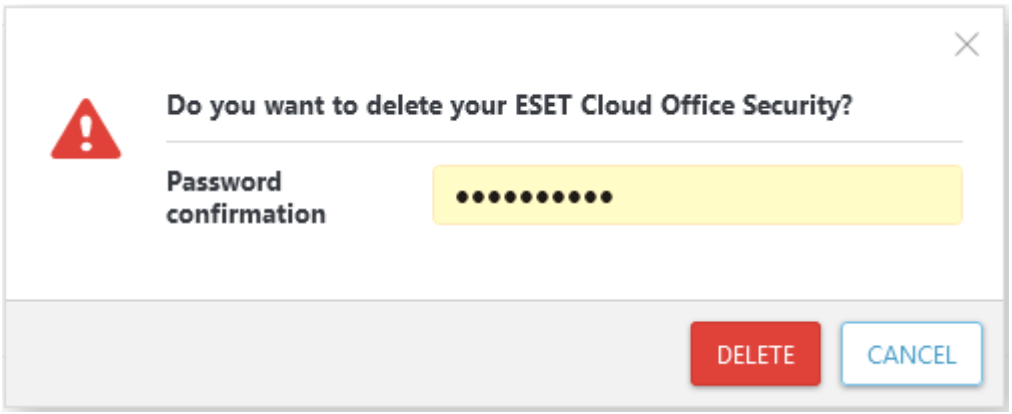


3. Alternativamente, navegue até a seção **Detalhes** e clique em **Remover**.



4. Uma janela de aviso aparece, avisando que todos os dados estão prestes a serem removidos. Digite sua senha ESET Business Account para confirmar e clique em **Remover**.

A remoção do ESET Cloud Office Security é permanente. Dados removidos não podem ser restaurados.



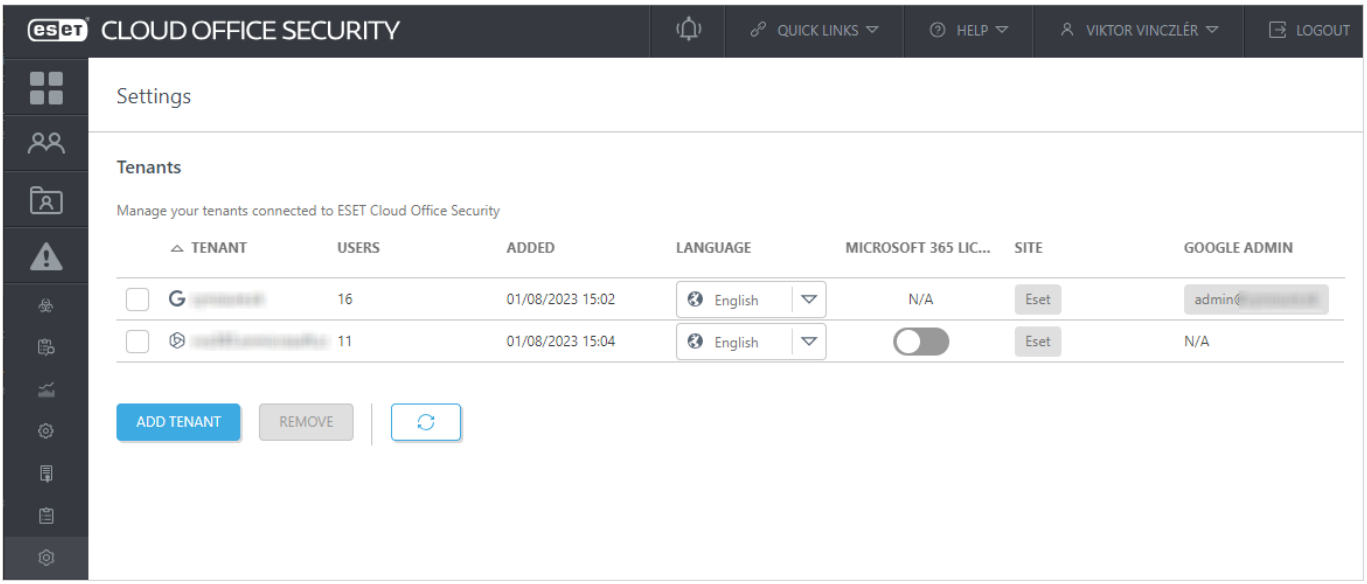
A ESET Cloud Office Security instância agora foi removida e o bloco de produto ESET Cloud Office Security reverte para o estado **Não ativado**. Você também receberá um e-mail de confirmação de ESET Business Account.

Gerenciar seus locatários em Configurações

Gerenciar locatários conectados ao ESET Cloud Office Security. Você pode ver todos os locatários registrados na tabela com detalhes para cada locatário. Use o botão Atualizar para recarregar a tabela com locatários.

Se quiser adicionar um novo locatário, clique em Adicionar locatário e escolha Microsoft 365 ou Google Workspace, dependendo da plataforma de nuvem que deseja proteger. Depois de concluir o processo de registro de locatário, seu Microsoft 365 ou Google Workspace está protegido pelo ESET Cloud Office Security.

Depois de adicionar o locatário, a tela muda, mostrando a lista de locatários associados a um site, você pode gerenciar seu locatário existente ou adicionar mais locatários. A tabela mostra o nome do locatário, o número de usuários, quando o locatário foi adicionado, a configuração de idioma, os usuários licenciados do Microsoft 365, o nome do site e o administrador do Google.



Idioma

Essa configuração determina o idioma das mensagens de notificação por e-mail para os membros do locatário. Você pode definir o idioma para cada locatário separadamente, por exemplo, no caso do MSP gerenciando várias empresas.

Para remover um locatário do ESET Cloud Office Security, selecione o locatário apropriado e clique em Remover.

Uma janela de confirmação será exibida para que você tome uma decisão final. Depois de removido, todos os dados do usuário serão removidos depois de 30 dias.

Usuários licenciados da Microsoft 365

Essa opção está ativada por padrão. Isto é equivalente a uma lista de usuários no centro de administrador da Microsoft 365 sob **Usuários** > **Usuários ativos** > Filtrar: **Usuários licenciados**.

Ao desativar essa opção, o ESET Cloud Office Security vai exibir todos os usuários, incluindo usuários sem uma licença válida do Microsoft 365 (por exemplo, caixas de entrada compartilhadas). Se você estiver usando a Proteção automática para grupo ou locatário que contém usuários sem licença do Microsoft 365, esses usuários vão se tornar visíveis, protegidos e consumirão as unidades de licença ESET Cloud Office Security. O status de proteção de usuários recentemente visíveis pode ficar **Pendente** por até 1 hora. Assim que o processo de Proteção automática estiver concluído, o status de proteção será alterado para **Protegido** ou outro status possível na seção Usuários.

> Se seu locatário ou grupo com Proteção automática tiver um usuário sem Caixa de entrada e OneDrive, esse usuário consumirá a unidade de licença ESET Cloud Office Security. Você verá um status de proteção de **Alerta** para esse usuário.

Ao reativar os Usuários licenciados da Microsoft 365, apenas os usuários com a licença da Microsoft 365 continuarão a ser exibidos. Se você tiver Proteger automaticamente usuários sem licença Microsoft 365, esses usuários vão desaparecer da seção Usuários e as unidades de licença do ESET Cloud Office Security serão liberadas. Pode levar até 1 hora para que a alteração seja realizada.

> Se você tiver protegido manualmente os usuários sem licença Microsoft 365 (enquanto a configuração **Usuários licenciados da Microsoft 365** estava desativada), esses usuários permanecerão visíveis e protegidos mesmo depois de ativar a opção **Usuários licenciados da Microsoft 365** (até que os usuários fiquem desprotegidos).

Site

Se você quiser alterar o site ao qual o locatário está associado, clique no nome do site para abrir a janela **Selecione um site para proteger** e faça as alterações necessárias.

Administrador do Google

O administrador do Google deve ser um e-mail ativo do administrador do Google Workspace.

> Se a função ou o endereço de e-mail do administrador estiver prestes a mudar, atualize as informações de administrador do Google clicando na opção. Faça isso com antecedência para garantir a funcionalidade do locatário e a proteção do seu site.

Consentimento da atualização

Se um botão amarelo for exibido, você poderá atualizar seu consentimento. A atualização do consentimento para locatário existente estende as permissões do ESET Cloud Office Security para sua conta do Microsoft 365, habilitando um recurso que fornece informações sobre o tipo de usuário. O tipo de usuário é definido no Active Directory do Azure e será exibido na seção Usuários em uma coluna dedicada. Por exemplo, você pode filtrar usuários do Microsoft 365 com base em seu tipo se quiser listar somente caixas de entrada compartilhadas.

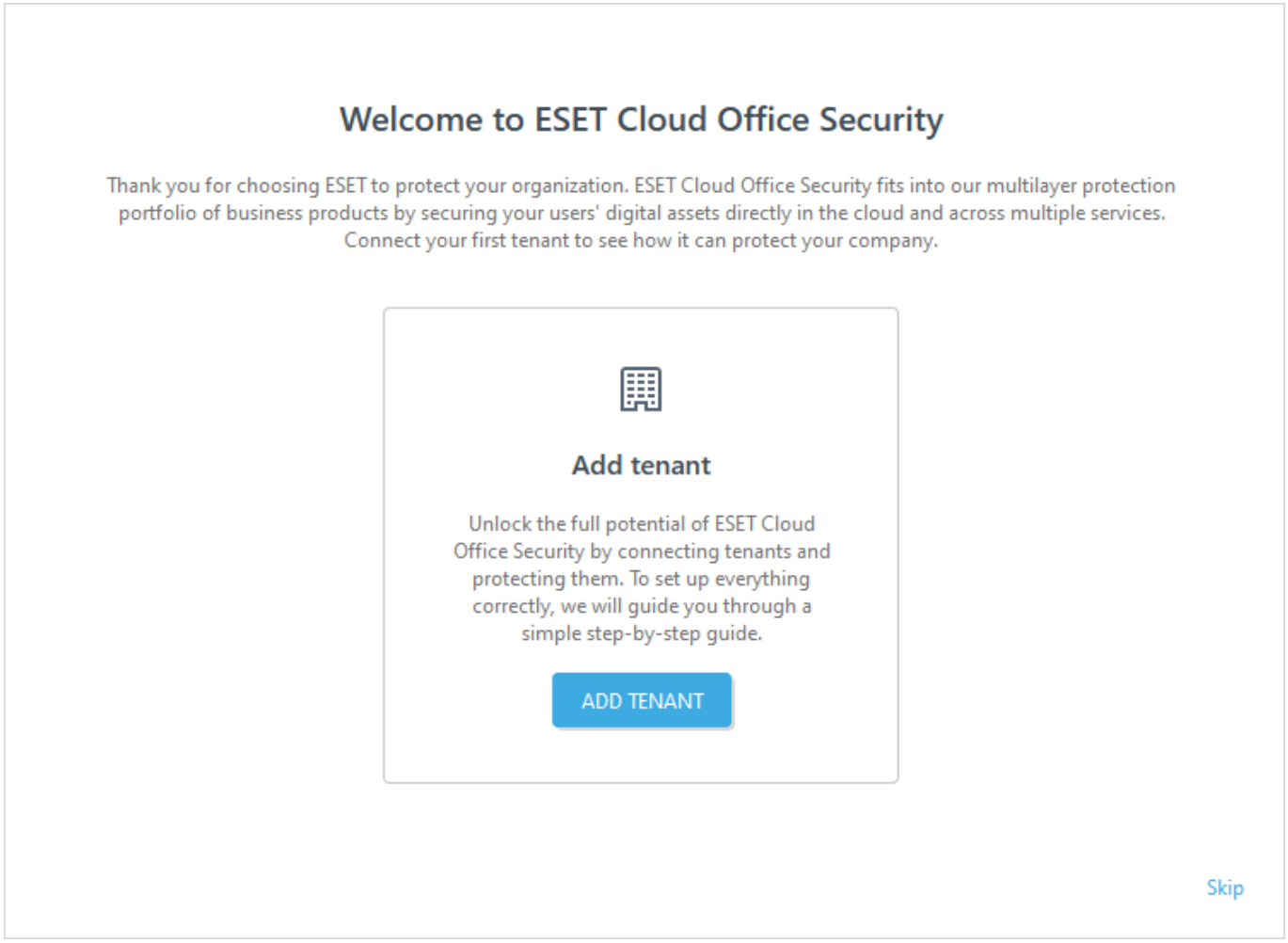
Clique no botão **Atualizar** para cada locatário para o qual você deseja habilitar esse recurso. Pode levar até 24

horas para atualizar o tipo de usuário do seu Azure AD.

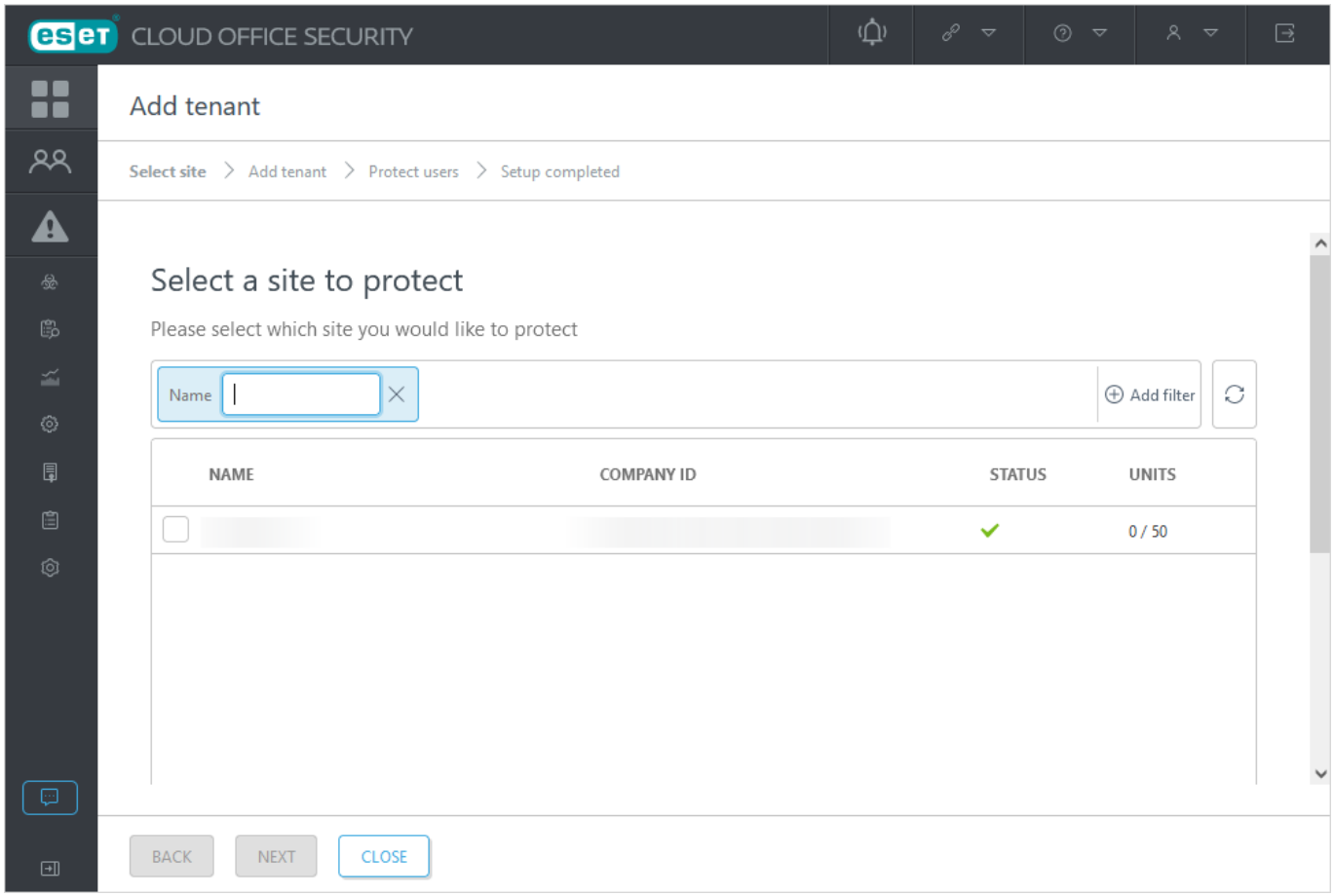
Se um botão vermelho for exibido, o consentimento foi revogado ou outra alteração foi feita que afetou a integração do locatário com o ESET Cloud Office Security. Clique no botão **Atualizar** se quiser continuar protegendo os usuários.

Adicionar seu primeiro locatário

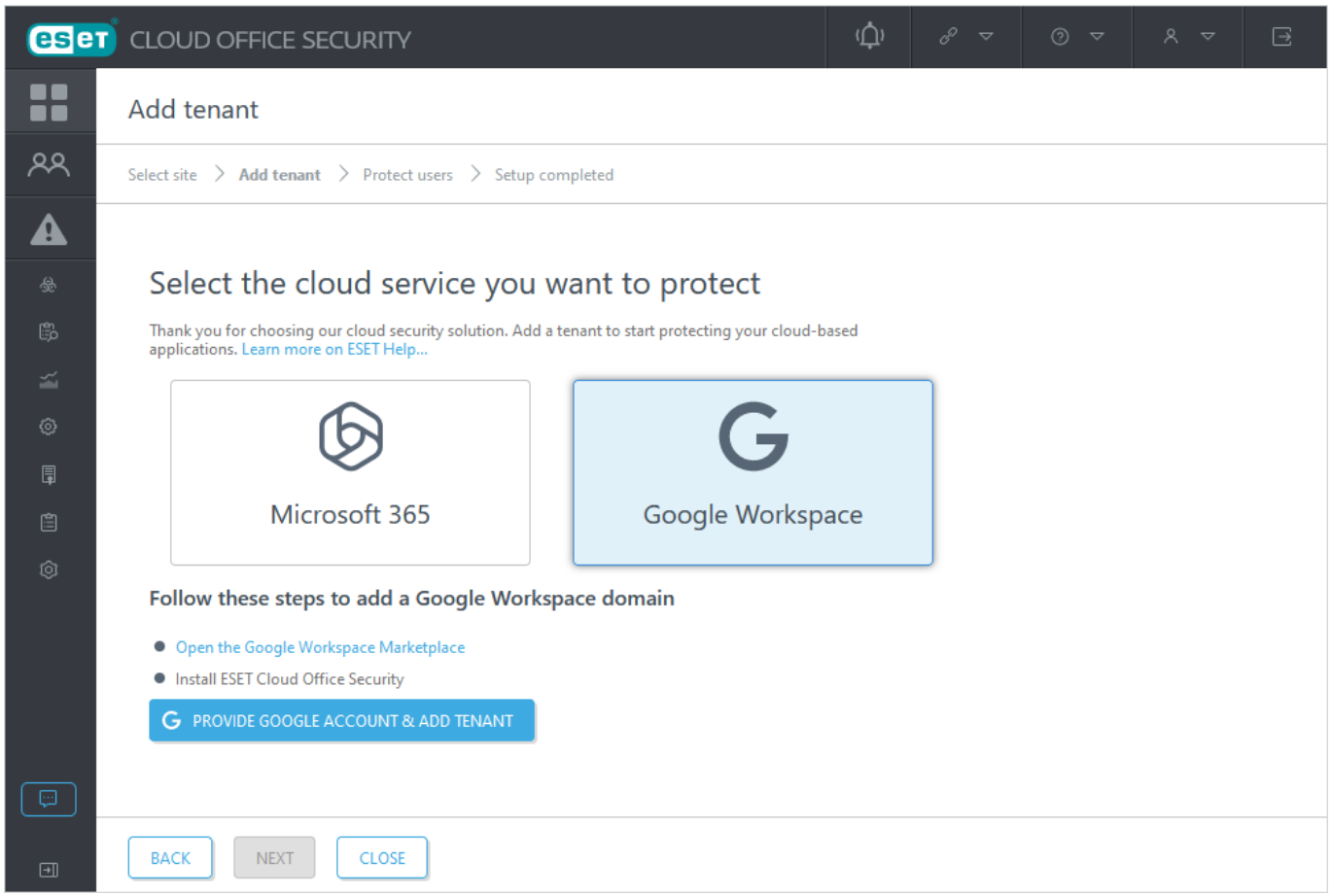
Para proteger sua plataforma de nuvem, clique em **Adicionar locatário** para conectar seu Microsoft 365 ou Google Workspace ao ESET Cloud Office Security.



Você verá uma lista de sites disponíveis na janela **Selecione um site para proteger**. Use a caixa de seleção para selecionar o site que você deseja associar a um locatário e clique em **Avançar**.



Clique no bloco Microsoft 365 ou Google Workspace na janela **Selecione o serviço de nuvem que deseja proteger** e siga as etapas dos marcadores:



Locatário do Microsoft 365

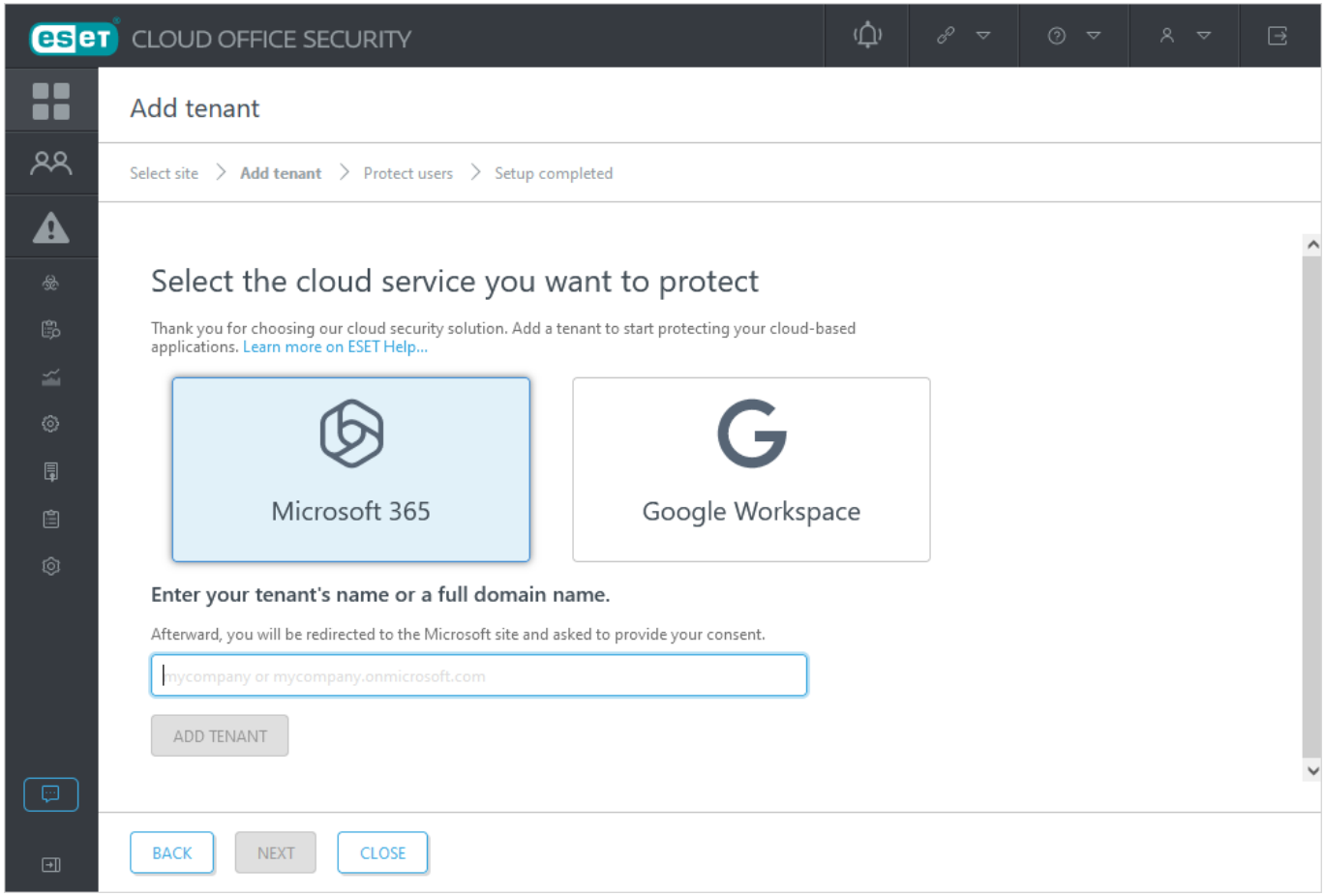
O Azure Active Directory (Azure AD) organiza objetos como usuários e aplicativos em grupos chamados de locatários. Uma forma típica de identificar um locatário é usando um nome de domínio. Se vários usuários compartilharem um nome de domínio, esses usuários fazem parte do mesmo locatário. Os locatários permitem que você defina políticas para usuários e aplicativos dentro da sua empresa para cumprir as políticas operacionais e de segurança. Você pode proteger e gerenciar vários locatários do Microsoft 365 de um console ESET Cloud Office Security.

Para mais detalhes, consulte o artigo da Microsoft sobre Locatários no Azure Active Directory.

Adicionar locatário

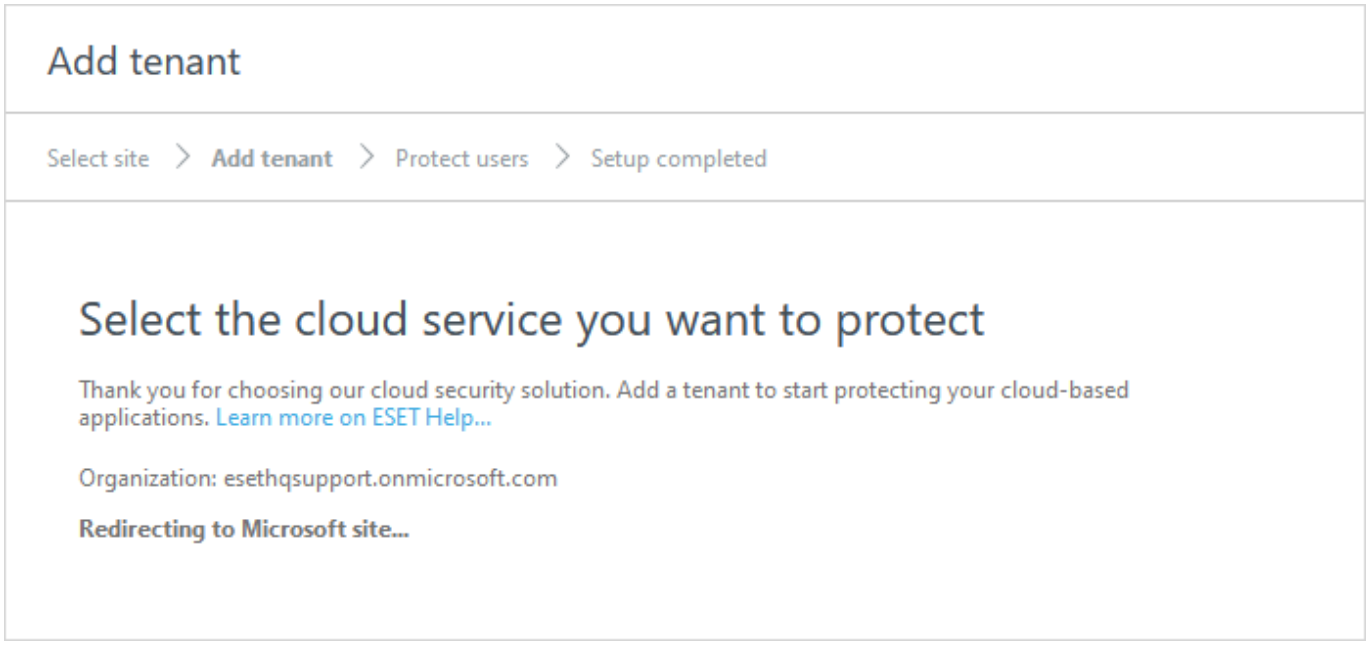
1. Vá para **Configurações** e clique em **Adicionar locatário** (ou em qualquer lugar que você veja o botão **Adicionar locatário**).

2. Clique no bloco **Microsoft 365**.

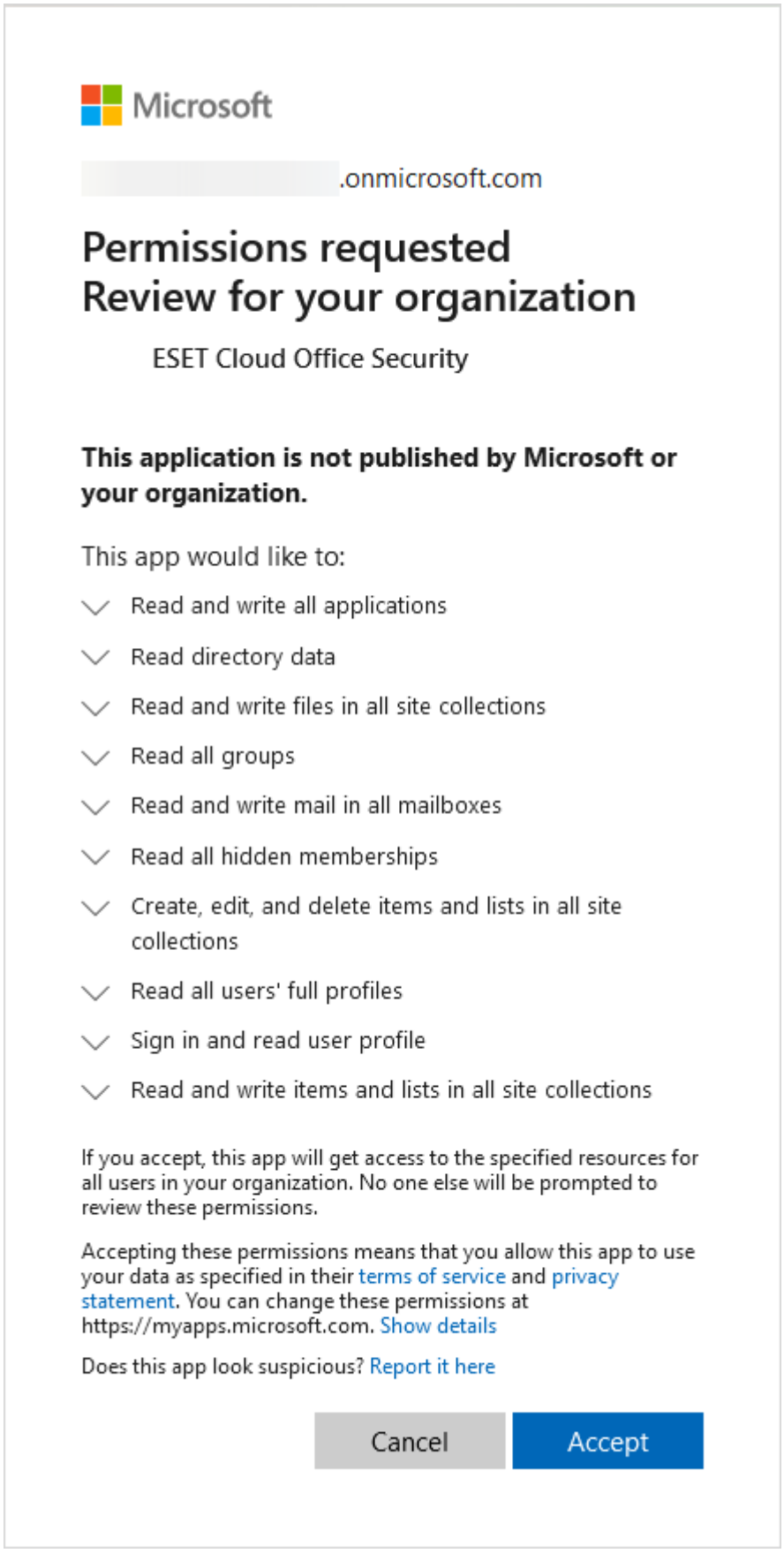


3. Digite seu nome de locatário do Microsoft 365 ou nome de domínio completo e clique em **Adicionar locatário**.

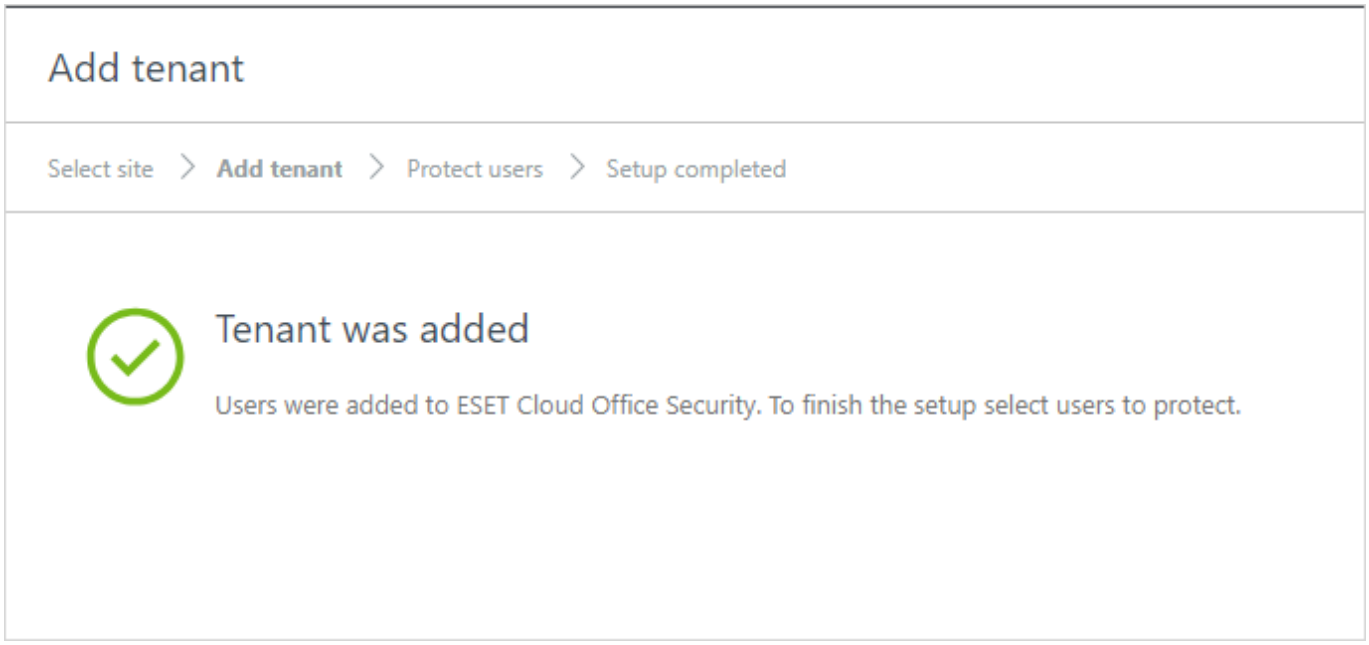
4. Você será redirecionado para a página de consentimento on-line da Microsoft com uma lista de permissões solicitadas pelo ESET Cloud Office Security.



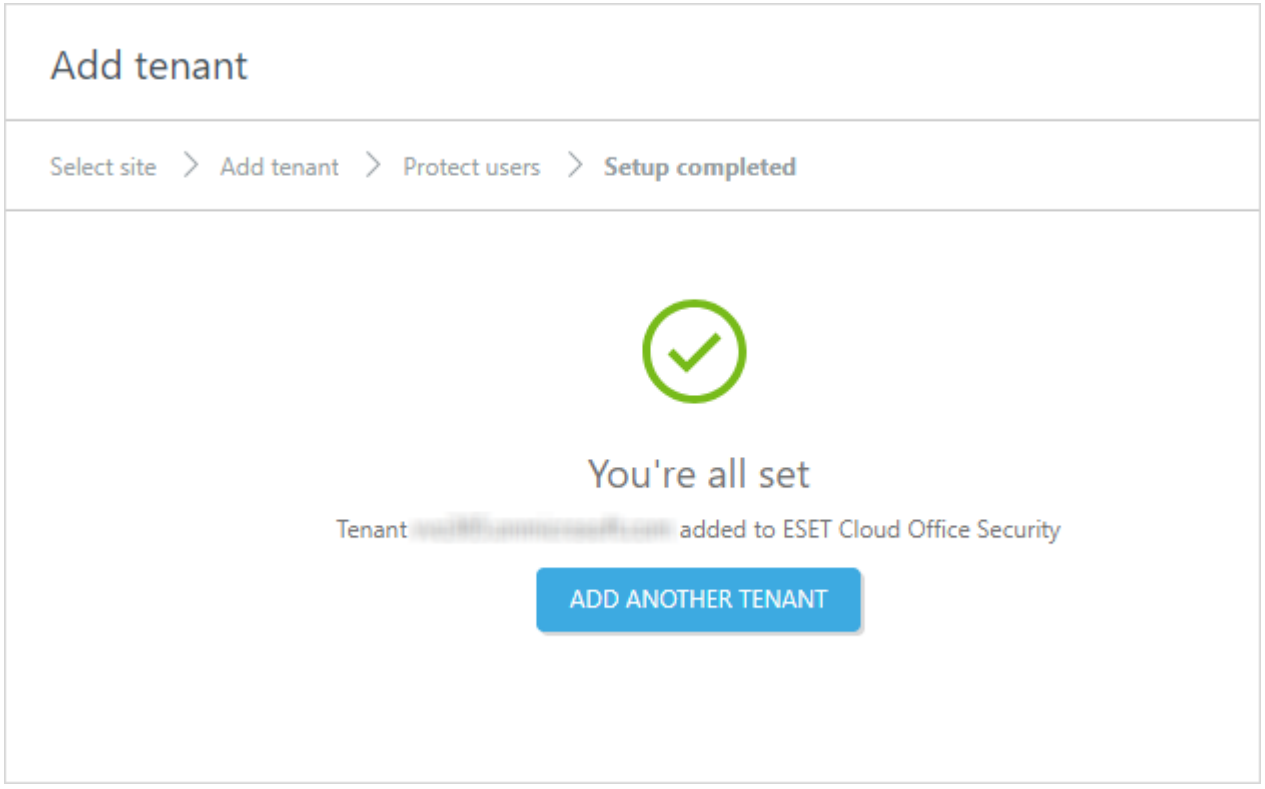
5. Digite as credenciais da sua conta de administrador do Microsoft 365 para permitir que o ESET Cloud Office Security acesse os dados localizados na sua conta da Microsoft, clique em **Aceitar**.



6. Seu locatário do Microsoft 365 foi adicionado, incluindo os usuários.



7. Para concluir a configuração, clique em **Avançar** e selecione os usuários a **Proteger**.



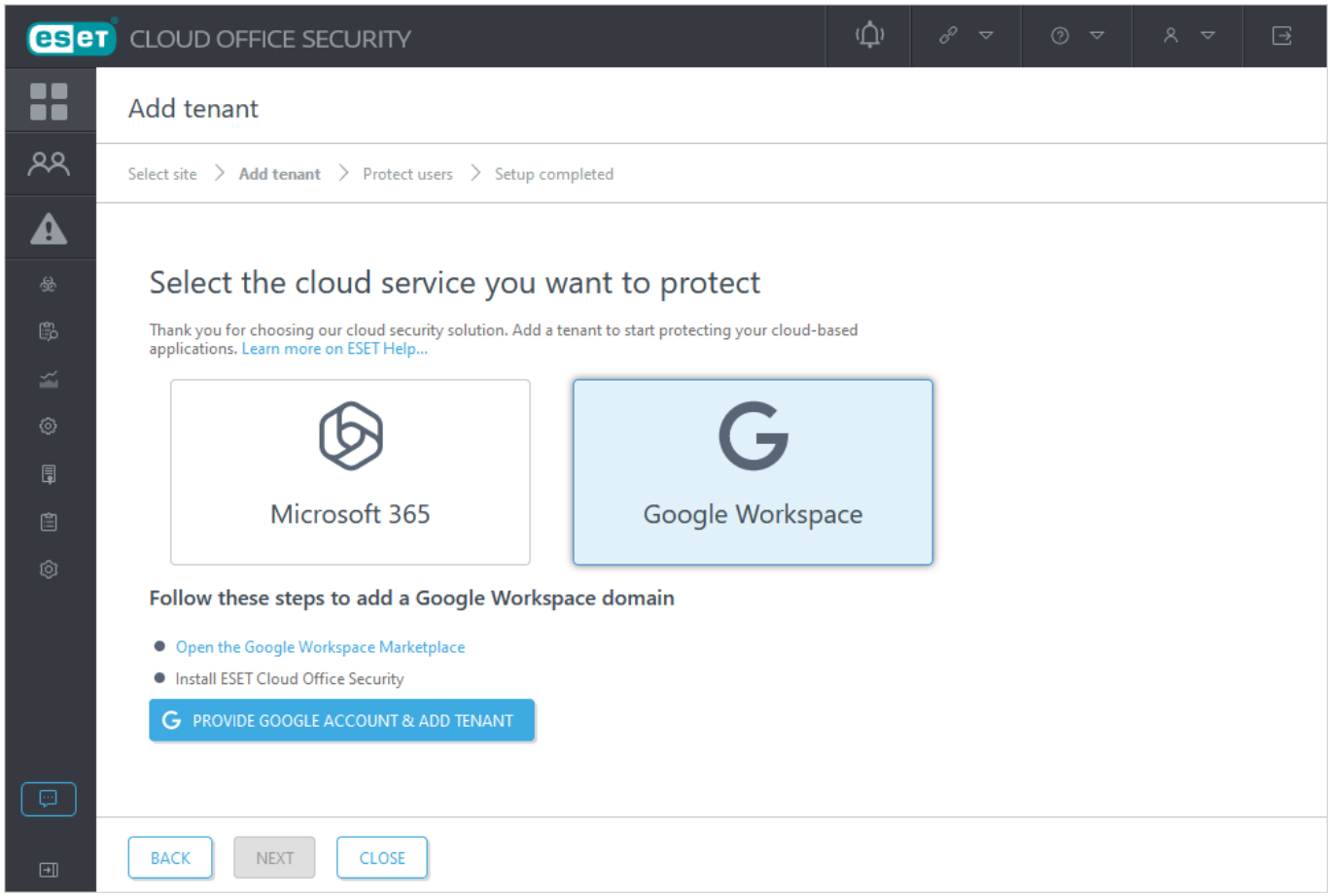
Locatário do Google Workspace

Integre seu locatário do Google Workspace com o ESET Cloud Office Security para ativar a proteção para os usuários do Google Workspace.

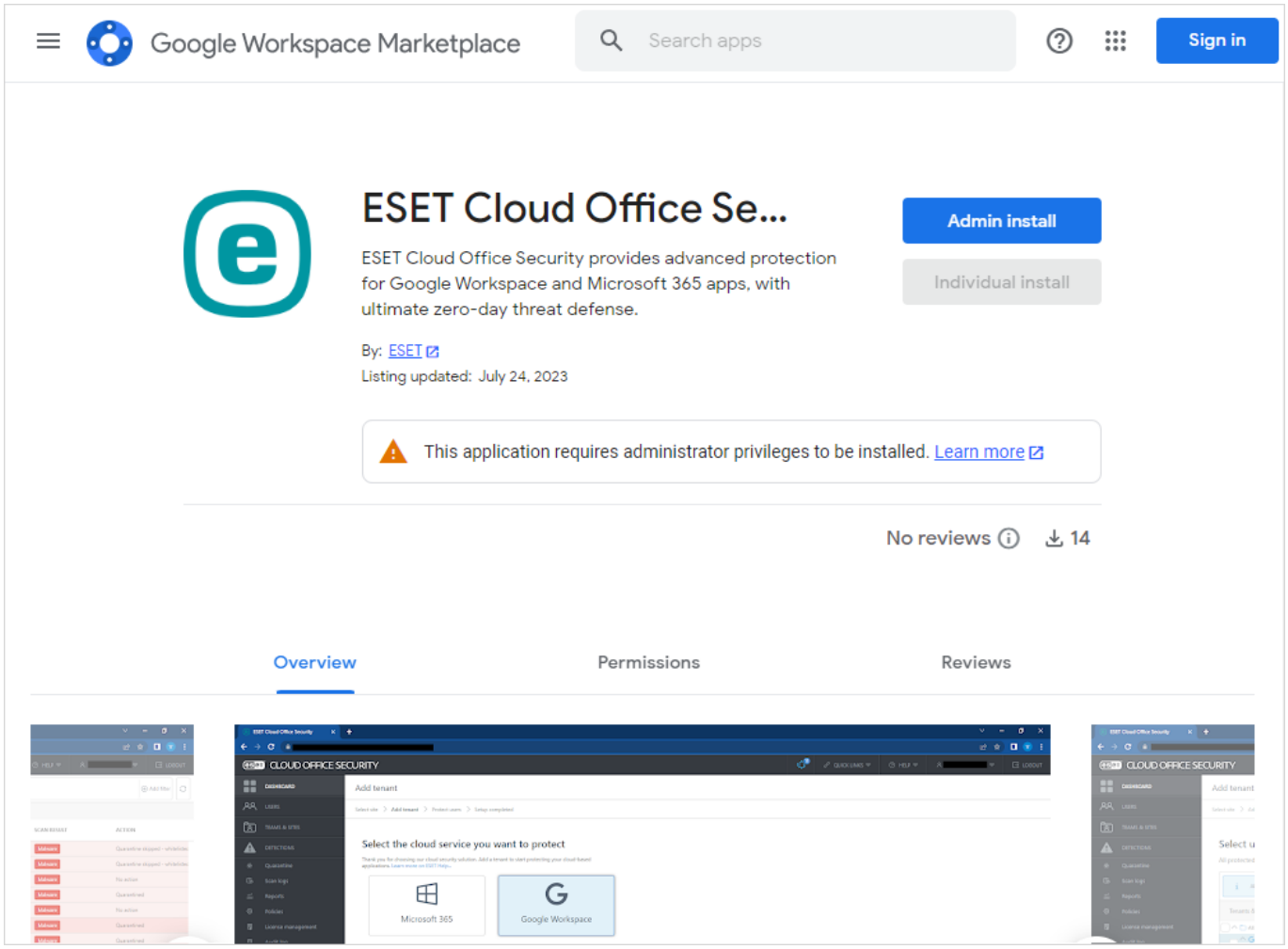
Adicionar locatário

1. Vá para **Configurações** e clique em **Adicionar locatário** (ou em qualquer lugar que você veja o botão **Adicionar locatário**).

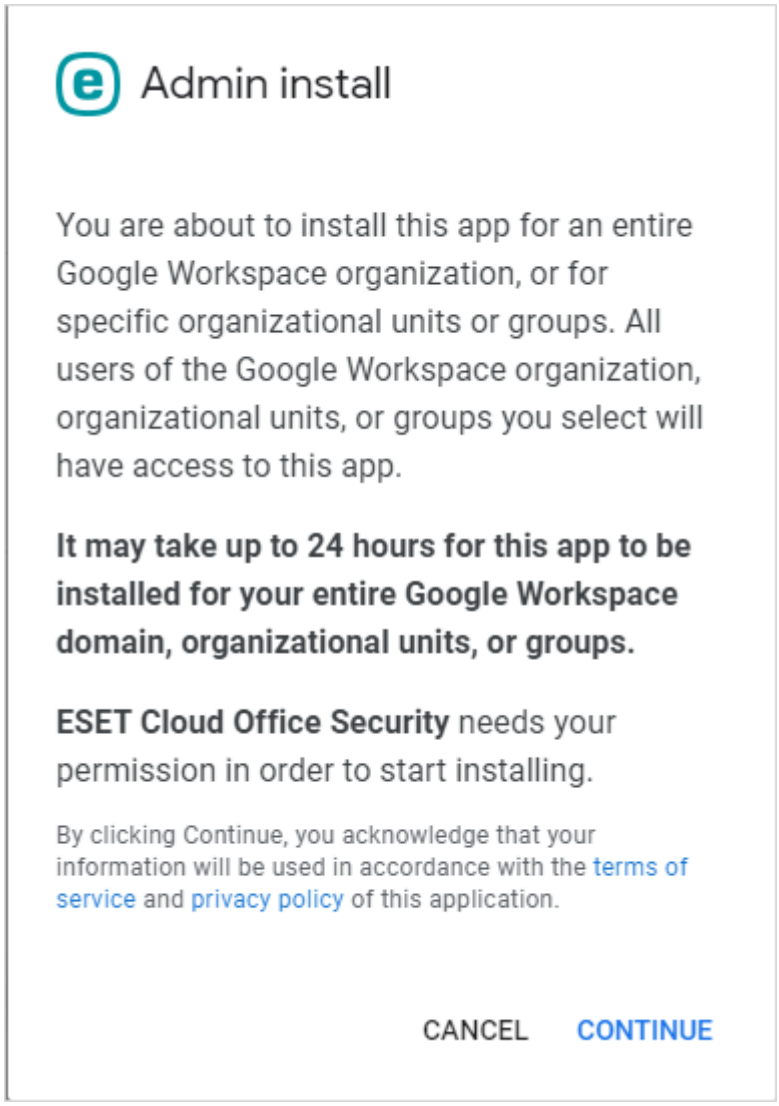
2. Clique no bloco do **Google Workspace**.



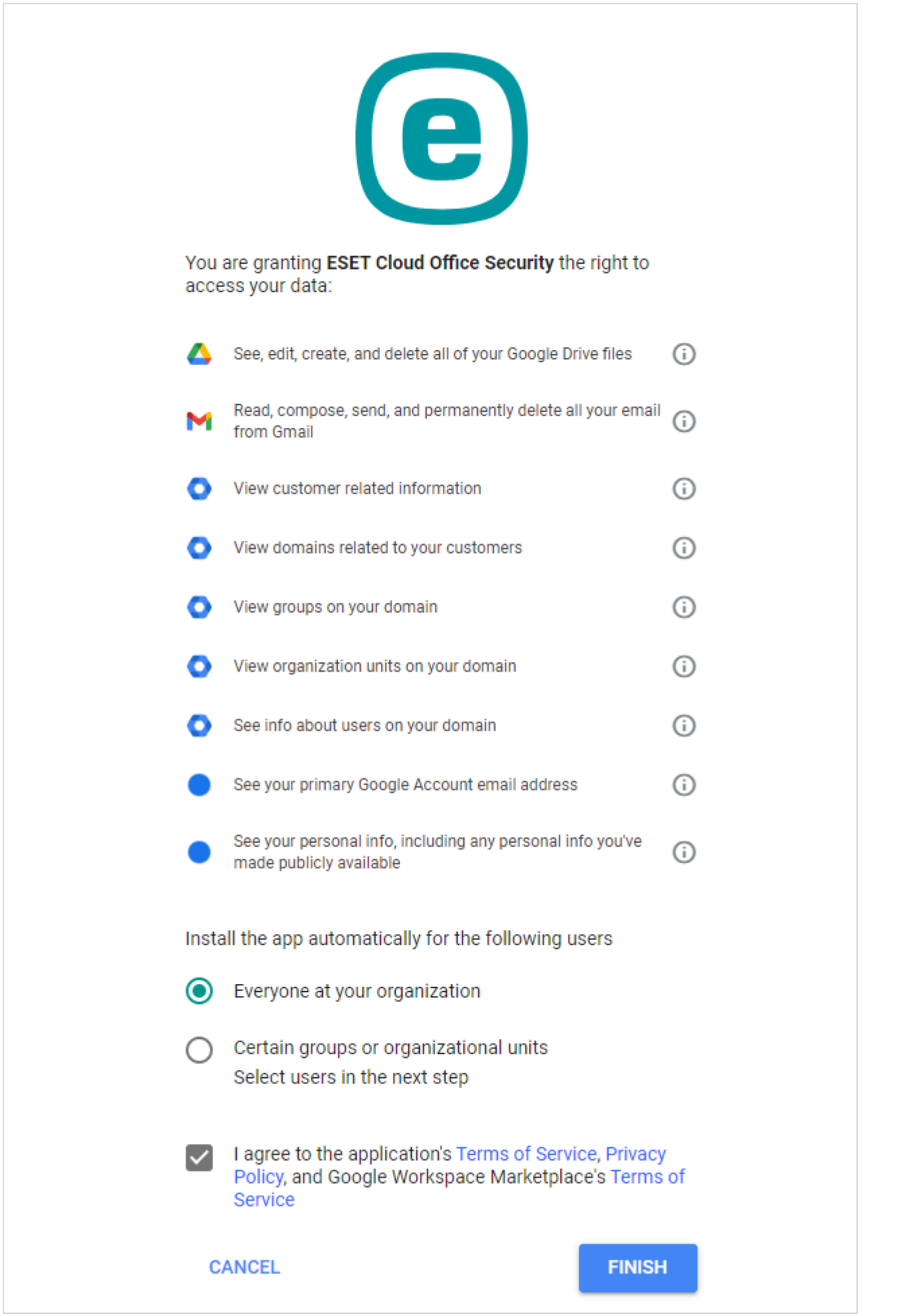
3. Clique em Abrir o Google Workspace Marketplace, instale o aplicativo ESET Cloud Office Security usando a conta de administrador. No momento, o aplicativo ESET Cloud Office Security está disponível no Google Workspace Marketplace apenas por meio do link direto deste assistente.



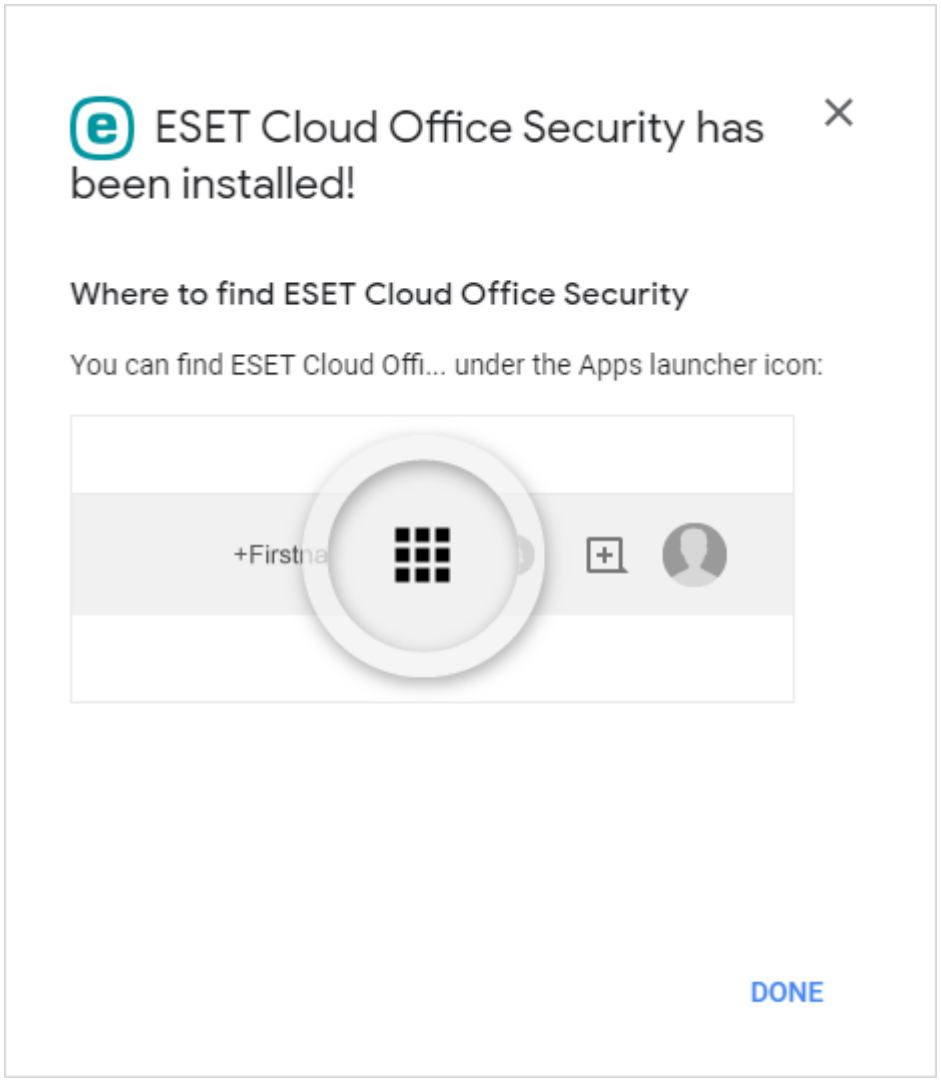
4. Clique em **Continuar** na tela **Instalação do administrador**.



5. Verifique se a opção **Todos na sua organização** está selecionada na tela de direitos de acesso. Além disso, a caixa de seleção Termos de serviço e Política de privacidade deve ser marcada antes de clicar em **Concluir**.

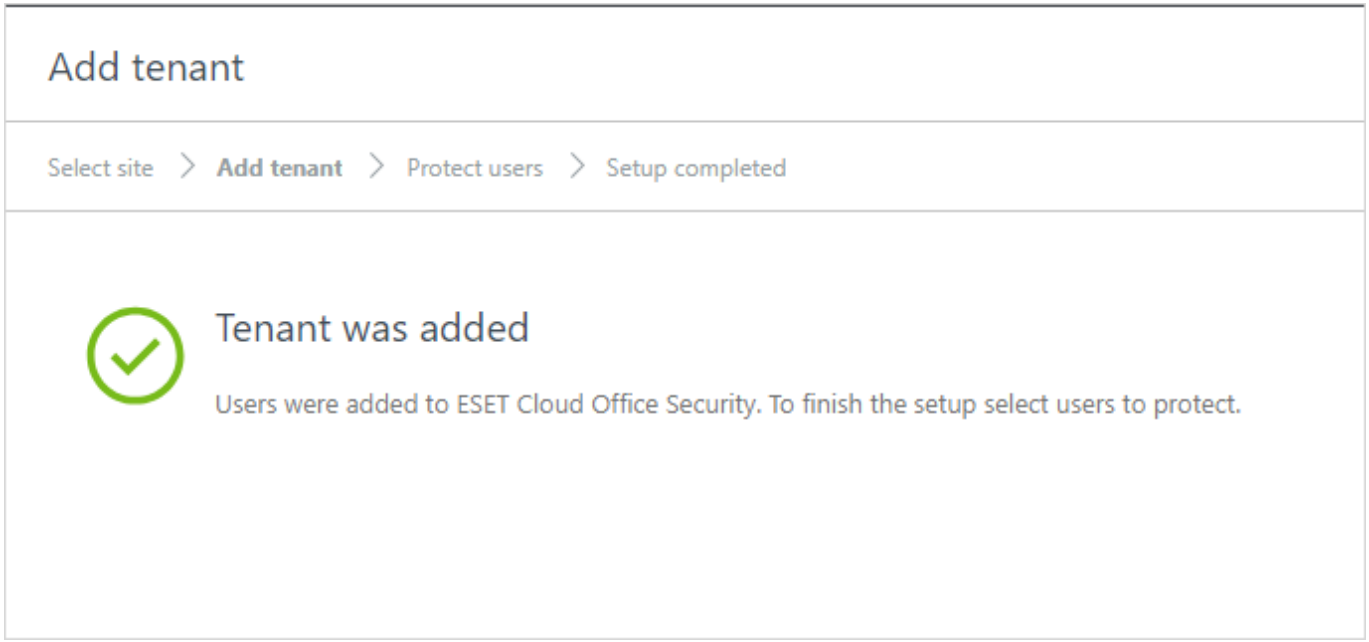

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your 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. O aplicativo ESET Cloud Office Security está instalado, clique em **Concluído**.

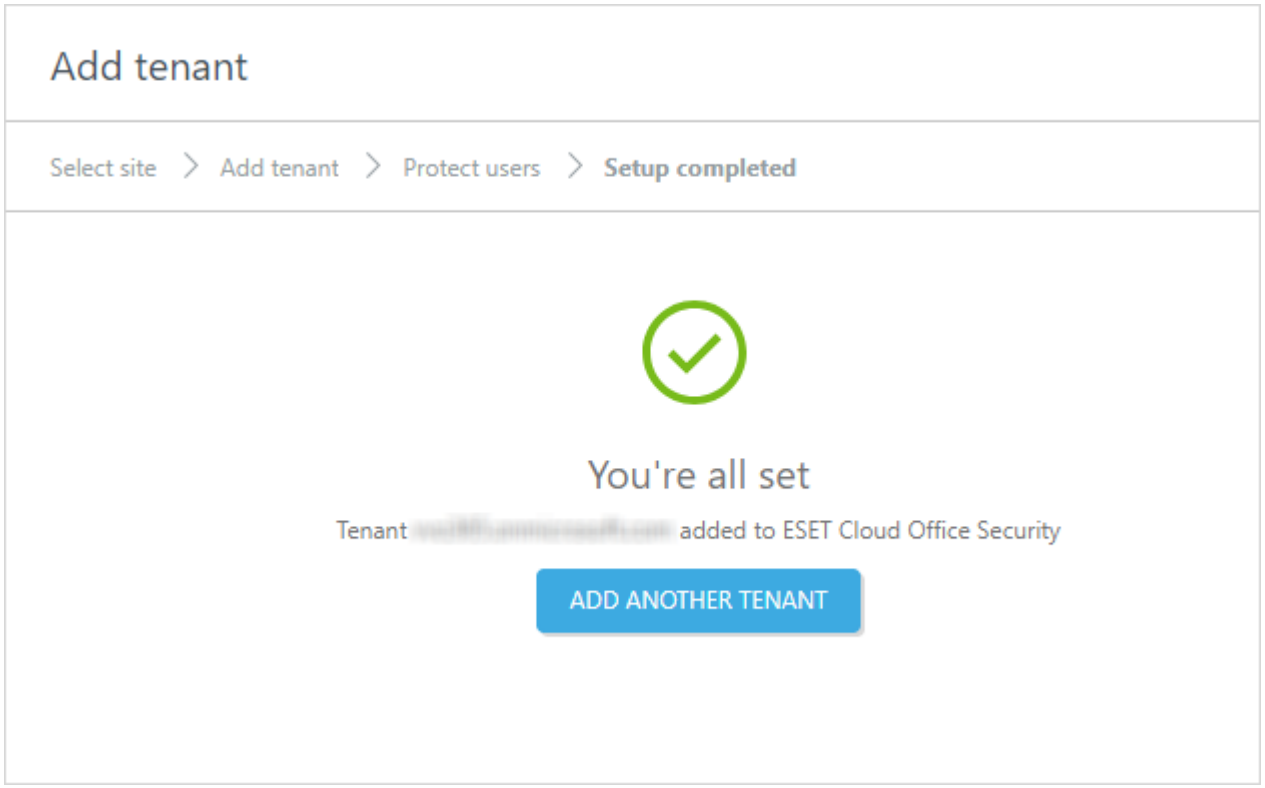


7. Depois que o aplicativo ESET Cloud Office Security for concluído, volte ao console ESET Cloud Office Security. Clique em **Fornecer conta do Google e adicionar locatário** para confirmar a propriedade e continuar.

8. Seu locatário do Google Workspace foi adicionado, incluindo os usuários.



9. Para concluir a configuração, clique em **Avançar** e selecione os usuários a **Proteger**. Então estará tudo pronto.

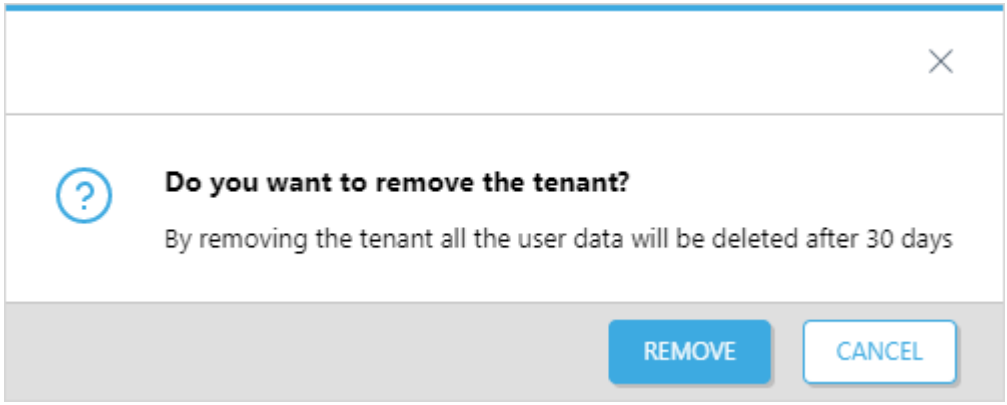


Remover locatário do ESET Cloud Office Security

1. Selecione **Configurações**.

2. Selecione o locatário aplicável e clique em **Remover**.

3. Uma janela de notificação alerta que esse processo vai remover os dados conforme descrito na Política de retenção de dados e limitações, e os usuários vão se tornar desprotegidos. Clique em **Remover** para confirmar a exclusão.



Quando você remove um locatário do console ESET Cloud Office Security, os dados do locatário são retidos por 30 dias (Quarentena, Relatórios do escaneamento e Estatísticas são removidos depois de 30 dias). Se você adicionar o locatário novamente dentro de 30 dias, todos os dados serão restaurados. Outros objetos (locatários, usuários, grupos, sites, relatórios, políticas) são removidos permanentemente depois de 90 dias. Para obter mais informações, consulte a Política de limitações e retenção de dados.

Remover o ESET Cloud Office Security do portal Azure

1. Entre no Portal Azure usando uma conta de administrador.

> Para remover um aplicativo, é preciso estar listado como proprietário do aplicativo ou ter privilégios de administrador.

2. Navegue para o serviço **Azure Active Directory** e selecione **Aplicativos corporativos**.

3. Localize e clique no aplicativo **ESET Cloud Office Security** na página visão geral, vá para **Propriedades** e clique em **Remover**.

Navegue no ESET Cloud Office Security

Veja como navegar pela interface do ESET Cloud Office Security. Você logo pode se familiarizar com os elementos e ferramentas de navegação do ESET Cloud Office Security, que visam ser intuitivo e fáceis de usar, além de interativos.

Use a barra de navegação no lado esquerdo para alternar entre partes diferentes do console ESET Cloud Office Security:

- Usuários
- Equipes e sites
- Detecções
- Quarentena
- Relatórios do escaneamento
- Relatórios
- Políticas
- Gerenciamento de licenças
- Relatório de auditoria
- Configurações

Fechar – Expanda e recolha o menu de navegação. Recolher o painel oferece mais espaço na tela do painel. Para expandir o painel de navegação, clique no ícone .

A barra de ferramentas na parte superior está disponível em todos os momentos:

Navegador de produto – acesso rápido aos consoles ESET e outros links úteis. (Você pode ver os respectivos produtos com base em sua licença e direitos de acesso).

ESET Business Account e **ESET MSP Administrator** (conta de licenciamento híbrido) – se você tiver o mesmo endereço de e-mail registrado no ESET MSP Administrator e no ESET Business Account (login único), você pode alternar entre a visualização do ESET Business Account e a do ESET MSP Administrator.

Mostrar notificações – para ver todas as notificações, clique no ícone de sino na barra superior.

Links rápidos – fornece acesso fácil a Adicionar locatário, Nova política, ESET Business Account ou ESET MSP Administrator.

Ajuda – o primeiro link neste menu é sempre um link para a Ajuda on-line da tela atual. Se não for possível resolver um problema, procure na Base de conhecimento da ESET ou no Fórum de suporte. Alternativamente, você pode Enviar feedback ou **Enviar uma amostra para análise**. Abra a página Sobre, que fornece informações detalhadas sobre a versão ESET Cloud Office Security e links para documentos legais.

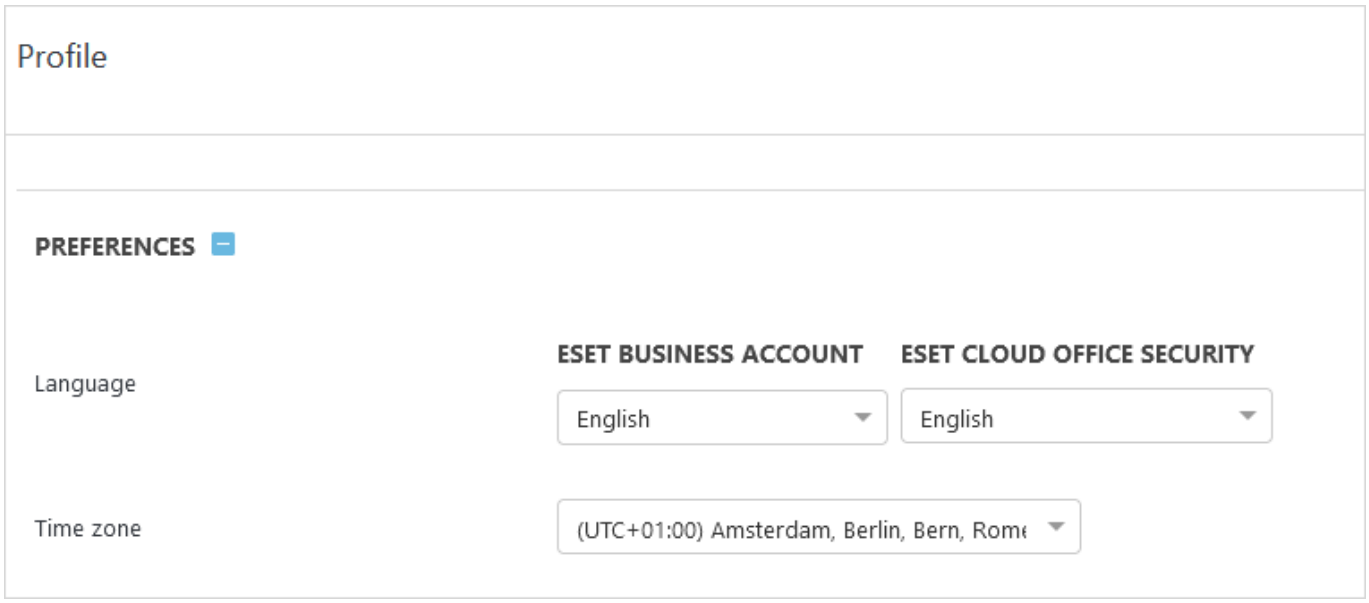
Usuário (conectado no momento) – Mostra o nome de usuário. Clique em **Definir tema** e selecione o desejado no menu suspenso:

- **Tema padrão (claro)** – o ESET Cloud Office Security usará um esquema de cores claras (padrão).
- **Tema escuro** – o ESET Cloud Office Security usará um esquema de cores escuras (modo escuro).
- **Tema do sistema operacional** – o esquema de cores do ESET Cloud Office Security é baseado nas configurações do sistema operacional.

Efetuar logout – clique nesse pictograma sempre presente para sair do console ESET Cloud Office Security.

Alterar idioma para o portal ESET Cloud Office Security

Entre no ESET Business Account ou ESET MSP Administrator, navegue até **Gerenciamento de usuários** e **Edite** o usuário. Procure a configuração de idioma ESET Cloud Office Security, mude para o idioma preferido e clique em **Salvar** antes de sair da tela **Perfil**.



ESET LiveGuard Advanced

O ESET LiveGuard Advanced fornece outra camada de segurança ao usar tecnologia avançada baseada em nuvem ESET para detectar o novo tipo de ameaças nunca vista antes. O ESET LiveGuard Advanced oferece a você a vantagem de estar protegido contra possíveis consequências causadas por novas ameaças. Se o ESET LiveGuard Advanced detectar um código ou comportamento suspeito, ele impede uma maior atividade de ameaça ao colocá-lo temporariamente na quarentena.

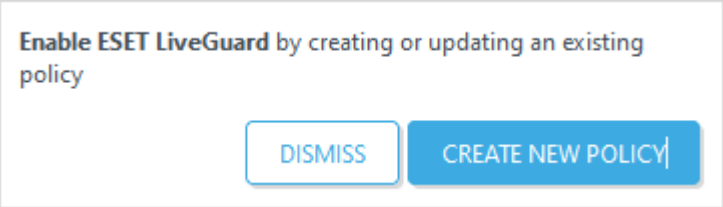
Uma amostra suspeita (arquivo ou mensagem de e-mail) é enviada automaticamente para o ESET Cloud, onde o servidor ESET LiveGuard Advanced analisa a amostra usando seus mecanismos de detecção de malware de tecnologia de ponta. Enquanto arquivos ou e-mails estão na quarentena, o ESET Cloud Office Security está aguardando os resultados do servidor ESET LiveGuard Advanced.

Depois de concluída a análise, seu ESET Cloud Office Security recebe um relatório com um resumo do comportamento das amostras observadas. Se a amostra se provar inofensiva, ela é liberada da quarentena. Caso contrário, ela é mantida em quarentena.

Os resultados das amostras para o ESET LiveGuard Advanced geralmente chegam dentro de alguns minutos para mensagens de e-mail. Porém, o intervalo de espera padrão está definido como 5 minutos. Em casos raros, quando os resultados do ESET LiveGuard Advanced não chegam dentro do intervalo, a mensagem é liberada. Você pode alterar o intervalo para o seu horário preferido (qualquer coisa entre 5 a 60 minutos, em incrementos de um minuto).

A licença do ESET Cloud Office Security faz com que você seja elegível para usar o recurso ESET LiveGuard Advanced sem nenhuma taxa adicional. Você verá o rótulo ELG ao lado do ID de licença no Gerenciamento de licenças.

Quando uma pequena janela pop-up aparecer, você pode ativar o ESET LiveGuard Advanced criando uma nova política ou atualizando uma política existente.



Para informações mais detalhadas sobre o ESET LiveGuard Advanced, veja Como as camadas de detecção do ESET LiveGuard Advanced funcionam .

Painel

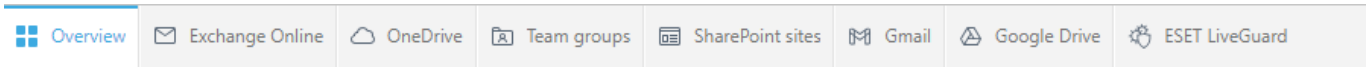
O Painel é um conjunto de widgets que fornecem uma visão geral das atividades de segurança do Microsoft 365. O Painel fornece informações essenciais em cada uma de suas guias de visão geral (Visão geral/Exchange Online/OneDrive/grupos de equipe/Sites do SharePoint, Gmail, Google Drive e ESET LiveGuard Advanced). **Visão geral** é a tela principal do painel que você vê toda vez que entra no console ESET Cloud Office Security. Ele exibe informações gerais e estatísticas.

> O intervalo de atualização do Painel é de 10 minutos. Se você não encontrar as informações mais recentes no seu Painel, pressione **F5** para atualizar manualmente.

Para ver as estatísticas do Painel, use filtros no topo para escolher o **Período de tempo** aplicável (últimas 24 horas, últimos 7, 30 ou 90 dias) e **Locatário**. Estatísticas adicionais de detecção e gráficos estão visíveis nas guias de visão geral do **Exchange Online**, **OneDrive**, **Grupos de equipe**, **sites SharePoint**, **Gmail**, **Google Drive** e **ESET LiveGuard Advanced**. Essas são estatísticas, como o número de e-mails e arquivos escaneados, e o número de spam/phishing/malware detectados. Os gráficos mostram o tráfego para cada tipo de detecção: spam, malware e phishing.

Ocasionalmente, a barra de anúncios pode aparecer. As cores indicam o tipo de anúncio (azul = notícias, amarelo = conhecimento, vermelho = alerta).

Use as guias do Painel para alternar entre os painéis de visualização:



Visão geral

mostra
- o número de Locatários e uso da Licença
- estatísticas por cada Locatário:

oNúmero total de usuários/usuários não protegidos
oPrincipais destinatários de spam/phishing/malware
oPrincipais contas suspeitas do OneDrive
oPrincipais grupos de Equipe suspeitos
oPrincipais sites suspeitos do Sharepoint

detalhamento
- clique no bloco Número total de usuários para abrir a seção Usuários
- clique em um usuário na seção estatísticas (spam/phishing/malware/OneDrive) para ver as Detecções

relevantes, ou clique em um grupo ou site para ver detecções e mais detalhes sobre o Grupo de equipe ou site do SharePoint suspeito.

Exchange Online

exibe
- número total de e-mails escaneados
- estatísticas de e-mails detectados de spam, malware e phishing
- gráficos onde cada um representando o tráfego de spam, malware e phishing

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

OneDrive

exibe
- o número de usuários protegidos
- número total de arquivos escaneados
- estatísticas de malware detectado
- um gráfico que representa tráfego de malware

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

Grupos de equipe

exibe
- o número de grupos protegidos
- número total de arquivos escaneados
- estatísticas de malware detectado
- um gráfico que representa tráfego de malware

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

Sites do SharePoint

exibe
- o número de sites protegidos
- número total de arquivos escaneados
- estatísticas de malware detectado
- um gráfico que representa tráfego de malware

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

Gmail

exibe
- número total de e-mails escaneados
- estatísticas de e-mails detectados de spam, malware e phishing
- gráficos onde cada um representando o tráfego de spam, malware e phishing

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

Google Drive

exibe
- o número de usuários protegidos
- número total de arquivos escaneados
- estatísticas de malware detectado
- um gráfico que representa tráfego de malware

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

ESET LiveGuard Advanced

exibe
- arquivos enviados (a contagem inclui duplicatas e o número pode ser maior do que arquivos únicos)
- número de detecções
- tempo médio de análise
- um gráfico que representa os arquivos enviados
- principais proprietários de arquivos enviados
- tipos de arquivo enviados

Os blocos são interativos. Clique em um bloco de interesse e vá para a seção relevante dentro do console ESET Cloud Office Security. Por exemplo, a seção Relatórios do escaneamento com registros de relatório relevantes será aberta.

Usuários

A entidade central que o ESET Cloud Office Security protege é a conta do usuário. Clique duas vezes em um usuário para encontrar informações úteis como Visão geral, Configurações definidas por Políticas, lista de Políticas atribuídas ao usuário e Detecções para o Gmail, Google Drive, Exchange Online e OneDrive. Você também pode escolher quais usuários serão Protegidos ou Desprotegidos. Os usuários são classificados em grupos e cada grupo é um locatário do Microsoft 365 contendo seus usuários. Para que seja mais fácil fazer a busca de um usuário específico dentro de um grupo, você pode usar a filtragem com vários critérios.

> Usuários sem uma licença Microsoft 365 não serão mostrados no console ESET Cloud Office Security por padrão. Isso inclui caixas de entrada compartilhadas sem uma licença Microsoft 365.
> Se quiser ver e gerenciar todos os usuários Microsoft 365, navegue até Configurações e desative Usuários licenciados da Microsoft 365.

Status de proteção:

Status	Descrição
Desprotegido	Um usuário não está sendo protegido no momento.
Protegido automaticamente	Usuário protegido com proteção automática.
Pendente	Estado de transição que ocorre durante o processo de proteção de um usuário. Assim que ele termina, o status do usuário muda para Protegido.
Protegido	A Caixa de entrada e OneDrive do usuário estão sendo protegidos por uma política Padrão ou Personalizada.
ATENÇÃO	O processo de proteção de um usuário não foi bem sucedido. Pode ter ocorrido um erro para os recursos, Caixa de entrada ou OneDrive. É provável que ambos os recursos não estejam disponíveis para o usuário. Verifique se o usuário tem uma licença válida do Microsoft 365 atribuída a ele.

Navegue dentro da árvore para ver os usuários para um determinado locatário ou grupo. Para ver todos os usuários em cada locatário e grupo, clique em **Todos**.

Para obter informações mais detalhadas, clique duas vezes em um usuário, ou clique no ícone e selecione uma ação (**Mostrar detalhes**, **Proteger** ou **Desproteger**). Clique em um usuário para abrir a janela **Mostrar detalhes** composta por quatro partes:

Ação	Uso
Visão geral	Exibe informações básicas sobre o usuário carregadas do Microsoft 365 (E-mail, Grupo, Perfil de trabalho, etc.). Além disso, o Status de proteção atual é exibido para a Caixa de entrada e o OneDrive.
Configuração	Contém uma lista somente leitura de Configurações e Políticas atribuídas a este usuário. Alternar entre as guias para ver a configuração ou uma lista de políticas atribuídas. Não é possível modificar as Configurações nem atribuir Políticas a usuários, vá para a seção Políticas.
Detecções	Mostrar todas as detecções para esta conta de usuário (Gmail, Google Drive, Exchange Online ou OneDrive).
Quarentena	Mostrar todos os e-mails colocados em quarentena e arquivos armazenados vindos deste usuário. Você também pode usar uma ação: Liberar, Fazer download ou Remover e-mails ou arquivos colocados em quarentena.

Você pode filtrar os usuários por vários critérios. Clique em **Adicionar filtro** e selecione um tipo de filtro no menu

suspenso ou insira uma string (repita ao combinar vários critérios):

Adicionar filtro	Uso
Status de proteção	Selecione o status Protegido, Desprotegido, Alerta ou Pendente de um usuário.
Protegido automaticamente	Exibir apenas usuários protegidos automaticamente.
Nome	Digite um nome de usuário válido.
E-mail	Digite um e-mail de usuário válido.
Tipo	Selecione o tipo de usuário (Desconhecido, Usuário, Vinculado, Caixa de entrada compartilhada, Sala, Equipamento, Outros).

Proteger usuários

1. Selecione os **Usuários** que serão protegidos e clique em **Proteger**.
2. Selecione o **pool de licenças** carregado do ESET Business Account e clique em **OK**. A política Padrão agora protege os usuários selecionados.
3. Se necessário, especifique uma política personalizada para os usuários na seção Políticas.

Desproteger usuários

Selecione os **Usuários** que serão desprotegidos e clique em **Desprotegido**.

Equipes e sites

O ESET Cloud Office Security fornece proteção para Grupos de equipe ou sites do SharePoint.

Alternar entre guias de Grupos de equipe e de sites do SharePoint. Exibe uma lista de Grupos de equipe ou sites do SharePoint para cada locatário.

Grupos de equipe

exibe objetos que são do tipo de grupo Microsoft 365, incluindo seu site de equipe padrão no SharePoint e OneDrive:

- nome
- status
- e-mail
- locatário

Para proteger os Grupos de equipe, certifique-se de que pelo menos um membro é um usuário protegido pelo ESET Cloud Office Security. Cada grupo Microsoft 365 tem um site de equipe padrão no SharePoint e OneDrive que também estão protegidos.

Sites do SharePoint

Exibe todos os sites raiz do SharePoint não associados ao grupo Microsoft 365:

- nome
- status

- URL
- locatário

Os sites SharePoint são protegidos automaticamente, incluindo seus Subsites (não exibido).

Para informações mais detalhadas, clique em um Grupo de equipe ou site do SharePoint para abrir a janela **Mostrar detalhes**, que é composta por quatro partes:

Ação	Uso
Visão geral	Exibe as informações necessárias sobre os Grupos de equipe ou sites SharePoint carregados da Microsoft 365 (E-mail, Proprietário, Membros, Autor, URL, etc.). Além disso, é exibido um Status de proteção atual para o Grupo de equipe ou site SharePoint.
Configuração	Contém uma lista somente leitura de Configurações e Políticas atribuídas. Alternar entre as guias para ver a configuração ou uma lista de políticas atribuídas. Não é possível modificar Configurações ou atribuir Políticas, vá para a seção Políticas.
Detecções	Exibir todas as detecções para o Grupo de equipe ou site SharePoint.
Quarentena	Exibir todos os arquivos colocados em quarentena. Você também pode usar uma ação: Liberar, Fazer download ou Remover os arquivos em quarentena.

Clique em **Adicionar filtro** para filtrar os Grupos de equipe ou sites do SharePoint.

Detecções

Lista todas as detecções feitas pelo ESET Cloud Office Security. Alternar entre o Gmail, Google Drive, Exchange Online, OneDrive, Grupos de equipe e sites do SharePoint usando as guias. Veja informações de cada detecção, por exemplo, arquivos detectados que foram enviados para um Grupo de equipe na guia Grupo de equipe.

Clique no ícone para abrir uma barra lateral com um resumo de um registro de relatório (detecção) específico. Para informações mais detalhadas, clique no ícone e selecione **Mostrar detalhes**.

Navegue dentro da árvore para ver as detecções apenas para um determinado locatário ou grupo. Para ver todas as detecções em cada locatário e grupo, clique em **Todos**. Para facilitar a busca por uma detecção específica, você pode filtrar usando vários critérios. Clique em **Adicionar filtro** e selecione o tipo de filtro no menu suspenso ou insira uma string (repita ao combinar critérios):

Adicionar filtro	Uso
Ocorreu de	Especifica um intervalo de "data a partir de".
Ocorreu a	Especifica um intervalo de "data até".
Assunto	Aplicável a mensagens que contêm ou não contêm uma string específica (ou uma expressão regular) no assunto.
ID da mensagem	Filtre mensagens de e-mail por um ID de mensagem único ao pesquisar uma mensagem específica, especialmente em grandes relatórios com muitas mensagens ou várias tentativas de entrega.
De	Filtra mensagens por remetente específico.
A	Filtra mensagens por destinatários.
Caixa de correio	Aplicável a mensagens localizadas em uma caixa de entrada específica.
Resultado do escaneamento	Selecione uma das seguintes opções: Malware, Malware (detectado por ESET LiveGuard Advanced), Phishing ou Spam.

Adicionar filtro	Uso
Ação	Selecionar uma das ações disponíveis.
Equipe	Digite o nome de equipe válido.
Site	Digite o nome de site válido.
Objeto	Digite um nome de objeto válido.
Detecção	Digite um nome de detecção válido.
Hash	Digite um hash de detecção válido.

Quando você clicar no ícone , uma opção **Remover da lista de permissões** estará disponível se você tiver colocado um arquivo na lista de permissões anteriormente, liberando-o da Quarentena para o mesmo usuário. Use esta opção para remover um arquivo da lista de permissões. Todos os arquivos futuros serão colocados em quarentena.

> O período de retenção para detecções é de 90 dias. Registros anteriores a 90 dias serão removidos permanentemente.

Reportar falso positivo (FP)/falso negativo (FN)

Você pode reportar manualmente as detecções de FP e FN para spam, phishing ou malware enviando uma amostra para os laboratórios da ESET para análise. Endereços de e-mail para os quais enviar as amostras:

Spam – envie um e-mail para nospam_ecos@eset.com para os e-mails marcados incorretamente como spam ou para spam_ecos@eset.com para o spam não detectado com a mensagem original como um anexo no formato *.eml* ou *.msg*.

Phishing – para reportar a classificação falso positivo ou negativo de phishing, mande uma nova mensagem de e-mail para samples@eset.com com *'phishing email'* na linha de assunto e inclua o e-mail de phishing como um anexo no formato *.eml* ou *.msg*.

Malware – para classificação falso positivo ou negativo de malware, mande uma nova mensagem de e-mail para a samples@eset.com com *'False positive'* ou *'Suspected infection'* na linha de assunto e inclua os arquivos compactados em um formato *.zip* ou *.rar* como um anexo.

Relatórios

Os relatórios ESET Cloud Office Security mantém você informado com uma visão geral das estatísticas da proteção ESET Cloud Office Security. Você pode escolher de dois tipos de relatórios, Relatórios estatísticos ou Relatórios de quarentena de e-mail.

Relatórios estatísticos contêm informações sobre o Gmail, Google Drive, Exchange Online, OneDrive, Grupos de equipe e proteção a sites SharePoint contém o número de e-mails, arquivos, malware detectados, phishing e spam para o período de tempo especificado. Os relatórios podem ser gerados e baixados manualmente no formato *PDF* ou *CSV* ou podem ser agendados e entregues aos destinatários selecionados via e-mail. O formato de saída *PDF* apresenta os dados de forma gráfica, exibe a média de longo prazo para comparação e inclui informações de tráfego para cada tipo de proteção, principais destinatários de malware, phishing e spam.

O relatório de Quarentena de e-mail contém uma lista de objetos recém-colocados em quarentena. O relatório é entregue aos destinatários selecionados por e-mail. Os destinatários podem liberar mensagens de spam (se consideradas seguras ou legítimas) clicando no link **Liberar**. Aplica-se apenas a spam; outros tipos de objetos colocados em quarentena não podem ser liberados.

Você pode acessar as estatísticas por e-mail, sem precisar entrar no console ESET Cloud Office Security. Configure e agende relatórios recorrentes e especifique destinatários de e-mail. Além disso, você pode gerar estatísticas de relatório imediatamente de dentro do console ESET Cloud Office Security. Selecione um relatório existente (também pode ser um relatório agendado) e clique em **Gerar e fazer download.** Clicar com o botão direito do mouse no menu suspenso também funciona. Você pode criar facilmente um novo modelo de relatório com configurações personalizadas.

Novo relatório

Clique em Novo relatório para abrir o assistente de modelo de relatório e especificar configurações personalizadas. Tipo o Nome e a Descrição do relatório.

Idioma

Escolha o idioma desejado no menu suspenso. O relatório será gerado no idioma selecionado.

Tipo

Selecione o tipo que você deseja que sejam incluídos nas estatísticas.

Relatórios estatísticos

Crie relatórios agendados ou sob demanda que consistem em informações de acordo com as opções escolhidas.

Relatórios de Quarentena de e-mail

Para informar os usuários sobre suas mensagens de e-mail recém-colocadas em quarentena, envie e-mails de notificação para os usuários selecionados. Você pode atribuir destinatários individuais ou múltiplos ou um grupo. Escolha um intervalo para os relatórios e a data e hora de início. Se for um relatório repetido, escolha quando ele deve terminar (em uma data, depois de várias ocorrências, ou nunca). O relatório de Quarentena de e-mail é acionado apenas quando há novos itens. Os destinatários do relatório podem liberar mensagens de spam (se considerados seguros ou legítimos) clicando no link Liberar (uma janela de confirmação abre em um navegador da web). A mensagem de spam liberada é entregue em um e-mail separado como um anexo.

Locatário

Esta opção está disponível para um ambiente de vários locatários. Você pode selecionar vários locatários para os quais gerar estatísticas. O relatório será gerado para cada locatário separadamente, e será entregue em um e-mail de relatório ESET Cloud Office Security com vários anexos.

Período

Define o período de tempo no qual você deseja que os resultados sejam exibidos (últimas 24 horas, semana, mês). Ao selecionar Personalizado, você pode especificar uma duração (Data de e Data até).

Saída

Selecione o formato de arquivo adequado, você poderá escolher *PDF* ou *CSV*. O formato *PDF* inclui dados mostrados em gráficos. *CSV* é adequado como dados brutos. Os relatórios serão coletados de acordo com as opções especificadas. Se você selecionar os dados do Gmail, Google Drive, Exchange Online, do OneDrive e dos Grupos de equipe ou sites do SharePoint, o arquivo de saída seria um arquivo em um formato ZIP que contém arquivos de relatório *PDF* ou *CSV*.

Whitelabel

Se você precisar que o logo da sua empresa apareça no relatório, ative este recurso. Você tem a opção de um cabeçalho de relatório incluindo a sua marca, exibindo seu logotipo junto com o logo ESET ou apenas seu logotipo. Enviar o logotipo no formato *PNG* ou *JPEG*.

Agendado

Use a agenda para que os relatórios sejam gerados em uma data e hora especificados, e também como um evento recorrente. Os relatórios agendados são entregues a destinatários selecionados, que receberão um e-mail de relatório ESET Cloud Office Security com anexos.

Repetir

Escolha se deseja que o relatório seja gerado uma vez ou repetidamente:

- **Uma vez** – o relatório será realizado apenas uma vez.
- **Diariamente** — o relatório será gerado e entregue repetidamente, todos os dias (a menos que você especifique a recorrência para terminar depois de ocorrências).
- **Semanalmente** – o relatório será gerado e entregue repetidamente no(s) dia(s) da semana selecionado(s).
- **Mensalmente** – o relatório será gerado e entregue uma vez por mês em um dia selecionado.

A partir de

Escolha a data de início dos relatórios.

Termina

Selecione quando o intervalo de recorrência termina.

Destinatários

Especifique o endereço de e-mail do destinatário do relatório, pressione enter para confirmar. Repita para adicionar vários destinatários.

Para informações detalhadas ou ações, clique no ícone e selecione uma ação:

Ação	Uso
Mostrar detalhes	Exibe informações detalhadas sobre um relatório.
Gerar e fazer download	Clique em Gerar e fazer download e escolha *PDF* ou *CSV*. O formato *PDF* inclui dados mostrados em gráficos. *CSV* é adequado como dados brutos. Os relatórios serão coletados de acordo com as opções especificadas. Se você selecionar os dados do Exchange Online, do OneDrive e dos Grupos de equipe ou sites do SharePoint, o arquivo de saída seria um arquivo em um formato *ZIP* que contém arquivos de relatório PDF ou *CSV*.
Editar	Edita a configuração de um relatório existente.
Excluir	Remove o relatório selecionado completamente.

Para filtrar relatórios, clique em **Adicionar filtro** e selecione um tipo de filtro no menu suspenso ou insira uma string (repita ao combinar vários critérios):

Adicionar filtro	Uso
Nome	Digite o nome do relatório parcial ou completo.

Adicionar filtro	Uso
Agendado	Selecione Não agendado, Uma vez, Diariamente, Semanalmente ou Mensalmente.
Dados	Selecione o Exchange Online, OneDrive, Grupos de equipe ou sites do SharePoint para filtrar por dados.

Quarentena

Um simples gerenciamento de objetos (e-mails e arquivos) que foram colocados em quarentena pelo ESET Cloud Office Security. Alternar entre o Gmail, Google Drive, Exchange Online, OneDrive, Grupos de equipe e sites do SharePoint usando as guias. Você pode ver informações substanciais sobre cada objeto.

Clique no ícone para abrir a barra lateral com um resumo de um objeto específico. Para informações mais detalhadas, clique no ícone e selecione **Mostrar detalhes**.

Navegue dentro da árvore para ver as objetos apenas para um determinado locatário ou grupo. Para ver todas as detecções em cada locatário e grupo, clique em **Todos**.

Inspeciona os arquivos ou mensagens de e-mail colocados em quarentena e faz uma ação (**Remover** ou **Liberar**). Você também pode **Fazer download** do arquivo original ou do Arquivo protegido por senha no formato *.zip*.

> Quando você considera uma detecção não maliciosa (falso positivo), você pode **Liberar** um arquivo da Quarentena. O arquivo liberado é colocado automaticamente em uma lista de permissões, com base no hash. Todas as ocorrências futuras do mesmo arquivo, para o mesmo usuário, não serão detectadas como suspeitas e não serão colocadas em quarentena. A colocação automática na lista de permissões é feita por usuário. Para outros usuários, o mesmo arquivo continuará sendo detectado como suspeito e colocado em quarentena.
> Você pode remover um arquivo da lista de permissões na lista de Detecções usando a opção **Remover da lista de permissões**.

Clique no ícone e selecione uma ação:

Ação	Uso
Mostrar detalhes	Exibe informações mais detalhadas sobre a mensagem de e-mail colocada em quarentena.
Liberação (e-mails ou arquivos)	Libera o e-mail ao seu destinatário original na forma de um e-mail de notificação da Quarentena com a mensagem original como um anexo. No caso de um item do OneDrive, o arquivo será carregado para seu local original no OneDrive do usuário. Ao liberar um arquivo de um Grupo de equipe ou site do SharePoint, o arquivo vai aparecer de volta em sua localização original. O arquivo liberado é colocado automaticamente em uma lista de permissões, com base no hash. Isso impede que o arquivo seja colocado em quarentena novamente.
Excluir	Exclui itens da quarentena.
Fazer download do arquivo original	Fazer download do arquivo não protegido em sua forma original.
Fazer download do Arquivo protegido por senha	Fazer download do arquivo protegido por senha.
Enviar amostra	A caixa de diálogo de envio de amostra permite enviar um arquivo suspeito ou spam para a ESET para análise. Escolha um motivo para enviar uma amostra do menu suspenso.

Para facilitar a busca de um objeto específico colocado em quarentena, você pode filtrar usando vários critérios. Clique em **Adicionar filtro** e selecione o tipo de filtro no menu suspenso ou insira uma string (repita ao combinar critérios):

Adicionar filtro	Uso
Ocorreu de	Especifica um intervalo de "data a partir de".
Ocorreu a	Especifica um intervalo de "data até".
Assunto	Aplicável a mensagens que contêm ou não contêm uma string específica (ou uma expressão regular) no assunto.
ID da mensagem	Filtre mensagens de e-mail por um ID de mensagem único ao pesquisar uma mensagem específica, especialmente em grandes relatórios com muitas mensagens ou várias tentativas de entrega.
De	Filtra mensagens por remetente específico.
A	Filtra mensagens por destinatários.
Caixa de correio	Aplicável a mensagens localizadas em uma caixa de entrada específica.
Resultado do escaneamento	Selecione uma das seguintes opções: Malware, Malware (detectado por ESET LiveGuard Advanced), Phishing ou Spam.
Equipe	Digite o nome de equipe válido.
Objeto	Digite um nome de objeto válido.
Site	Digite um nome de site válido.

O período de retenção para objetos em quarentena é de 30 dias. Objetos com mais de 30 dias serão removidos da quarentena permanentemente.

Relatórios do escaneamento

Lista todos os resultados de escaneamento pelo ESET Cloud Office Security. Os relatórios são similares às Detecções, mas além disso, você pode ter objetos limpos incluídos na lista (ativar a configuração Registrar em relatório todos os objetos nas políticas). Alternar entre o Gmail, Google Drive, Exchange Online, OneDrive, Grupos de equipe, sites SharePoint e Arquivos enviados usando as guias. Você pode ver uma quantidade substancial de informações para cada detecção. Arquivos enviados é uma lista de arquivos enviados para análise pelo ESET LiveGuard Advanced.

Clique no ícone para abrir uma barra lateral com um resumo de um registro de relatório específico. Para informações mais detalhadas, clique no ícone e selecione **Mostrar detalhes**.

Navegue dentro da árvore para ver os registros de relatório apenas para um determinado locatário ou grupo. Para ver todas as detecções em cada locatário e grupo, clique em **Todos**.

Se um resultado de escaneamento for **Não escaneado**, o motivo pode variar. Veja as Limitações para detalhes.

Ao clicar no ícone de engrenagem no canto superior direito para acessar **Exportar para CSV** do menu de contexto, você pode exportar a tabela para o formato *CSV* e usá-la em outros aplicativos para trabalhar com a lista.

Para facilitar a busca por um registro em relatório em particular, você pode filtrar usando vários critérios. Clique em **Adicionar filtro** e selecione o tipo de filtro no menu suspenso ou insira uma string (repita ao combinar critérios):

Adicionar filtro	Uso
Ocorreu de	Especifica um intervalo de "data a partir de".
Ocorreu a	Especifica um intervalo de "data até".
Origem de dados	Selecione uma das seguintes opções: Exchange Online, OneDrive, Grupos de equipe e site do SharePoint.
Caixa de correio	Aplicável a mensagens localizadas em uma caixa de entrada específica.
De	Filtra mensagens por remetente específico.
A	Filtra mensagens por destinatários.
Assunto	Aplicável a mensagens que contêm ou não contêm uma string específica no assunto.
ID da mensagem	Filtre mensagens de e-mail por um ID de mensagem único ao pesquisar uma mensagem específica, especialmente em grandes relatórios com muitas mensagens ou várias tentativas de entrega.
Resultado do escaneamento	Selecione uma das seguintes opções: Malware, Malware (detectado pelo ESET LiveGuard Advanced), Phishing, Spam, Limpo, Não escaneado, Erro ou Desativado.
Ação	Selecionar uma das ações disponíveis.
Proprietários	Digite o nome de proprietário válido.
Objeto	Digite um nome de objeto válido.
Detecção	Digite um nome de detecção válido.
Hash	Digite um hash de detecção válido.
Equipe	Digite um nome de equipe válido.
Site	Digite um nome de site válido.

Há um período de retenção de 90 dias para registros de relatório. Registros anteriores a 90 dias serão removidos permanentemente. Se você tiver uma política que usa **Registrar todos os objetos**, a retenção para os registros de relatório com o resultado de escaneamento **Limpo** é de 3 dias. Resultados de escaneamento limpos com mais de três dias serão removidos permanentemente.

Políticas

Empresas maiores geralmente têm vários departamentos e querem configurar diferentes configurações de proteção para cada unidade organizacional. O ESET Cloud Office Security fornece configurações de proteção baseadas em políticas que você pode personalizar e atribuir a Usuários e Grupos de usuários, Locatários, Grupos de equipe ou sites SharePoint selecionados.

Para adicionar critérios de filtragem, clique em **Adicionar filtro** e selecione o **Nome** do item aplicável e digite o nome de política válido. A árvore de Políticas mostra Locatários e seus grupos de usuário, Grupos de equipe ou sites SharePoint, incluindo um grupo **Não atribuído** que contém políticas personalizadas que não estão atribuídas a nenhum usuário.

Você pode adicionar uma nova política ou modificar uma política existente e suas configurações:

1. Clique em **Políticas** > **Nova política**.

2. Digite um **Nome** e **Descrição** para uma nova política.

3. Selecione um destino e configure uma política para:

   - **Locatários** – Configure a proteção do Gmail, Google Drive, Exchange Online, OneDrive, sites SharePoint e

grupos de equipe e atribua-a a locatários selecionados

• **Usuários** – proteção do Gmail, Google Drive, Exchange Online e OneDrive, atribuída aos usuários selecionados ou ao(s) grupo(s) de usuário

• **Grupos de equipe** – Configure a proteção de grupos de equipe e atribua-a a grupos de equipe selecionados

• **Sites do SharePoint** – Configure a proteção a sites do SharePoint e atribua-a a sites selecionados

4. Personalize as **Configurações** de proteção para o Exchange online, Gmail, OneDrive, Google Drive, Grupos de equipe, Sites SharePoint ou ESET LiveGuard Advanced e clique em **Avançar**.

5. Clique em **Atribuir** e escolha um destino ao qual a política será atribuída.

6. Clique em **Salvar alterações** para salvar a configuração de política.

Princípios da política

Política padrão • Aplica-se a todos os usuários (protegidos e desprotegidos) • Não é possível modificar ou remover
A política personalizada pode ser atribuída a: • **Usuários** – aplicável a usuários individuais selecionados manualmente • **Grupos** – aplicável a todos os membros do grupo de usuários • **Locatários** – a política se aplica a todas as entidades dentro do locatário • **Grupos de equipe** – aplicável a um Grupo de equipe • **Sites SharePoint** – aplicável a um site do SharePoint
A política personalizada atribuída a um **Locatário** ou **Grupo** será mesclada com a política padrão A **Política de locatário**, **Política do grupo**, **Política de grupo de equipe** ou **Política de site SharePoint** tem prioridade sobre a política padrão A política personalizada atribuída a um **usuário** é mesclada com as políticas de **Locatário**, **Grupo**, **Grupos de equipe**, **sites SharePoint** e a política padrão Uma política de **Usuário** personalizada tem prioridade sobre uma diretiva de locatário ou de grupo e sobre uma diretiva padrão. Porém, quando um usuário envia um arquivo para o Grupo de equipe ou para o site SharePoint, a política para o Grupo de equipe ou do site SharePoint é aplicada.
Usuários e Locatários podem receber a atribuição de várias **políticas personalizadas**, mas a política eficiente é calculada com base na prioridade (ordem).

Configuração de listas Anti-spam ao mesclar políticas

A opção de mesclar se aplica às Listas Antispam e às configurações Notificar administrador (endereços para e-mails de notificação pelo Antimalware e Antiphishing).
Quando você tem várias políticas com listas Antispam (listas aprovadas, bloqueadas e ignoradas de endereços IP, domínios ou endereços de e-mail) ou endereços de administrador Antimalware e Antiphishing para e-mails de notificação, escolha a estratégia de mesclagem:
Substituir – mantém apenas as novas entradas da lista (opção padrão). As novas entradas de lista da política atual substituem todas as listas das políticas anteriores.
Anexar – estende as listas das políticas anteriores ao anexar novas entradas. Mescla listas das políticas anteriores com novas entradas da política atual. As novas entradas são colocadas no final (fundo) das listas existentes das políticas anteriores.

Antes da opção de mesclar se tornar disponível, o comportamento padrão era **Substituir**. Se você já estiver usando políticas com listas Antispam específicas, você pode manter o **Substituir** padrão ou alterar para **Anexar**, se for preferível.

Crie uma nova política com uma lista Antispam definida, e selecione a opção de mesclagem (assumindo que existem políticas com listas Antispam implementadas).
1. Clique em **Políticas** > **Nova política**.
2. Digite um **Nome** e **Descrição** para a nova política, selecione **Locatários** como destino e clique em **Avançar**.
3. Abra **Exchange Online - Antispam** e clique em **Editar** ao lado da lista de IP bloqueado.
4. Clique em **Adicionar**, digite o endereço IP, pressione a tecla **Enter** para concluir a ação (alternativamente, importe a lista de um arquivo) e clique em **Salvar alterações**.
5. Escolha **Anexar** como uma opção de mesclagem no menu suspenso e clique em **Avançar**.
6. Clique em **Atribuir**, escolha **Atribuir a locatários** do menu suspenso, selecione a caixa de seleção ao lado do locatário e clique em **OK**.
7. Clique em **Salvar alterações** para concluir o processo.

Para reorganizar a prioridade da política, clique em **Alterar ordem**. Selecione uma política, ou várias políticas, e clique em **Aplicar antes** ou **Aplicar depois** para alterar sua prioridade. As políticas serão aplicadas globalmente (independentemente da atribuição – locatário, grupo ou usuário) na ordem especificada, de cima para baixo. A política padrão será sempre aplicada primeiro.

Para realizar as ações a seguir, selecione a política e clique no ícone :

Ação	Uso
Mostrar detalhes	Exibe informações detalhadas sobre uma política criada, configurações e a quem as políticas estão atribuídas.
Editar	Editar a configuração de uma política existente.
Atribuir	Selecione Usuários, Locatários, Grupos de equipe ou sites do SharePoint aos quais a política se aplica.
Duplicar	Criar uma nova política com base no modelo selecionado. Um novo nome será necessário para a política duplicada.
Excluir	Remove completamente a política selecionada.

Cria uma política de locatário personalizada para ver todos os resultados de escaneamento (incluindo limpo) em Relatórios do escaneamento. A Política de locatário é aplicada a todos os usuários (protegidos e desprotegidos).

1. Clique em **Políticas** > **Nova política**.
2. Digite um **Nome** e **Descrição** para a nova política, selecione **Locatários** como destino e clique em **Avançar**.
3. Expanda o **Exchange Online – Configurações gerais** e clique na opção para ativar **Registrar todos os objetos**.
4. Expanda o **OneDrive – Configurações gerais** e clique na opção para ativar **Registrar todos os objetos**.
5. Expanda o **Grupos de equipe – Configurações gerais** e clique na opção para ativar **Registrar todos os objetos**.
6. Expanda os **Sites Sharepoint – Configurações gerais** e clique na opção para ativar **Registrar todos os objetos** e clique em **Avançar**.
7. Clique em **Atribuir**, selecione a caixa de seleção ao lado do locatário e clique em **OK**.
8. Clique em **Salvar alterações** para concluir o processo.

Crie uma política personalizada para usuários específicos com configurações avançadas que vão afetar a forma como o Malware, Spam e Phishing são tratados. Com essa política implementada, anexos de e-mail com malware serão removidos, as mensagens de spam serão movidas para a pasta de lixo do usuário, os e-mails de phishing terão seus assuntos marcados e colocados em quarentena, e o conteúdo dos arquivos de malware localizados no OneDrive será substituído pelo texto simples para evitar qualquer dano.

1. Clique em **Políticas** > **Nova política**.
2. Digite um **Nome** e **Descrição** para a nova política, selecione **Usuários** como destino e clique em **Avançar**.
3. Abra **Exchange Online - Antimalware** e use o menu suspenso ao lado de **Quando os itens são reportados** para selecionar **Remover anexo**.
4. Abra **Exchange Online - Antispam** e use o menu suspenso ao lado de **Quando os itens são reportados** para selecionar **Mover para o lixo eletrônico**.
5. Expanda o **Exchange Online – Antiphishing** e clique na opção para habilitar **Marcar assunto**. Você também pode alterar o **texto da Marcação no assunto** para personalizá-lo.
6. Abra **OneDrive - Antimalware**, use o menu suspenso ao lado de **Quando os itens são reportados** para selecionar **Substituir** e clique em **Avançar**.
7. Clique em **Atribuir**, marque as caixas de seleção ao lado dos usuários aos quais deseja aplicar a política e clique em **OK**. Se um usuário tiver uma política personalizada existente aplicada, ela será substituída pela nova.
8. Clique em **Salvar alterações** para concluir o processo.

Configurações de proteção para o Exchange Online

Esta seção fornece informações sobre como alterar configurações e opções gerais, Antimalware, Antispam ou Antiphishing do Exchange Online.

Exchange Online - Configurações gerais

ESET LiveGrid®Feedback sobre o
Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre ESET LiveGrid® no glossário .

Registrar todos os objetos
Se esta opção estiver selecionada, todos os resultados de escaneamento (incluindo limpos) serão exibidos em Relatórios do escaneamento. A política de retenção para resultados de escaneamento limpo é de três dias. Os resultados de escaneamento com mais de três dias serão removidos permanentemente.

Exchange Online - Antimalware

Habilitar o Antimalware do Exchange Online
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Proteção de relatórios e aprendizado de máquina
O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia o seguinte antes de modificar um limite (ou nível) para a categoria Relatório:
Quando os itens são reportados
- **Deixar** – deixar será realizada e o e-mail será entregue ao destinatário
- **Mover para o lixo eletrônico** – o e-mail será movido para a pasta de Lixo eletrônico.
- **Movido para o lixo** – o e-mail será movido para a pasta Lixo.
- **Remover mensagem** – o e-mail será excluído
- **Mensagem de quarentena** – o e-mail original será removido e uma cópia do e-mail será armazenada em quarentena. Se você decidir liberar o e-mail da quarentena, ele será enviado como um anexo em um novo e-mail e entregue ao destinatário.
- **Remover anexo** – o anexo da mensagem será removido, e a mensagem será entregue ao destinatário sem o anexo.
- **Substituir anexo** – o anexo é substituído por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
- **Anexo em quarentena** – o anexo será removido do e-mail e colocado na quarentena de arquivos.

Texto de substituição do anexo
Substitui o anexo por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
Assunto da marca
Quando ativado, você pode modificar os modelos adicionados ao assunto das mensagens infectadas.
Texto de assunto da marca
Você pode adicionar uma marcação personalizada aos assuntos das mensagens afetadas.
Notificar o proprietário da caixa de entrada
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Idioma
Escolha o idioma desejado no menu suspenso. O proprietário da caixa de entrada receberá e-mails de notificação no idioma selecionado quando um objeto for liberado da quarentena do Exchange Online. Essa opção substitui o idioma padrão do locatário nas configurações.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Exchange Online - Antispam

Habilitar o Antispam do Exchange Online
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Quando os itens são reportados
- **Deixar** – deixar será realizada e o e-mail será entregue ao destinatário
- **Mover para o lixo eletrônico** – o e-mail será movido para a pasta de Lixo eletrônico.
- **Movido para o lixo** – o e-mail será movido para a pasta Lixo.
- **Remover mensagem** – o e-mail será excluído
- **Mensagem de quarentena** – o e-mail original será removido e uma cópia do e-mail será armazenada em quarentena. Se você decidir liberar o e-mail da quarentena, ele será enviado como um anexo em um novo e-mail e entregue ao destinatário.

Assunto da marca
Quando ativado, você pode modificar os modelos adicionados ao assunto das mensagens infectadas.
Texto de assunto da marca
Você pode adicionar uma marcação personalizada aos assuntos das mensagens afetadas.
É possível configurar listas **Aprovadas**, **Bloqueadas** e **Ignoradas** ao especificar critérios como endereço IP ou intervalo, nome de domínio, etc. Para adicionar, modificar ou remover critérios, clique em **Editar** para a lista que deseja gerenciar. Alternativamente, você pode importar sua lista personalizada de um arquivo em vez de adicionar todas as entradas manualmente, clique em **Importar** e procure seu arquivo (*.txt*) que contém as entradas que você deseja adicionar à lista. De forma semelhante, se você precisar exportar sua lista existente para um arquivo (*.txt*), selecione **Exportar** do menu de contexto.

Lista de IP aprovada	Coloca automaticamente na lista de permissões e-mails originados de endereços IP especificados. O conteúdo do e-mail não será verificado.
Lista de IP bloqueada	Bloqueia automaticamente e-mails originados de endereços IP especificados.
Lista de IP ignorada	Lista de endereços IP que serão ignorados durante a classificação. O conteúdo do e-mail será verificado.
Lista de remetentes aprovados	Coloca na lista de permissões de e-mails originados de um remetente ou domínio específico. Apenas um endereço do remetente ou um domínio inteiro é usado para verificação com base na seguinte prioridade: 1.Endereço SMTP 'MAIL FROM' 2.Campo de cabeçalho do e-mail do "Return-Path:" 3.Campo de cabeçalho do e-mail do "X-Env-Sender:" 4.Campo de cabeçalho do e-mail do "From:" 5.Campo de cabeçalho do e-mail do "Sender:" 6.Campo de cabeçalho do e-mail do "X-Apparently-From:"
Lista de remetentes bloqueados	Bloqueia e-mails originados de um remetente ou domínio específico. Todos os endereços do remetente identificados ou domínios inteiros são usados para verificação: Endereço SMTP 'MAIL FROM' Campo de cabeçalho do e-mail do "Return-Path:" Campo de cabeçalho do e-mail do "X-Env-Sender:" Campo de cabeçalho do e-mail do "From:" Campo de cabeçalho do e-mail do "Sender:" Campo de cabeçalho do e-mail do "X-Apparently-From:"

Exchange Online Antiphishing

Habilitar o Antiphishing do Exchange Online
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Quando os itens são reportados
- **Deixar** – nenhuma ação será realizada e o e-mail com anexo malicioso será entregue ao destinatário.
- **Mover para o lixo eletrônico** – o e-mail será movido para a pasta de Lixo eletrônico.
- **Movido para o lixo** – o e-mail será movido para a pasta Lixo.
- **Remover mensagem** – o e-mail será excluído
- **Mensagem de quarentena** – o e-mail original será removido e uma cópia do e-mail será armazenada em quarentena. Se você decidir liberar o e-mail da quarentena, ele será enviado como um anexo em um novo e-mail e entregue ao destinatário.

Assunto da marca
Quando ativado, você pode modificar os modelos adicionados ao assunto das mensagens infectadas.
Texto de assunto da marca
Você pode adicionar uma marcação personalizada aos assuntos das mensagens afetadas.
Notificar o proprietário da caixa de entrada
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Notificar o administrador
Especifique o endereço de e-mail (tecle enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada para qualquer usuário do Exchange Online.

Configurações de proteção para Gmail

Esta seção fornece informações sobre como alterar configurações e opções gerais, Antimalware, Antispam ou Antiphishing do Gmail.

Gmail Geral

ESET LiveGrid®Feedback sobre o
Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre ESET LiveGrid® no glossário .
Registrar todos os objetos
Se esta opção estiver selecionada, todos os resultados de escaneamento (incluindo limpos) serão exibidos em Relatórios do escaneamento. A política de retenção para resultados de escaneamento limpo é de três dias. Os resultados de escaneamento com mais de três dias serão removidos permanentemente.

Gmail Antimalware

Ativar o Gmail Antimalware
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Proteção de relatórios e aprendizado de máquina
O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia o seguinte antes de modificar um limite (ou nível) para a categoria Relatório:
Quando os itens são reportados
- **Deixar** – deixar será realizada e o e-mail será entregue ao destinatário
- **Mover para o lixo eletrônico** – o e-mail será movido para a pasta de Lixo eletrônico.
- **Movido para o lixo** – o e-mail será movido para a pasta Lixo.
- **Remover mensagem** – o e-mail será excluído
- **Mensagem de quarentena** – o e-mail original será removido e uma cópia do e-mail será armazenada em quarentena. Se você decidir liberar o e-mail da quarentena, ele será enviado como um anexo em um novo e-mail e entregue ao destinatário.
- **Remover anexo** – o anexo da mensagem será removido, e a mensagem será entregue ao destinatário sem o anexo.
- **Substituir anexo** – o anexo é substituído por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
- **Anexo em quarentena** – o anexo será removido do e-mail e colocado na quarentena de arquivos.

Texto de substituição do anexo
Substitui o anexo por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
Assunto da marca
Quando ativado, você pode modificar os modelos adicionados ao assunto das mensagens infectadas.
Texto de assunto da marca
Você pode adicionar uma marcação personalizada aos assuntos das mensagens afetadas.
Notificar o proprietário da caixa de entrada
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Idioma
Escolha o idioma desejado no menu suspenso. O proprietário da caixa de entrada receberá e-mails de notificação no idioma selecionado quando um objeto for liberado da quarentena. Essa opção substitui o idioma padrão do locatário nas configurações.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Gmail Anti-Spam

Ativar o Gmail Antisspam
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Quando os itens são reportados
- **Deixar** – deixar será realizada e o e-mail será entregue ao destinatário
- **Mover para o lixo eletrônico** – o e-mail será movido para a pasta de Lixo eletrônico.
- **Movido para o lixo** – o e-mail será movido para a pasta Lixo.
- **Remover mensagem** – o e-mail será excluído
- **Mensagem de quarentena** – o e-mail original será removido e uma cópia do e-mail será armazenada em quarentena. Se você decidir liberar o e-mail da quarentena, ele será enviado como um anexo em um novo e-mail e entregue ao destinatário.

Assunto da marca
Quando ativado, você pode modificar os modelos adicionados ao assunto das mensagens infectadas.
Texto de assunto da marca
Você pode adicionar uma marcação personalizada aos assuntos das mensagens afetadas.
É possível configurar listas **Aprovadas**, **Bloqueadas** e **Ignoradas** ao especificar critérios como endereço IP ou intervalo, nome de domínio, etc. Para adicionar, modificar ou remover critérios, clique em **Editar** para a lista que deseja gerenciar. Alternativamente, você pode importar sua lista personalizada de um arquivo em vez de adicionar todas as entradas manualmente, clique em **Importar** e procure seu arquivo (*.txt*) que contém as entradas que você deseja adicionar à lista. De forma semelhante, se você precisar exportar sua lista existente para um arquivo (*.txt*), selecione **Exportar** do menu de contexto.

Lista de IP aprovada	Coloca automaticamente na lista de permissões e-mails originados de endereços IP especificados. O conteúdo do e-mail não será verificado.
Lista de IP bloqueada	Bloqueia automaticamente e-mails originados de endereços IP especificados.
Lista de IP ignorada	Lista de endereços IP que serão ignorados durante a classificação. O conteúdo do e-mail será verificado.
Lista de remetentes aprovados	Coloca na lista de permissões de e-mails originados de um remetente ou domínio específico. Apenas um endereço do remetente ou um domínio inteiro é usado para verificação com base na seguinte prioridade: 1.Endereço SMTP 'MAIL FROM' 2.Campo de cabeçalho do e-mail do "Return-Path:" 3.Campo de cabeçalho do e-mail do "X-Env-Sender:" 4.Campo de cabeçalho do e-mail do "From:" 5.Campo de cabeçalho do e-mail do "Sender:" 6.Campo de cabeçalho do e-mail do "X-Apparently-From:"
Lista de remetentes bloqueados	Bloqueia e-mails originados de um remetente ou domínio específico. Todos os endereços do remetente identificados ou domínios inteiros são usados para verificação: Endereço SMTP 'MAIL FROM' Campo de cabeçalho do e-mail do "Return-Path:" Campo de cabeçalho do e-mail do "X-Env-Sender:" Campo de cabeçalho do e-mail do "From:" Campo de cabeçalho do e-mail do "Sender:" Campo de cabeçalho do e-mail do "X-Apparently-From:"

Gmail Antiphishing

Ativar Gmail Antiphishing
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Quando os itens são reportados
- **Deixar** – nenhuma ação será realizada e o e-mail com anexo malicioso será entregue ao destinatário.
- **Mover para o lixo eletrônico** – o e-mail será movido para a pasta de Lixo eletrônico.
- **Movido para o lixo** – o e-mail será movido para a pasta Lixo.
- **Remover mensagem** – o e-mail será excluído
- **Mensagem de quarentena** – o e-mail original será removido e uma cópia do e-mail será armazenada em quarentena. Se você decidir liberar o e-mail da quarentena, ele será enviado como um anexo em um novo e-mail e entregue ao destinatário.

Assunto da marca
Quando ativado, você pode modificar os modelos adicionados ao assunto das mensagens infectadas.
Texto de assunto da marca
Você pode adicionar uma marcação personalizada aos assuntos das mensagens afetadas.
Notificar o proprietário da caixa de entrada
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Configurações de proteção para o OneDrive

Esta seção fornece informações sobre como alterar as configurações e opções gerais ou antimalware do OneDrive.

OneDrive - Configurações gerais

ESET LiveGrid®Feedback sobre o
Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre esses aplicativos no glossário.
Registrar todos os objetos
Se esta opção estiver selecionada, todos os resultados de escaneamento (incluindo limpos) serão exibidos em Relatórios do escaneamento. A política de retenção para resultados de escaneamento limpo é de três dias. Os resultados de escaneamento com mais de três dias serão removidos permanentemente.

OneDrive - Antimalware

OneDrive - Antimalware
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Proteção de relatórios e aprendizado de máquina
O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia o seguinte antes de modificar um limite (ou nível) para a categoria Relatório:
Quando os itens são reportados
- **Deixar** – deixar será realizada e o arquivo permanecerá no OneDrive
- **Mover para o lixo** – o arquivo será movido para a Lixeira.
- **Substituir** – o conteúdo do arquivo original será substituído pelo texto definido abaixo na janela Texto de substituição do arquivo.
- **Quarentena** – o arquivo original será movido para a Lixeira e copiado para a quarentena. Quando o arquivo é liberado, o arquivo removido anteriormente permanece no lixo e uma nova cópia é carregada para a pasta original do OneDrive.

Texto de substituição de arquivo
Substitui o anexo por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
Notificar o proprietário
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Configurações de proteção para o Google Drive

Esta seção fornece informações sobre como alterar as configurações e opções gerais ou antimalware do Google Drive.

Google Drive Geral

ESET LiveGrid®Feedback sobre o
Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre esses aplicativos no glossário.
Registrar todos os objetos
Se esta opção estiver selecionada, todos os resultados de escaneamento (incluindo limpos) serão exibidos em Relatórios do escaneamento. A política de retenção para resultados de escaneamento limpo é de três dias. Os resultados de escaneamento com mais de três dias serão removidos permanentemente.

Google Drive Antimalware

Google Drive Antimalware
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Proteção de relatórios e aprendizado de máquina
O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia o seguinte antes de modificar um limite (ou nível) para a categoria Relatório:
Quando os itens são reportados
- **Deixar** – deixar será realizada e o arquivo permanecerá no Google Drive
- **Mover para o lixo** – o arquivo será movido para a Lixeira.
- **Substituir** – o conteúdo do arquivo original será substituído pelo texto definido abaixo na janela Texto de substituição do arquivo.
- **Quarentena** – o arquivo original será movido para a Lixeira e copiado para a quarentena.
- **Remover** – o arquivo original é removido permanentemente do Google Drive.

Texto de substituição de arquivo
Substitui o anexo por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
Notificar o proprietário
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Configurações de proteção para Grupos de equipe

Esta seção fornece informações sobre como alterar as configurações e opções gerais dos Grupos de equipe ou Grupos de equipe antimalware.

Grupos de equipe - Configurações gerais

ESET LiveGrid®Feedback sobre o
Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre esses tipos de aplicativos no glossário.
Registrar todos os objetos
Se esta opção estiver selecionada, todos os resultados de escaneamento (incluindo limpos) serão exibidos em Relatórios do escaneamento. A política de retenção para resultados de escaneamento que estão limpos é de três dias. Os resultados de escaneamento com mais de três dias serão removidos permanentemente.

Grupos de equipe - Antimalware

Grupos de equipe - Antimalware
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Proteção de relatórios e aprendizado de máquina
O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia o seguinte antes de modificar um limite (ou nível) para a categoria Relatório:
Quando os itens são reportados
- **Nenhuma ação** – Nenhuma ação será realizada, o arquivo permanecerá intacto.
- **Movido para o lixo** – O arquivo será movido para a Lixeira de equipes.
- **Substituir** – o conteúdo do arquivo original será substituído pelo texto definido abaixo no campo "Texto de substituição do arquivo"
- **Quarentena** – o arquivo original será movido para a Lixeira de equipes e copiado para a Quarentena. Quando o arquivo é liberado, o arquivo removido anteriormente permanece na Lixeira e uma nova cópia é colocada de volta no local original.

Texto de substituição de arquivo
Substitui o anexo por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
Notificar o proprietário
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Configurações de proteção para sites SharePoint

Esta seção fornece informações sobre como alterar as configurações e opções gerais dos sites SharePoint ou sites do Sharepoint antimalware.

Sites Sharepoint - Configurações gerais

ESET LiveGrid®Feedback sobre o
Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre esses tipos de aplicativos no glossário.
Registrar todos os objetos
Se esta opção estiver selecionada, todos os resultados de escaneamento (incluindo limpos) serão exibidos em Relatórios do escaneamento. A política de retenção para resultados de escaneamento que estão limpos é de três dias. Os resultados de escaneamento com mais de três dias serão removidos permanentemente.

Sites Sharepoint - Antimalware

Sites Sharepoint - Antimalware
Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.
Proteção de relatórios e aprendizado de máquina
O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia o seguinte antes de modificar um limite (ou nível) para a categoria Relatório:
Quando os itens são reportados
- **Nenhuma ação** – Nenhuma ação será realizada, o arquivo permanecerá intacto.
- **Movido para o lixo** – O arquivo será movido para a lixeira do SharePoint.
- **Substituir** – o conteúdo do arquivo original será substituído pelo texto definido abaixo no campo "Texto de substituição do arquivo"
- **Quarentena** – o arquivo original será movido para a Lixeira do SharePoint e copiado para a Quarentena. Quando o arquivo é liberado, o arquivo removido anteriormente permanece na Lixeira e uma nova cópia é colocada de volta no local original.

Texto de substituição de arquivo
Substitui o anexo por um arquivo de texto que contém informações detalhadas sobre uma ação realizada.
Notificar o proprietário
Quando habilitado, o usuário receberá um e-mail de notificação quando uma detecção for encontrada.
Notificar o administrador
Especifique o endereço de e-mail (tecle Enter para adicionar vários endereços) que receberá e-mails de notificação sempre que uma detecção for encontrada.

Configurações de proteção para ESET LiveGuard Advanced

Para usar o recurso ESET LiveGuard Advanced, configure uma política que permita a análise ESET LiveGuard Advanced. Usuários ou grupos atribuídos com esta política terão proteção adicional. Os arquivos enviados para análise pelo ESET LiveGuard Advanced estão listados na guia Arquivos enviados, isto se aplica a amostras suspeitas desconhecidas (nunca vistas antes). Arquivos maliciosos conhecidos (com base em hash) não são enviados para análise pelo ESET LiveGuard Advanced.

Você verá os resultados do ESET LiveGuard Advanced nos Relatórios do escaneamento (Exchange Online, OneDrive, Grupos de equipe ou sites SharePoint) marcados como Malware .

ESET LiveGuard Advanced

Quando habilitado, este recurso está ativo e você pode configurar opções detalhadas.

> O ESET LiveGuard Advanced ativará automaticamente o feedback do ESET LiveGrid®. Os dados serão enviados para o ESET Research Lab para análise posterior. Leia mais sobre ESET LiveGrid® no glossário .

Limite de detecção

Resultados com um nível de limite selecionado e acima dele serão considerados como ameaças.

Envio automático de amostras suspeitas (menu suspenso)

Esta configuração está relacionada ao ESET LiveGrid® e permite as seguintes ações: Todos, Tudo exceto documentos, Nenhum.

Envio automático de amostras suspeitas (deslizante)

Escolha quais tipos de arquivo serão enviados para o ESET LiveGuard Advanced se eles conterem código suspeito, que se parece com ameaças ou apresentar características ou comportamento incomuns:

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

Remove amostras suspeitas dos servidores da ESET

Escolha quando remover as amostras que foram enviadas para análise. Remover amostras da nuvem ESET LiveGuard Advanced: Nunca, Depois de 30 dias, Imediatamente depois da análise.

Documentos

Use o controle deslizante para permitir que documentos, PDFs e outros tipos de documentos do Microsoft Office sejam enviados para análise pelo ESET LiveGuard Advanced.

Excluir documentos dos servidores da ESET

Remover amostras de formato de arquivo de documento da nuvem ESET LiveGuard Advanced: Nunca, Depois de 30 dias, Imediatamente depois da análise.

Proteção de relatórios e aprendizado de máquina

O mecanismo de detecção protege contra ataques de sistemas maliciosos ao escanear arquivos, e-mails e a comunicação de rede. Se um objeto classificado como malware for detectado, a correção será iniciada. O mecanismo de detecção pode eliminá-lo ao bloqueá-lo primeiro e, depois, realizar ações como limpeza, remoção ou mover para quarentena.

Proteção em tempo real e Machine Learning

O aprendizado de máquina avançado agora é uma parte do mecanismo de detecção como uma camada avançada de proteção, que melhora a detecção. Leia mais sobre esse tipo de proteção no glossário . Você pode configurar os Níveis de relatório para as categorias a seguir:

Malware

Um vírus de computador é um pedaço de código malicioso que é anexado a arquivos existentes no seu computador. Porém, o termo "vírus" é frequentemente mal usado. "Malware" (software malicioso) é um termo mais preciso. A detecção de malware é realizada pelo módulo do mecanismo de detecção combinado com o componente de aprendizado de máquina. Leia mais sobre esses tipos de aplicativos no glossário.

Aplicativos potencialmente indesejados (PUAs)

Um Aplicativo potencialmente indesejado é um software com uma intenção que não é inegavelmente maliciosa. Mas que pode instalar software indesejado adicional, alterar o comportamento do dispositivo digital, realizar atividades não aprovadas ou esperadas pelo usuário ou com outros objetivos que não estão claros.
Essa categoria inclui: software de exibição de propagandas, empacotadores de download, barras de ferramenta

variadas de navegadores, software com comportamento enganoso, bundleware, trackware.
Leia mais sobre esses tipos de aplicativos no glossário.

Aplicativos potencialmente suspeitos

É um software comprimido com empacotadores ou protetores usados frequentemente para impedir a engenharia reserva ou para ofuscar o conteúdo do arquivo executável (por exemplo, para ocultar a presença de malware) por métodos proprietários de compressão e/ou criptografia.
Essa categoria inclui: todos os aplicativos desconhecidos que são comprimidos com um compactador ou protetor frequentemente usado para comprimir malware.

Arquivos potencialmente inseguros

Essa classificação é dada para software comercial e legítimo que pode ser usado indevidamente para fins maliciosos. Um aplicativo inseguro refere-se a software comercial legítimo que tenha o potencial de ser usado indevidamente para fins maliciosos.
Essa categoria inclui: ferramentas de cracking, geradores de chave de licença, ferramentas de hacking, ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.
Leia mais sobre esses tipos de aplicativos no glossário.

Relatórios

O relatório é realizado pelo mecanismo de detecção e pelo componente de aprendizado de máquina. Você pode definir o limite de relatório para adaptá-lo melhor ao seu ambiente e às suas necessidades. Não há uma única configuração correta. Portanto, recomendamos que você monitore o comportamento dentro do seu ambiente e decida se uma configuração de Relatório diferente é mais adequada.

O relatório não realiza ação com objetos. Ele passa informações para uma respectiva camada de proteção e a camada de proteção realiza uma ação de acordo.

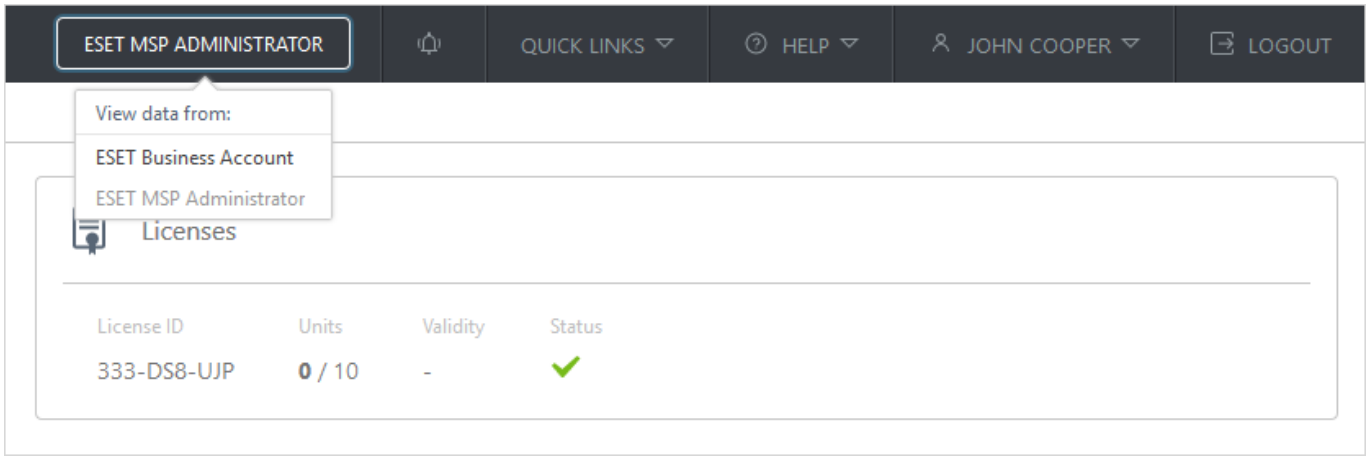
Agressivo	**Relatório configurado para sensibilidade máxima. Mais detecções são reportadas. Embora a configuração Agressiva possa parecer a mais segura, ela pode ser frequentemente muito sensível, o que pode até ser contraproducente.** A configuração agressiva pode identificar erroneamente os objetos como maliciosos, e a ação será realizada com esses objetos (dependendo das configurações de Proteção).
Equilibrado	Essa configuração é um equilíbrio ideal entre desempenho e precisão de taxas de detecção e o número de objetos erroneamente reportados.
Cuidado	Relatório configurado para minimizar objetos identificados erroneamente enquanto mantém um nível suficiente de proteção. Os objetos são reportados apenas quando a probabilidade é evidente e quando correspondem ao comportamento malicioso.
Desativar	O relatório não está ativo. As detecções não são encontradas, reportadas ou limpas. Não foi possível desativar o relatório de malware, portanto a configuração Desativado não está disponível para Malware.

Gerenciamento de licenças

Na janela principal, você terá uma visão geral das licenças que estão sendo puxadas do ESET Business Account ou ESET MSP Administrator. Você pode ver todos os pools de licença, sites ou empresas que estão disponíveis no ESET Business Account ou no portal ESET MSP Administrator. O gerenciamento de licenças permite a você

proteger ou desproteger usuários.

Se você tiver o mesmo endereço de e-mail registrado no ESET MSP Administrator e no ESET Business Account (login único), você pode alternar entre a visualização do ESET Business Account e a do ESET MSP Administrator (conta de licenciamento híbrido).



A licença ESET Cloud Office Security permite que você use o recurso ESET LiveGuard Advanced gratuitamente. Você verá o rótulo ELG ao lado do ID de licença.

Gerenciamento de licenças com o ESET Business Account

Exibe informações da licença e uso (nome do pool de licenças, ID da licença, unidades, validade e status). As licenças e os pools de licença são carregados do ESET Business Account. Pools de licença estão disponíveis apenas se você tiver sites existentes no ESET Business Account. (sites são úteis para categorização). Uma unidade representa a proteção ESET Cloud Office Security de um único usuário para o Exchange Online e OneDrive.

> Uma unidade de licença é usada por cada usuário protegido. Isto independentemente de quais serviços Microsoft 365 são usados. Um usuário com o Exchange Online ou OneDrive (ou ambos) sempre consome uma unidade de licença.
> Uma unidade de licença não é usada por grupos de equipe ou sites do SharePoint.

Todo novo usuário será exibido na seção Usuários como Desprotegido. Se você usar proteção automática por Locatário ou Grupo, novos usuários serão protegidos automaticamente e aparecerão como Protegidos.
Ao proteger os usuários, você tem duas opções:

- **Proteção automática por Locatário ou Grupo (recomendado)** – sem necessidade de manutenção, qualquer usuário recém-adicionado que esteja em um grupo do Azure AD, ou que pertença a um Locatário, será automaticamente protegido. Veja a observação abaixo para detalhes.
- **Proteção individual do usuário** – requer gerenciamento e você deve proteger manualmente cada novo usuário.

Proteger usuários (sem Pool de licença)

1. Clique em **Proteger**.
2. Selecione o Locatário ou Grupo para a proteção automática de usuário e clique em **Proteger**. Para proteção de usuários individuais, selecione os usuários que deseja proteger e clique em **Proteger**. A política Padrão agora protege os usuários.
3. Se necessário, especifique uma política personalizada para os usuários na seção Políticas.

Proteger usuários (usando o Pool de licença)

1. Selecione o Pool de licença e clique no ícone de três pontos > **Mostrar detalhes** ao lado do pool de licenças.
2. Clique em **Proteger**.
3. Selecione o Locatário ou Grupo para a proteção automática de usuário e clique em **Proteger**. Para proteção de usuários individuais, selecione os usuários que deseja proteger e clique em **Proteger**. A política Padrão agora protege os usuários.
4. Se necessário, especifique uma política personalizada para os usuários na seção Políticas.

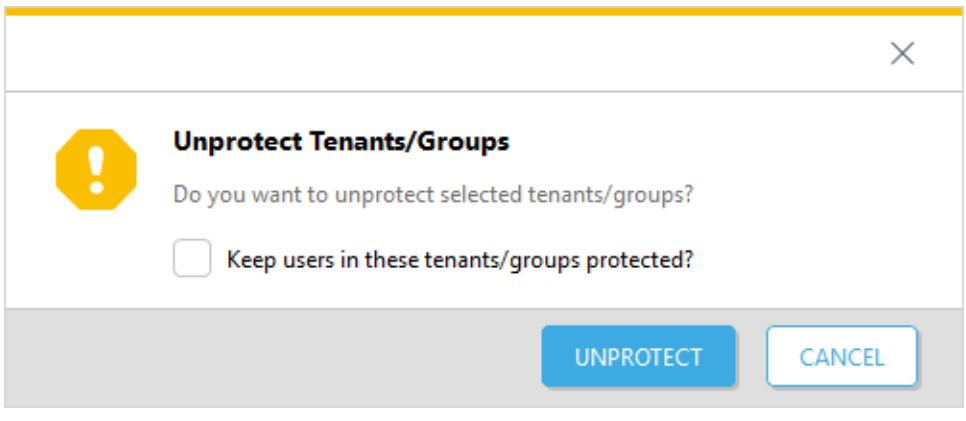
> Certifique-se de ter unidades de licença suficientes, especialmente com a proteção automática habilitada quando o número de usuários aumentar. Quando todas as unidades de licença são usadas, qualquer novo usuário que se tornar membro de um Locatário ou Grupo não será protegido. A proteção de usuários existentes continua não sendo afetada.
> Se você estiver temporariamente sem unidades de licença e quiser que usuários específicos sejam protegidos, use grupos desprotegidos (não use a proteção automática) e proteja manualmente os usuários. Depois de aumentar os pools de licença com mais unidades, você pode reverter para proteção automática para facilitar o gerenciamento.

Mover

Para mover os usuários entre os pools de licença e para operações mais avançadas com licenças, clique em abrir ESET Business Account .

Desprotegido

1. Selecione usuários individuais, um locatário ou um grupo e clique em **Desproteger**.
2. Ao remover a proteção automática do Locatário ou Grupo, você será solicitado a confirmar se deseja **Manter os usuários nesses locatários/grupos protegidos**. Se você optou por não usar essa opção, os usuários ficarão desprotegidos. Se você marcar a caixa de seleção, a proteção de locatário ou grupo será desativada e mudará para proteção de usuário individual. Os usuários ainda estão protegidos, mas você deve proteger manualmente todos os usuários recém-adicionados.



Exibe informações da licença e uso (empresa do cliente, ID da licença, unidades e status).

> Uma unidade de licença é usada por cada usuário protegido. Isto independentemente de quais serviços Microsoft 365 são usados. Um usuário com o Exchange Online ou OneDrive (ou ambos) sempre consome uma unidade de licença.
> Uma unidade de licença não é usada por grupos de equipe ou sites do SharePoint.

Todo novo usuário será exibido na seção Usuários como **Desprotegido**. Se você usar proteção automática por Locatário ou Grupo, novos usuários serão protegidos automaticamente e aparecerão como **Protegidos**.
Ao proteger os usuários, você tem duas opções:

- **Proteção automática por Locatário ou Grupo (recomendado)** – sem necessidade de manutenção, qualquer usuário recém-adicionado que seja membro do grupo Azure AD, ou que pertença a um Locatário, será automaticamente protegido. Veja a observação abaixo para detalhes.
- **Proteção individual do usuário** – requer o gerenciamento e você precisará proteger manualmente todos os novos usuários.

Proteger usuários

1. Clique em **Proteger**.
2. Selecione o Locatário ou Grupo para a proteção automática de usuário e clique em **Proteger**. Para proteção de usuários individuais, selecione os usuários que deseja proteger e clique em **Proteger**. A política Padrão agora protege os usuários.
3. Se necessário, especifique uma política personalizada para os usuários na seção Políticas.

> Certifique-se de ter unidades de licença suficientes, especialmente com a proteção automática habilitada quando o número de usuários aumentar. Quando todas as unidades de licença são usadas, qualquer novo usuário que se tornar membro de um Locatário ou Grupo não será protegido. A proteção de usuários existentes continua não sendo afetada.
> Se você estiver temporariamente sem unidades de licença e quiser que usuários específicos sejam protegidos, use grupos desprotegidos (não use a proteção automática) e proteja manualmente os usuários. Depois de aumentar os pools de licença com mais unidades, você pode reverter para proteção automática para facilitar o gerenciamento.

Desprotegido

1. Selecione usuários individuais, um locatário ou um grupo e clique em **Desproteger**.
2. Ao remover a proteção automática do Locatário ou Grupo, você será solicitado a confirmar se deseja **Manter os usuários nesses locatários/grupos protegidos**. Se você optou por não usar essa opção, os usuários ficarão desprotegidos. Se você marcar a caixa de seleção, a proteção de locatário ou grupo será desativada e mudará para proteção de usuário individual. Os usuários ainda estão protegidos, mas você deve proteger manualmente todos os usuários recém-adicionados.

Acesso do usuário do ESET Cloud Office Security a uma empresa específica

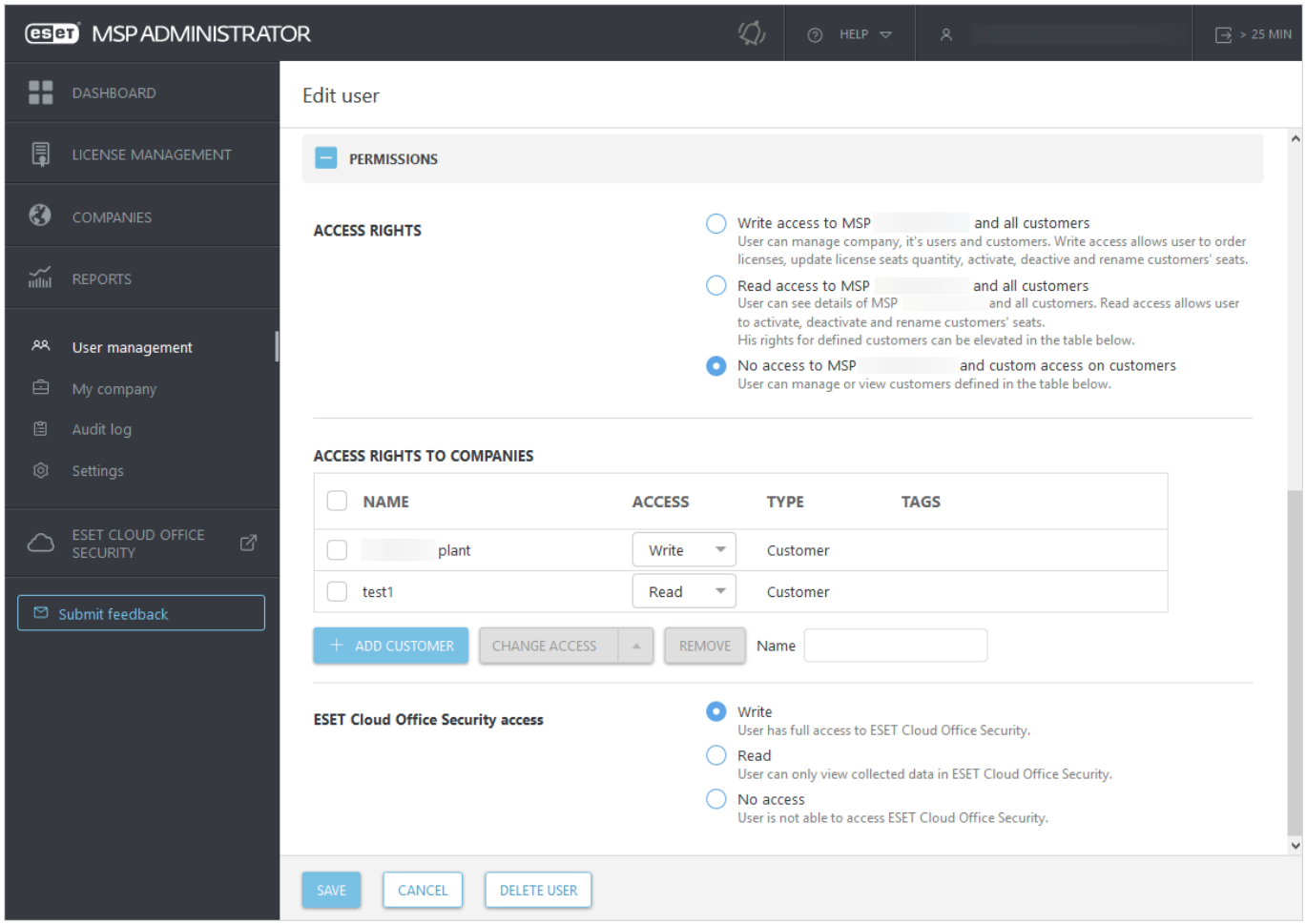
Em um ambiente com vários locatários, você pode fornecer a um usuário acesso ao ESET Cloud Office Security para permitir que o usuário veja apenas uma empresa específica (com permissão de leitura ou gravação). Geralmente é usado por MSPs.

Configure os direitos de acesso de usuário no ESET MSP Administrator ao atribuir a uma empresa a permissão de **Gravação** e acesso à **Gravação** para o ESET Cloud Office Security:

1. Entre no ESET MSP Administrator como administrador.

2. Edite um usuário e configure os **Direitos de acesso para empresas** sob Permissões, e selecione o acesso de **Gravação**. O usuário pode ver apenas a empresa atribuída com seu pool de licenças.

3. Defina o acesso de **Gravação** para o ESET Cloud Office Security para que o usuário possa proteger uma empresa adicionando um locatário. Um usuário com acesso de Leitura não é capaz de adicionar ou remover um locatário.



Apenas um tipo de acesso ao ESET Cloud Office Security pode ser configurado como uma configuração global e se aplica a todas as empresas (se um usuário estiver atribuído a várias empresas).

Relatório de auditoria

Escaneia alterações na configuração ou proteção do ESET Cloud Office Security. Os registros de Relatório de auditoria não fazem parte das atividades e mostram a sequência na qual ocorreram. Os relatórios de auditoria armazenam informações sobre a operação ou evento específico. Os relatórios de auditoria são criados sempre que um objeto ESET Cloud Office Security (pool de licenças, usuário, política, relatório, item de quarentena como anexo) é criado ou modificado.

Ao clicar no ícone de engrenagem no canto superior direito para acessar **Exportar para CSV** do menu de contexto, você pode exportar a tabela para o formato *CSV* e usá-la em outros aplicativos para trabalhar com a lista.

Clique no ícone para abrir uma barra lateral com um resumo de um Relatório de auditoria específico. Para informações mais detalhadas, clique no ícone e selecione **Mostrar detalhes**.

Bloco	Detalhe
Informações básicas	Exibe os dados gerais do relatório de auditoria (Ocorreu, Ação, Gravidade, Resultado, Seção).
Usuário	Exibe informações sobre o usuário que fez a ação ou uma alteração, incluindo o e-mail e o endereço IP do usuário.
Alterações	Detalhes sobre as alterações feitas.
Configurações antigas	Exibe configurações de política anteriores.
Novas configurações	Exibe as configurações de política atual.
Objetos	Lista os objetos afetados pela alteração ou ação (usuário, política, anexo, etc.).

Você pode filtrar os usuários por vários critérios. Clique em **Adicionar filtro** e selecione um tipo de filtro no menu suspenso ou insira uma string (repita ao combinar vários critérios):

Adicionar filtro	Uso
Ação	Selecionar uma das ações disponíveis.
Objeto	Digite um nome de objeto válido.
Status	Selecione uma das seguintes opções: Sucesso, Falha, Iniciado ou Parcialmente bem-sucedido
Usuário	Digite o usuário que realizou alterações.
Gravidade	Selecione o nível de gravidade: Baixo, Médio ou Alto
Ocorreu a partir de / Ocorreu até	Filtrar pela hora da ocorrência. Use Ocorreu a partir de e clique na data para exibir somente registros mais novos do que a data especificada. Use Ocorreu para registros anteriores a, ou use ambos para o intervalo de tempo desejado.
Sistema iniciado	Filtra os registros feitos pelo sistema.

Enviar feedback

Para enviar seu feedback, no seu console ESET Cloud Office Security, use a barra de ferramentas no canto superior direito, passe o cursor do mouse sobre a **Ajuda** e clique em **Enviar feedback**, escolha **Dê sua opinião** (compartilhar ideias e experiências) ou **Relatar um problema ou bug**.

Suporte técnico

Use os links a seguir com informações de suporte que o ajudarão a solucionar eventuais problemas:

Pesquisar a base de conhecimentos ESET

Base de conhecimento ESET contém as respostas à maioria das perguntas mais frequentes e as soluções recomendadas para diversos problemas. A atualização regular feita pelos especialistas técnicos da ESET tornam a base de conhecimento a ferramenta mais poderosa para a solução de diversos tipos de problemas.

Visite o Fórum de Segurança ESET

Fórum de suporte O Fórum ESET fornece aos usuários da ESET uma maneira fácil de obter ajuda e ajudar os outros. Você pode postar qualquer problema ou pergunta relacionada aos seus produtos ESET.

Entrar em contato com o Suporte técnico

Formulário de Suporte Técnico ESET Preencha o formulário para fornecer seus dados, incluindo a descrição do problema.

Entre em contato com seu parceiro ESET local para obter suporte

Entre em contato com o suporte local da ESET Localize as informações de contato de suporte para o suporte ESET em sua região do seu e-mail de licença ESET.

Enviar feedback

Enviar feedback Dê sua opinião (compartilhe ideias e experiências) ou reporte um problema ou bug.

Sugerir melhoria na Ajuda on-line

Você pode postar sua classificação e fornecer feedback sobre um tópico específico na Ajuda on-line clicando no link **Esta informação foi útil?** abaixo da página de ajuda. Diga-nos se o conteúdo ajudou ou como você acha que o Redator técnico pode melhorá-lo.

Disponibilidade do serviço

O Portal de Status ESET exibe o status atual dos serviços de nuvem da ESET, interrupções programadas e incidentes passados. Se você estiver enfrentando um problema com um serviço ESET e não o vir listado no Portal de Status, entre em contato com o Suporte Técnico ESET.

As equipes de monitoramento verificam possíveis problemas internamente e os incidentes confirmados são postados e atualizados manualmente para manter a credibilidade e precisão. Portanto, eles aparecem no Portal de Status com um pequeno atraso. Podemos não publicar incidentes curtos se eles forem resolvidos antes de serem confirmados manualmente.

Security for ESET Cloud Office Security

Introdução

O objetivo deste documento é controlar as práticas de segurança e os controles de segurança aplicados dentro do ESET Cloud Office Security. As práticas e controles de segurança são feitos para proteger a confidencialidade, integridade e disponibilidade das informações do cliente. Observe que as práticas e controles de segurança podem mudar.

Escopo

O escopo deste documento é ampliar as práticas de segurança e controles de segurança para infraestrutura do ESET Cloud Office Security, ESET Business Account (doravante chamado de "EBA"), ESET Data Framework, ESET LiveGrid, Atualização, AntiSpam, infraestrutura do ESET Dynamic Threat Defense, organização, pessoal e processos operacionais. Práticas e controles de segurança incluem:

1. Políticas de segurança da informação
2. Organização da segurança da informação

3. Segurança de recursos humanos
4. Gerenciamento de ativos
5. Controle de Acesso
6. Criptografia
7. Segurança física e ambiental
8. Segurança de operações
9. Segurança de comunicações
10. Aquisição, desenvolvimento e manutenção do sistema
11. Relação de fornecedor
12. Gerenciamento de incidentes de segurança de informações
13. Aspectos de segurança de informação do gerenciamento de continuidade dos negócios
14. Compliance

Conceito de segurança

A empresa ESET s.r.o. é certificada pela ISO 27001:2013 com o escopo de sistema de gerenciamento integrado explicitamente cobrindo ESET Cloud Office Security, EBA e outros serviços.

Portanto, o conceito de segurança da informação usa a estrutura ISO 27001 para implementar uma estratégia de defesa de segurança em camadas ao aplicar controles de segurança na camada de rede, sistemas operacionais, bancos de dados, aplicativos, pessoal e processos operacionais. As práticas de segurança aplicadas e controles de segurança têm como objetivo se sobrepor e se complementar.

Práticas e controles de segurança

1. Políticas de segurança da informação

A ESET usa políticas de segurança da informação para cobrir todos os aspectos do padrão ISO 27001, incluindo a governança da segurança da informação e controles e práticas de segurança. As políticas são revisadas anualmente e atualizadas depois de alterações significativas para garantir sua adequação e eficácia contínuas.

A ESET realiza revisões anuais desta política e verificações de segurança internas para garantir a coerência com esta política. A não conformidade com as políticas de segurança da informação está sujeita a ações disciplinares para os funcionários da ESET ou penalidades contratuais até a rescisão do contrato para os fornecedores.

2. Organização da segurança da informação

A organização da segurança da informação para ESET Cloud Office Security é composta por várias equipes e pessoas envolvidos na segurança da informação e de TI, incluindo:

- Gerenciamento executivo da ESET
- Equipes de segurança interna da ESET
- Equipes de TI de aplicativos empresariais
- Outras equipes de apoio

As responsabilidades de segurança da informação são alocadas alinhadas com as políticas de segurança da informação implementadas. Processos internos são identificados e avaliados para qualquer risco de modificação não autorizada ou não intencional ou uso indevido dos ativos ESET. Atividades perigosas ou sensíveis de processos internos adotam o princípio da separação de deveres para mitigar o risco.

A equipe jurídica da ESET é responsável por contatos com autoridades do governo, incluindo reguladores eslovacos sobre cibersegurança e proteção de dados pessoais. A equipe de Segurança Interna da ESET é

responsável por entrar em contato com grupos de interesse especiais como ISACA. A equipe do laboratório de pesquisa da ESET é responsável pela comunicação com outras empresas de segurança e pela comunidade de cibersegurança em geral.

A segurança de informações é contada no gerenciamento de projeto usando a estrutura de gerenciamento de projeto aplicada, desde a concepção do projeto até sua conclusão.

O trabalho remoto e a troca de dados são cobertos pelo uso de uma política implementada em dispositivos móveis, que inclui o uso de uma forte proteção criptográfica de dados em dispositivos móveis enquanto viajam por redes não confiáveis. Controles de segurança em dispositivos móveis são projetados para funcionar independentemente das redes internas e dos sistemas internos da ESET.

3. Segurança de recursos humanos

A ESET usa práticas padrão de recursos humanos, incluindo políticas projetadas para ajudar na segurança da informação. Essas práticas cobrem todo o ciclo de vida dos funcionários, e são aplicadas a todas as equipes que acessam o ambiente ESET Cloud Office Security.

4. Gerenciamento de ativos

A infraestrutura ESET Cloud Office Security é incluída nas responsabilidades da ESET com propriedade rígida e regras aplicadas de acordo com o tipo de modelo e sensibilidade. A ESET tem um esquema de classificação interna definido. Todos os dados e configurações do ESET Cloud Office Security são classificados como confidenciais.

5. Controle de Acesso

A política de Controle de acesso da ESET governa todos os acessos no ESET Cloud Office Security. O controle de acesso é definido na infraestrutura, serviços de rede, sistema operacional, banco de dados e nível de aplicativo. O gerenciamento completo do acesso do usuário no nível do aplicativo é autônomo. O login único do ESET Cloud Office Security e ESET Business Account é governado por um provedor de identidade central, que garante que o usuário possa acessar apenas o locatário autorizado. O aplicativo usa permissões padrão do ESET Cloud Office Security para aplicar o controle de acesso baseado em função para o locatário.

O acesso ao backend da ESET é estritamente limitado a pessoas e funções autorizadas. Processos padrão da ESET para (des)registro de usuário, (de)provisionamento, gerenciamento de privilégios e revisão dos direitos de acesso do usuário são usados para gerenciar o acesso de funcionários da ESET à infraestrutura e às redes do ESET Cloud Office Security.

Uma autenticação forte está implementada para proteger o acesso a todos os dados do ESET Cloud Office Security.

6. Criptografia

Para proteger os dados do ESET Cloud Office Security, uma criptografia forte é usada para criptografar dados em descanso e em trânsito. Uma autoridade de certificação geralmente confiável é usada para emitir certificados para serviços públicos. A infraestrutura interna de chave pública ESET é usada para gerenciar chaves dentro da infraestrutura do ESET Cloud Office Security. Os dados armazenados no banco de dados são protegidos por chaves de criptografia geradas pela nuvem. Todos os dados de backup são protegidos por chaves gerenciadas pela ESET.

7. Segurança física e ambiental

Como o ESET Cloud Office Security e o ESET Business Account são baseados na nuvem, contamos com o Microsoft Azure para a segurança física e ambiental. O Microsoft Azure usa centros de dados certificados com medidas robustas de segurança física. A localização física do centro de dados depende da escolha da região do cliente.

8. Segurança de operações

O serviço ESET Cloud Office Security é operado através de meios automatizados com base em procedimentos operacionais e modelos de configuração estritos. Todas as alterações, incluindo alterações de configuração e nova implantação de pacote, são aprovadas e testadas em um ambiente de teste dedicado antes da implantação para a produção. Ambientes de desenvolvimento, teste e produção são separados um do outro. Os dados ESET Cloud Office Security estão localizados apenas no ambiente de produção.

O ambiente ESET Cloud Office Security é supervisionado usando o monitoramento operacional para identificar problemas e fornecer capacidade suficiente para todos os serviços na rede e nos níveis de host.

Todos os dados de configuração são armazenados em nossos repositórios de backup regulares para permitir a recuperação automatizada da configuração de um ambiente. Os backups de dados ESET Cloud Office Security são armazenados no local e fora do local.

Backups são criptografados e testados regularmente para capacidade de recuperação como parte de testes de negócios.

A auditoria em sistemas é realizada de acordo com padrões e diretrizes internos. Relatórios e eventos da infraestrutura, sistema operacional, banco de dados, servidores de aplicativo e controles de segurança são coletados continuamente. Os relatórios são processados ainda mais por equipes de TI e segurança interna para identificar anomalias operacionais e de segurança e incidentes de segurança de informações.

A ESET usa um processo geral de gerenciamento de vulnerabilidades técnicas para lidar com a ocorrência de vulnerabilidades na infraestrutura ESET, incluindo ESET Cloud Office Security e outros produtos ESET. Esse processo inclui o escaneamento proativo de vulnerabilidade e testes repetitivos de segurança de infraestrutura, produtos e aplicativos.

A ESET declara diretrizes internas para a segurança da infraestrutura interna, redes, sistemas operacionais, bancos de dados, servidores de aplicativos e aplicativos. Essas diretrizes são verificadas através do monitoramento de conformidade técnica e do nosso programa interno de auditoria de segurança de informações.

9. Segurança de comunicações

O ambiente ESET Cloud Office Security é segmentado através da segmentação de nuvem nativa com acesso de rede limitado apenas aos serviços necessários entre os segmentos de rede. A disponibilidade de serviços de rede é realizada através de controles nativos da nuvem como zonas de disponibilidade, balanceamento de carga e redundância. Componentes dedicados de balanceamento de carga são implantados para fornecer endpoints específicos para roteamento de instância do ESET Cloud Office Security que aplicam a autorização de tráfego e balanceamento de carga. O tráfego da rede é monitorado continuamente em busca de anomalias operacionais e de segurança. Os potenciais ataques podem ser resolvidos usando controles nativos de nuvem ou soluções de segurança implantadas. Toda a comunicação de rede é criptografada através de técnicas geralmente disponíveis, incluindo IPsec e TLS.

10. Aquisição, desenvolvimento e manutenção do sistema

O desenvolvimento de sistemas ESET Cloud Office Security é realizado de acordo com a política de

desenvolvimento de software seguro da ESET. Equipes de segurança interna são incluídas no projeto de desenvolvimento do ESET Cloud Office Security desde a fase inicial e supervisionam todas as atividades de desenvolvimento e manutenção. A equipe de segurança interna define e verifica o cumprimento dos requisitos de segurança em diversos momentos do desenvolvimento do software. A segurança de todos os serviços, incluindo os recentemente desenvolvidos, é testada continuamente depois do lançamento.

11. Relação de fornecedor

Uma relação de fornecedor relevante é conduzida de acordo com diretrizes válidas da ESET, que cobrem o gerenciamento de relacionamento por completo e os requisitos contratuais da perspectiva de segurança da informação e privacidade. A qualidade e a segurança dos serviços prestados pelo provedor de serviço crítico são avaliados regularmente.

12. Gerenciamento de segurança de informações

O gerenciamento de incidentes de segurança de informações no ESET Cloud Office Security é realizado de forma similar a outras infraestruturas da ESET e conta com procedimentos de resposta a incidentes definidos. As funções dentro da resposta a incidentes são definidas e alocadas em várias equipes, incluindo TI, segurança, jurídico, recursos humanos, relações públicas e gerenciamento executivo. A equipe de resposta a incidentes para um incidente é estabelecida com base na triagem de incidentes pela equipe de segurança interna. Essa equipe fornecerá ainda mais informações sobre outras equipes lidando com o incidente. A equipe de segurança interna também é responsável pela coleta de provas e por lições aprendidas. A ocorrência e a resolução de incidentes são comunicadas às partes afetadas. A equipe jurídica da ESET é responsável por notificar os corpos regulatórios se necessário, de acordo com o Regulamento Geral de Proteção de Dados (GDPR) e com a Lei de Cibersegurança que transpõe a Diretiva de Segurança da Informação e Rede (NIS).

13. Aspectos de segurança de informação do gerenciamento de continuidade dos negócios

A continuidade de negócios do serviço ESET Cloud Office Security é codificada na arquitetura robusta usada para aumentar ao máximo a disponibilidade dos serviços fornecidos. A restauração completa de dados de backup e configuração fora do local é possível no caso de uma falha total de todos os nós redundantes para componentes do ESET Cloud Office Security ou o serviço ESET Cloud Office Security. O processo de restauração é testado regularmente.

14. Compliance

A conformidade com os requisitos regulatórios e contratuais do ESET Cloud Office Security é regularmente avaliada e revisada de maneira semelhante a outras infraestruturas e processos da ESET, e as medidas necessárias são realizadas continuamente para garantir a conformidade. A ESET está registrada como um provedor de serviço digital para o serviço digital de Computação em nuvem, que cobre vários serviços ESET, inclusive o ESET Cloud Office Security. Observe que as atividades de conformidade da ESET não necessariamente significam que os requisitos gerais de conformidade dos clientes estão cumpridos como tal.

Termos de uso

Em vigor a partir de 23 de outubro de 2023 | Veja uma versão anterior dos Termos de Uso | Comparar alterações

Este Contrato ESET Cloud Office Security (doravante os "Termos") constitui o contrato especial entre a ESET, spol. s r. o., tendo sua sede em Einsteinova 24, 85101 Bratislava, Slovak Republic, registrada no Registro Comercial administrado pelo Tribunal Regional de Bratislava I, Seção Sro, Registro Nº. 3586/B, Número de Registro Comercial: 31333532 (doravante a "ESET" ou "Provedor") e você, uma pessoa física ou jurídica (doravante "Você"

ou "Usuário") que acessa uma conta para administração, ESET Cloud Office Security e que acessa um portal baseado na web que é de propriedade de e controlado pela ESET (doravante a "Conta") para usar o ESET Cloud Office Security. Se você usar a Conta e o ESET Cloud Office Security (doravante denominados conjuntamente "Produto") em nome de uma organização, então estará concordando com estes Termos para essa organização e estará garantindo que tem a autoridade para vincular essa organização a estes Termos. Nesse caso, Você e Usuário se referirão a essa organização. Leia esses Termos com cuidado, eles se relacionam também aos serviços prestados pela ESET através de ou em relação ao Produto. As condições específicas para o uso de serviços individuais além desses Termos são declaradas em cada serviço, com a aceitação fazendo parte do processo de ativação do serviço. Os anexos a este documento suplementam os Termos.

Segurança e Proteção de dados

A Conta oferece acesso aos serviços fornecidos pela ESET. O nome completo do usuário, nome da empresa, país, endereço de email válido, número de telefone, dados de licenciamento e estatísticas são necessários para o registro e uso da Conta e para o fornecimento e manutenção dos serviços acessados através da Conta. Você doravante concorda que dados sejam coletados e transferidos para os servidores do Provedor ou de seus parceiros, sendo a finalidade disso garantir a funcionalidade e a autorização para usar os serviços do Software e a proteção dos direitos do Provedor. Seguindo a conclusão destes Termos, o Provedor ou qualquer de seus parceiros comerciais terão o direito de transferir, processar e armazenar dados essenciais que identifiquem Você para fins de suporte e para os fins da execução destes Termos. Você está autorizado a usar a Conta apenas para os fins e para a forma pretendidos sob esses Termos, termos de serviço individuais e documentação.

Você é responsável por manter a segurança da sua Conta e das credenciais necessárias para fazer login. A ESET não será responsável por quaisquer perdas ou danos resultantes da sua falha em cumprir com esta obrigação de manter a segurança. O Usuário também é responsável por qualquer atividade relacionada ao uso da Conta, autorizada ou não. Se a Conta for comprometida você deve notificar o Provedor imediatamente.

Para fornecer o serviço de administração da Conta, é necessária a coleta de dados em relação aos dispositivos gerenciados junto com as informações de administração (doravante os “Dados”). Dados são fornecidos a Você pela ESET apenas para os fins do fornecimento de serviço de administração da Conta. Os Dados serão processados e armazenados de acordo com as políticas e práticas de segurança da ESET, assim como de acordo com a Política de Privacidade.

Detalhes sobre a privacidade, proteção de dados pessoais e direitos como sujeito de dados podem ser encontrados na Política de Privacidade.

Política de Uso Justo

Você é obrigado a cumprir com as limitações técnicas estipuladas na documentação. Você concorda que Você somente usará a Conta e suas funções de uma forma que não limite as possibilidades de outros Usuários acessarem esses serviços. O Provedor reserva o direito de limitar o escopo de serviços oferecidos para os Usuários individuais, para habilitar o uso de serviços pelo número mais alto possível de Usuários. A limitação do escopo de serviços também deve significar a eliminação total da possibilidade de usar qualquer uma das funções da Conta e exclusão dos Dados e informação.

Detalhes sobre limitações técnicas podem ser encontrados em Limitações.

Localização

O Provedor pode permitir que você escolha entre os locais de hospedagem disponíveis para a Conta, incluindo a localização recomendada escolhida pelo Provedor. Você reconhece que, ao escolher outro local que não o

recomendado, sua experiência de usuário pode ser afetada. Com base no local escolhido, poderão ser aplicáveis o Contrato de Proteção de Dados incluído no Anexo nº. 2 desse Contrato e as Cláusulas Contratuais Padrão incluídas no Anexo nº. 3 desse Contrato. A ESET reserva-se o direito de alterar um local específico a qualquer momento, sem aviso prévio, com o objetivo de aprimorar os serviços prestados pela ESET, em conformidade com Suas preferências de local (por exemplo, União Europeia).

Software

A ESET ou seus respectivos fornecedores possuem ou podem exercer direitos autorais em todos os softwares disponíveis como parte do Produto (doravante denominados "Software"). O Software pode ser usado somente de acordo com o Acordo de licença do Usuário Final incluído no Anexo nº. 1 deste Contrato. Outras informações sobre licenças, direitos autorais, documentação e marcas registradas estão estipuladas no Informações legais.

Restrições

Você não pode copiar, distribuir, extrair componentes ou produzir trabalhos derivativos da Conta. Ao usar a Conta, Você é obrigado a cumprir as seguintes restrições:

(a) Você não pode usar, modificar, traduzir ou reproduzir a Conta ou transferir direitos para uso da Conta ou seus componentes de qualquer forma que não conforme expressamente fornecido nestes Termos.

(b) Você não pode vender, sublicenciar, arrendar ou alugar ou emprestar a Conta ou usar a Conta para a prestação de serviços comerciais.

(c) Você não pode fazer engenharia reversa, reverter a compilação ou desmontar a Conta ou tentar descobrir de outra maneira o código fonte da Conta, exceto na medida em que essa restrição for expressamente proibida por lei.

(d) Você concorda que Você usará a Conta somente de uma maneira que esteja de acordo com todas as leis aplicáveis na jurisdição em que Você usa a Conta, incluindo sem limitação, restrições aplicáveis relacionadas a direitos autorais e a outros direitos de propriedade intelectual.

Aviso de isenção de responsabilidade

COMO O USUÁRIO, VOCÊ RECONHECE QUE A CONTA, ASSIM COMO OS SERVIÇOS, SÃO FORNECIDOS "NA CONDIÇÃO EM QUE SE ENCONTRAM", SEM UMA GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, E NA EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL. O PROVEDOR, NEM OS LICENCIADORES NEM OS AFILIADOS NEM OS DETENTORES DOS DIREITOS AUTORAIS FAZEM QUALQUER TIPO DE REPRESENTAÇÕES OU GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE OU QUE A CONTA OU SERVIÇO NÃO INFRINGIRÁ QUAISQUER PATENTES DE TERCEIROS, DIREITOS AUTORAIS, MARCAS COMERCIAIS OU OUTROS DIREITOS. NÃO HÁ GARANTIA DO PROVEDOR OU QUALQUER OUTRA PARTE DE QUE A CONTA OU OS SERVIÇOS ATENDERÃO SEUS REQUISITOS OU QUE A OPERAÇÃO DA CONTA OU DOS SERVIÇOS NÃO SERÁ INTERROMPIDA E NÃO TERÁ ERROS. VOCÊ ASSUME TOTAL RESPONSABILIDADE E RISCO PELA SELEÇÃO E USO DA CONTA E DOS SERVIÇOS PARA ATINGIR OS RESULTADOS PRETENDIDOS E OBTIDOS A PARTIR DELA.

Estes Termos não criam obrigações por parte do Provedor e de seus licenciadores diferentes daquelas especificamente definidas neste documento.

Limitação de Responsabilidade

ATÉ A EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, EM NENHUMA HIPÓTESE, O PROVEDOR, SEUS FUNCIONÁRIOS OU CONTRATADOS DEVERÃO SER CONSIDERADOS RESPONSÁVEIS POR QUALQUER PERDA DE LUCROS, RECEITA, VENDAS, DADOS OU CUSTOS DE AQUISIÇÃO DE BENS OU SERVIÇOS, DANOS MATERIAIS, DANOS PESSOAIS, INTERRUPÇÃO NOS NEGÓCIOS, PERDA DE INFORMAÇÕES COMERCIAIS OU POR QUAISQUER DANOS DIRETOS, INDIRETOS, ACIDENTAIS, ECONÔMICOS, DE COBERTURA, PUNITIVOS, ESPECIAIS OU SUBSEQUENTES, MAS CAUSADOS POR E DECORRENTES DO CONTRATO, DANOS, NEGLIGÊNCIA OU OUTRA TEORIA DE RESPONSABILIDADE, DECORRENTE DO USO OU DA INCAPACIDADE DE USAR A CONTA, MESMO QUE O PROVEDOR, SEUS CONTRATADOS OU AFILIADOS SEJAM AVISADOS DA POSSIBILIDADE DE TAIS DANOS. COMO ALGUNS PAÍSES E JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO DA RESPONSABILIDADE, MAS PODEM PERMITIR A SUA LIMITAÇÃO, A RESPONSABILIDADE DO PROVEDOR, SEUS FUNCIONÁRIOS, CONTRATADOS OU AFILIADOS, NESSES CASOS, DEVERÁ ESTAR LIMITADA À SOMA QUE VOCÊ PAGOU PELO SERVIÇO OU CONTA EM QUESTÃO.

Conformidade com o controle comercial

(a) Você não vai, direta ou indiretamente, exportar, reexportar, transferir ou disponibilizar o Software a qualquer pessoa, nem utilizá-lo de qualquer maneira ou estar envolvido em qualquer ação que possa resultar na ESET ou em suas empresas proprietárias, subsidiárias e as subsidiárias de qualquer uma de suas proprietárias, bem como entidades controladas por suas proprietárias ("Filiais"), violando ou sujeitas a consequências negativas sob as Leis de Controle Comercial, que incluem:

i. quaisquer leis que controlem, restrinjam ou imponham requisitos de licenciamento para a exportação, reexportação ou transferência de bens, software, tecnologia ou serviços, emitidos ou adotados por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Cingapura, Reino Unido, União Europeia ou qualquer um de seus Estados-Membros ou qualquer país no qual as obrigações sob esses Termos sejam executadas, ou no qual a ESET ou qualquer uma de suas Filiais seja incorporada ou onde opere e

ii. quaisquer sanções, restrições, embargos econômicos, financeiros, comerciais ou outros, proibição de importação ou exportação, proibição da transferência de fundos ou ativos ou da realização de serviços, ou medidas equivalentes impostas por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Cingapura, Reino Unido, União Europeia ou qualquer um de seus Estados Membros, ou qualquer país no qual as obrigações sob esses Termos sejam executadas, ou no qual a ESET ou qualquer uma de suas Filiais seja incorporada ou onde opere (os atos legais mencionados nos pontos i e ii. acima, juntos, como "Leis de Controle Comercial").

(b) A ESET terá o direito de suspender suas obrigações sob, ou rescindir, esses Termos com efeito imediato no caso de:

i. A ESET determinar que, em sua opinião razoável, o Usuário infringiu ou provavelmente vai infringir a disposição da seção (a) desta cláusula de Conformidade com o controle comercial desses Termos; ou

ii. o Usuário Final e/ou o Software se tornar sujeito às Leis de Controle Comercial e, como resultado, a ESET determinar que, em sua opinião razoável, o desempenho contínuo de suas obrigações sob esses Termos poderia resultar na ESET ou suas Filiais violarem, ou estarem sujeitas a consequências negativas sob, as Leis de Controle Comercial.

(c) Nada nesses Termos tem a intenção de, e nada deve ser interpretado ou construído, para induzir ou requerer que qualquer uma das partes aja ou não aja (ou concorde em agir ou não agir) de qualquer maneira que não seja consistente com, que seja penalizada por ou proibida sob qualquer Lei de Controle Comercial aplicável.

Legislação governante e idioma

Esses Termos serão governados por e construídos de acordo com a legislação eslovaca. O Usuário Final e o Provedor concordam que as disposições conflitantes da legislação reguladora e a Convenção das Nações Unidas sobre Contratos de Venda Internacional de Bens não deverão se aplicar a este Contrato. Se Você é um consumidor com residência habitual na UE, Você também tem proteção adicional concedida a Você pelas disposições obrigatórias da lei aplicável em seu país de residência.

Você concorda expressamente que a jurisdição exclusiva para qualquer reivindicação ou disputa com o Provedor ou relacionada de qualquer forma ao seu uso do Software, da Conta ou dos Serviços ou que surja desses Termos ou Termos Especiais (se aplicável) reside no Tribunal Regional de Bratislava I, Eslováquia, e você também concorda e consente expressamente com o exercício da jurisdição pessoal no Tribunal Regional de Bratislava I em conexão com tal disputa ou reivindicação. Se Você é um consumidor e tem residência habitual na UE, Você também pode fazer uma reivindicação para aplicar seus direitos de consumidor no lugar de jurisdição exclusiva ou no país da UE em que Você vive. Além disso, Você também pode usar uma plataforma de solução de disputas on-line, que pode ser acessada aqui: https://ec.europa.eu/consumers/odr/. Porém, considere entrar em contato conosco primeiro antes de criar qualquer reivindicação oficialmente.

Se ocorrer qualquer discrepância entre as versões de idiomas destes Termos, a versão em inglês disponível aqui deverá sempre prevalecer.

Disposições gerais

A ESET reserva o direito de revisar estes Termos e documentação ou qualquer parte deles, a qualquer momento atualizando o documento relevante para refletir alterações na legislação ou alterações na Conta. Você será notificado sobre qualquer revisão desses Termos através da sua Conta. Se você não concordar com as alterações destes Termos, você pode cancelar sua Conta. A menos que Você cancele sua Conta depois de ser notificado sobre as mudanças, Você estará vinculado a quaisquer aditamentos ou revisões desses Termos. Você é incentivado a visitar periodicamente esta página para verificar os Termos atualizado que se aplicam ao seu uso da Conta.

Avisos

Todos os avisos devem ser entregues a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Anexo nº. 1

Acordo de Licença do Usuário Final

Anexo nº. 2

Contrato de processamento de dados

Anexo nº. 3

Cláusulas contratuais padrão

Acordo de licença de usuário final

IMPORTANTE: leia atentamente os termos e as condições relativos ao produto estabelecidos a seguir antes do download, da instalação, da cópia ou do uso. **POR MEIO DO DOWNLOAD, DA INSTALAÇÃO, DA CÓPIA OU DO USO DO SOFTWARE, VOCÊ EXPRESSA SEU CONSENTIMENTO COM ESTES TERMOS E CONDIÇÕES E RECONHECE A POLÍTICA DE PRIVACIDADE.**

Acordo de Licença do Usuário Final

Sob os termos deste Contrato de licença para o usuário final (doravante denominado “Contrato”) executado por e entre a ESET, spol. s r. o., tendo sua sede em Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada no Registro Comercial do Tribunal Regional de Bratislava I, Seção Sro, Nº de entrada 3586/B, Número de registro da empresa: 31333532 (doravante denominada "ESET" ou “Provedor”) e Você, uma pessoa física ou jurídica (doravante denominada “Você” ou “Usuário final”), recebe o direito de uso do Software definido no Artigo 1 deste Contrato. O Software definido no Artigo 1 deste Contrato pode ser armazenado em um carregador de dados, enviado por e-mail, obtido por download da Internet, obtido por download de servidores do Provedor ou obtido de outras fontes, sujeito aos termos e às condições especificados a seguir.

ESTE É UM CONTRATO SOBRE DIREITOS DO USUÁRIO FINAL E NÃO UM CONTRATO DE VENDA. O Provedor permanece o proprietário da cópia de Software e da mídia física fornecida na embalagem comercial e de todas as outras cópias a que o Usuário final tiver direito nos termos deste Contrato.

Ao clicar na opção “Eu aceito” ou “Eu aceito...” durante a instalação, download, cópia ou uso do Software, Você concorda com os termos e condições deste Contrato. Se Você não concordar com os termos e as condições deste Contrato, clique imediatamente na opção para cancelar, cancele a instalação ou o download, ou destrua ou devolva o Software, a mídia de instalação, a documentação que vem com o produto e o recibo de vendas para a ESET ou a loja onde Você adquiriu o Software.

VOCÊ CONCORDA QUE SEU USO DO SOFTWARE CONFIRMA QUE VOCÊ LEU ESTE CONTRATO, QUE O COMPREENDEU E CONCORDA EM ESTAR VINCULADO A ELE POR MEIO DE SEUS TERMOS E CONDIÇÕES.

1. **Software.** Conforme usado neste Contrato, o termo "Software" significa: (i) o programa de computador acompanhado por este Contrato e todos os seus componentes; (ii) todos os conteúdos de discos, CD-ROMs, DVDs, e-mails e anexos, ou outras mídias nas quais este Contrato é fornecido, inclusive o formulário de código de objeto do Software fornecido no transportador de dados, através de correio eletrônico ou baixado na Internet; (iii) qualquer material explicativo por escrito relacionado e qualquer outra documentação possível em relação ao Software, sobretudo qualquer descrição do Software, suas especificações, qualquer descrição das propriedades ou operação do Software, qualquer descrição do ambiente operacional no qual o Software é usado, instruções para o uso ou instalação do Software ou qualquer descrição sobre como usar o Software (doravante chamado de "Documentação"); (iv) cópias do Software, patches para possíveis erros no Software, adições ao Software, extensões ao Software, versões modificadas do Software e atualizações de componentes do Software se houverem, são licenciadas a Você pelo Provedor de acordo com o Artigo 3 deste Contrato. O Software será fornecido exclusivamente na forma de código de objeto executável.

2. **Instalação, Computador e uma Chave de Licença**. O Software fornecido em um carregador de dados, enviado por email eletrônico, obtido por download da Internet, obtido por download de servidores do Provedor ou obtido de outras fontes requer instalação. Você deve instalar o Software em um Computador configurado corretamente que, pelo menos, esteja de acordo com os requisitos definidos na Documentação. A metodologia de instalação é descrita na Documentação. Nenhum computador ou hardware que possa ter um efeito adverso no Software pode ser instalado no Computador no qual Você instalar o Software. Computer significa hardware, incluindo sem limitação computadores pessoais, notebooks, estações de trabalho, computadores tipo palmtop, smartphones,

dispositivos eletrônicos manuais ou outros dispositivos eletrônicos para os quais o Software foi projetado, no qual ele será instalado e/ou usado. Chave de licença significa a sequência exclusiva de símbolos, letras, números ou sinais especiais fornecidos ao Usuário Final para permitir o uso legal do Software, sua versão específica ou extensão do termo da Licença em conformidade com esse Contrato.

3. **Licença**. Desde que Você tenha concordado com os termos deste Contrato e cumprido com todos os termos e condições estabelecidos neste documento, o Provedor deverá conceder a Você os seguintes direitos (doravante denominado "Licença"):

a) **Instalação e uso.** Você deverá ter o direito não exclusivo e não transferível para instalar o Software no disco rígido de um computador ou outra mídia permanente para armazenamento dos dados, instalação e armazenamento do Software na memória de um sistema computacional e para implementar, armazenar e exibir o Software.

b) **Estipulação do número de licenças.** O direito de utilizar o Software deverá estar vinculado ao número de Usuários finais. Um Usuário final deverá ser selecionado para referir-se ao seguinte: (i) instalação do Software em um sistema computacional; ou (ii) se a extensão de uma licença estiver vinculada ao número de caixas de email, então um Usuário final deverá ser selecionado para referir-se a um usuário de computador que aceita e-mail através de um Agente de usuário de email (doravante denominado “MUA”). Se um MUA aceitar e-mail e, subsequentemente, distribuí-lo de forma automática a vários usuários, então o número de Usuários finais deverá ser determinado de acordo com o número real de usuários para os quais o e-mail será distribuído. Se um servidor de email executar a função de um portal de email, o número de Usuários finais deverá ser igual ao número de servidores de email para o qual esse portal oferece serviços. Se um número não especificado de endereços de emails eletrônicos for direcionado para um usuário e aceito por ele (por exemplo, por meio de alias) e as mensagens não forem automaticamente distribuídas pelo cliente para um número maior de usuários, uma licença para um computador será exigida. Você não deve usar a mesma Licença ao mesmo tempo em mais de um computador. O Usuário Final tem o direito de inserir a Chave de Licença para o Software apenas até a extensão em que ela tem o direito de usar o Software de acordo com a limitação criada pelo número de Licenças oferecido pelo Provedor. A Chave de licença é considerada confidencial, Você não deve compartilhar a Licença com terceiros ou permitir que terceiros usem a Chave de licença a menos que isso seja permitido por esse Contrato ou pelo Provedor. Se sua Chave de licença for comprometida, notifique o Provedor imediatamente.

c) **Business Edition.** Uma versão Business Edition do Software deve ser obtida para usar o Software em servidores de email, relés de correio, gateways de correio ou gateways de Internet.

d) **Vigência da licença**. O direito de utilizar o Software deverá estar limitado a um período.

e) **Software OEM**. O Software OEM deve estar limitado ao Computador com o qual Você obteve o software. Ele não pode ser transferido para um computador diferente.

f) **Software NFR, AVALIAÇÃO**. Software classificado como "Não para revenda", NFR ou AVALIAÇÃO não pode ser atribuído para pagamento e deve ser usado apenas para demonstração ou teste dos recursos do Software.

g) **Término da licença**. A Licença deverá terminar automaticamente no final do período para o qual ela foi concedida. Se Você deixar de cumprir qualquer das cláusulas deste Contrato, o Provedor terá o direito de retirar-se do Contrato, sem prejuízo de qualquer direito ou solução jurídica abertos ao Provedor em tais eventualidades. No caso de cancelamento da Licença, Você deve excluir, destruir ou devolver imediatamente, às suas custas, o Software e todas as cópias de backup para a ESET ou loja em que Você obteve o Software. Mediante a rescisão da Licença o Provedor também estará autorizado a cancelar o direito do Usuário Final de usar as funções do Software que exigem conexão aos servidores do Provedor ou servidores de terceiros.

4.**Funções com coleta de dados e requisitos de conexão com a internet**. Para operar corretamente, o Software

exige conexão com a Internet e deve conectar-se em intervalos regulares aos servidores do Provedor ou a servidores de terceiros e a coleta de dados aplicáveis de acordo com a Política de Privacidade. A conexão com a Internet e coleta de dados aplicáveis é necessária para os seguintes recursos do Software:

a) **Atualizações para o Software.** O Provedor deverá emitir, de vez em quando, atualizações para o Software ("Atualizações"), mas não deverá ser obrigado a fornecer Atualizações. Esta função está ativada nas configurações padrão do Software, e as Atualizações são, portanto, instaladas automaticamente, a menos que o Usuário Final tenha desativado a instalação automática das Atualizações. Para o fornecimento de Atualizações, a verificação de autenticidade da Licença é necessária incluindo informações sobre o Computador e/ou a plataforma na qual o Software está instalado de acordo com a Política de Privacidade.

b) Encaminhamento de infiltrações e informações ao Provedor. O Software contém funções que coletam amostras de vírus de computador e outros programas maliciosos de computador e objetos suspeitos, problemáticos, potencialmente indesejados ou potencialmente inseguros como arquivos, URLs, pacotes de IP e quadros de ethernet (doravante as “Infiltrações”) e então envia-os ao Provedor, incluindo mas não limitado a informações sobre o processo de instalação, o Computador e/ou a plataforma na qual o Software está instalado, e informações sobre as operações e funcionalidades do Software (doravante as “Informações”). As Informações e Infiltrações podem conter dados (inclusive dados pessoais obtidos de forma aleatória ou acidental) sobre o Usuário Final ou outros usuários do computador no qual o Software está instalado, e arquivos afetados por Infiltrações com os metadados associados. Informação e Infiltrações podem ser coletadas pela funções de Software a seguir:

i. A função do Sistema de Reputação LiveGrid inclui a coleta e envio de hashes unidirecionais relacionadas a Infiltrações para o Provedor. Esta função é ativada nas configurações padrão do software.

ii. A função do Sistema de Feedback LiveGrid inclui a coleta e envio de Infiltrações com metadados e Informação associados para o Provedor.

O Provedor deverá usar apenas as Informações e Infiltrações recebidas para o objetivo de análise e pesquisa de infiltrações, melhoria de Software e verificação de autenticidade da Licença, e deverá tomar as medidas adequadas para garantir que as Infiltrações e Informações recebidas permaneçam seguras. Ao ativar esta função do Software, Infiltrações e Informações podem ser coletadas e processadas pelo Provedor como especificado na Política de Privacidade e de acordo com os regulamentos legais relevantes. Estas funções podem ser desativadas a qualquer momento.

Para os fins desse Contrato é necessário coletar, processar e armazenar dados permitindo ao Provedor identificar Você de acordo com a Política de Privacidade. Você doravante reconhece que o Provedor verifica usando seus próprios meios se Você está usando o Software de acordo com as cláusulas deste Contrato. Você doravante reconhece que, para os fins deste Contrato, é necessário que seus dados sejam transferidos durante a comunicação entre o Software e os sistemas computacionais do Provedor ou de seus parceiros comerciais como parte da rede de distribuição e suporte do Provedor para garantir a funcionalidade do Software e a autorização para usar o Software e para a proteção dos direitos do Provedor.

Seguindo a conclusão deste Contrato, o Provedor ou qualquer de seus parceiros comerciais como parte da rede de distribuição e suporte do Provedor terão o direito de transferir, processar e armazenar dados essenciais que identifiquem Você, para fins de faturamento, execução deste Contrato e transmissão de notificações no seu Computador. Você concorda em receber notificações e mensagens em relação ao produto incluindo mas não limitado a informações de marketing.

Detalhes sobre privacidade, proteção de dados pessoais e seus direitos como um assunto de dados podem ser encontrados na Política de Privacidade, que está disponível no site do Provedor e pode ser acessada diretamente a partir do processo de instalação. Você também pode visitar a seção de ajuda do Software.

5. **Exercício dos direitos do Usuário final**. Você deve exercer os direitos do Usuário final em pessoa ou por meio de seus funcionários. Você somente pode usar o Software para garantir suas operações e proteger esses Computadores ou sistemas computacionais para os quais Você tiver obtido uma Licença.

6. **Restrições aos direitos.** Você não pode copiar, distribuir, extrair componentes ou produzir trabalhos derivativos do Software. Ao usar o Software, Você é obrigado a cumprir as seguintes restrições:

a) Você pode fazer uma cópia do Software em uma mídia para armazenamento permanente como uma cópia de backup de arquivos, desde que a sua cópia de backup de arquivos não seja instalada ou usada em qualquer computador. Quaisquer outras cópias que Você fizer do Software constituirá uma violação deste Contrato.

b) Você não pode usar, modificar, traduzir ou reproduzir o Software ou transferir direitos para uso do Software nem cópias do Software de qualquer forma que não conforme expressamente fornecido neste Contrato.

c) Você não pode vender, sublicenciar, arrendar ou alugar ou emprestar o Software ou usar o Software para a prestação de serviços comerciais.

d) Você não pode fazer engenharia reversa, reverter a compilação ou desmontar o Software ou tentar descobrir de outra maneira o código fonte do Software, exceto na medida em que essa restrição for expressamente proibida por lei.

e) Você concorda que Você usará o Software somente de uma maneira que esteja de acordo com todas as leis aplicáveis na jurisdição em que Você usa o Software, incluindo sem limitação, restrições aplicáveis relacionadas a direitos autorais e a outros direitos de propriedade intelectual.

f) Você concorda que Você somente usará o Software e suas funções de uma forma que não limite as possibilidades de outros Usuários Finais acessarem esses serviços. O Provedor reserva o direito de limitar o escopo de serviços oferecidos para os usuários finais individuais, para habilitar o uso de serviços pelo número mais alto possível de Usuários Finais. A limitação do escopo de serviços também deve significar a eliminação total da possibilidade de usar qualquer uma das funções do Software e exclusão dos Dados e informação sobre os servidores do Provedor ou servidores de terceiro relacionados a uma função específica do Software.

g) Você concorda em não exercer nenhuma atividade que envolva o uso da Chave de licença que seja contrária aos termos desse Contrato ou que cause o fornecimento da Chave de licença para qualquer pessoa que não tenha o direito de usar o Software, como a transferência de Chaves de licença usadas ou não usadas de qualquer forma, assim como a reprodução ou distribuição não autorizada de Chaves de licença duplicadas ou geradas ou o uso do Software como resultado do uso de uma Chave de licença obtida de uma origem que não sejam o Provedor.

7. **Direitos autorais**. O Software e todos os direitos, incluindo, sem limitação, direitos de propriedade e direitos de propriedade intelectual, mencionados neste documento são de propriedade da ESET e/ou seus licenciadores. Eles estão protegidos pelas cláusulas de tratados internacionais e por todas as outras leis aplicáveis do país no qual o Software está sendo utilizado. A estrutura, a organização e o código do Software são segredos comerciais valiosos e informações confidenciais da ESET e/ou de seus licenciadores. Você não deve copiar o Software, exceto conforme especificado no Artigo 6(a). Quaisquer cópias que Você tiver permissão para fazer de acordo com este Contrato devem conter os mesmos avisos de direitos autorais e de propriedade que aparecerem no Software. Se Você fizer engenharia reversa, reverter a compilação, desmontar ou tentar descobrir de outra maneira o código fonte do Software, em violação das cláusulas deste Contrato, Você concorda que quaisquer informações relacionadas obtidas deverão automática e irrevogavelmente ser consideradas transferidas ao Provedor e de propriedade do Provedor em sua totalidade a partir do momento em que essas informações existirem, não obstante os direitos do Provedor em relação à violação deste Contrato.

8. **Reserva de direitos**. O Provedor reserva todos os direitos ao Software, com exceção dos direitos expressamente concedidos, nos termos deste Contrato, a Você como o Usuário final do Software.

9. **Versões em diversos idiomas, software de mídia dupla, várias cópias**. No caso de o Software suportar diversas plataformas ou idiomas ou se Você receber diversas cópias do Software, Você poderá usar o Software apenas para o número de sistemas computacionais e para as versões para as quais Você obteve uma Licença. Você não pode vender, alugar, arrendar, sublicenciar, emprestar ou transferir versões ou cópias do Software que Você não usar.

10. **Início e término do Contrato**. Este Contrato é vigente a partir da data em que Você concordar com os termos deste Contrato. Você pode terminar este Contrato a qualquer momento ao desinstalar, destruir e devolver definitivamente, às suas custas, o Software, todas as cópias de backup e todos os materiais relacionados fornecidos pelo Provedor ou pelos seus parceiros comerciais. Independentemente do modo de término deste Contrato, as cláusulas dos Artigos 7, 8, 11, 13, 19 e 21 deverão continuar a ser aplicadas por um tempo ilimitado.

11. **DECLARAÇÕES DO USUÁRIO FINAL**. COMO O USUÁRIO FINAL, VOCÊ RECONHECE QUE O SOFTWARE É FORNECIDO "NA CONDIÇÃO EM QUE ENCONTRA", SEM UMA GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, E NA EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL. O PROVEDOR, NEM OS LICENCIADORES NEM OS AFILIADOS NEM OS DETENTORES DOS DIREITOS AUTORAIS FAZEM QUALQUER TIPO DE REPRESENTAÇÕES OU GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE OU QUE O SOFTWARE NÃO INFRINGIRÁ QUAISQUER PATENTES DE TERCEIROS, DIREITOS AUTORAIS, MARCAS COMERCIAIS OU OUTROS DIREITOS. NÃO HÁ GARANTIA DO PROVEDOR OU QUALQUER OUTRA PARTE DE QUE AS FUNÇÕES CONTIDAS NO SOFTWARE ATENDERÃO SEUS REQUISITOS OU QUE A OPERAÇÃO DO SOFTWARE NÃO SERÁ INTERROMPIDA E NÃO TERÁ ERROS. VOCÊ ASSUME TOTAL RESPONSABILIDADE E RISCO PELA SELEÇÃO DO SOFTWARE PARA ATINGIR OS RESULTADOS PRETENDIDOS E PARA A INSTALAÇÃO, USO E RESULTADOS OBTIDOS A PARTIR DELE.

12. **Não há outras obrigações**. Este Contrato não cria obrigações por parte do Provedor e de seus licenciadores diferentes daquelas especificamente definidas neste documento.

13. **LIMITAÇÃO DE RESPONSABILIDADE**. ATÉ A EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, EM NENHUMA HIPÓTESE, O PROVEDOR, SEUS FUNCIONÁRIOS OU LICENCIADORES DEVERÃO SER CONSIDERADOS RESPONSÁVEIS POR QUALQUER PERDA DE LUCROS, RECEITA, VENDAS, DADOS OU CUSTOS DE AQUISIÇÃO DE BENS OU SERVIÇOS, DANOS MATERIAIS, DANOS PESSOAIS, INTERRUPÇÃO NOS NEGÓCIOS, PERDA DE INFORMAÇÕES COMERCIAIS OU POR QUAISQUER DANOS DIRETOS, INDIRETOS, ACIDENTAIS, ECONÔMICOS, DE COBERTURA, PUNITIVOS, ESPECIAIS OU SUBSEQUENTES, MAS CAUSADOS POR E DECORRENTES DO CONTRATO, DANOS, NEGLIGÊNCIA OU OUTRA TEORIA DE RESPONSABILIDADE, DECORRENTE DO USO OU DA INCAPACIDADE DE USAR O SOFTWARE, MESMO QUE O PROVEDOR OU SEUS LICENCIADORES OU AFILIADOS SEJAM AVISADOS DA POSSIBILIDADE DE TAIS DANOS. COMO ALGUNS PAÍSES E JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO DA RESPONSABILIDADE, MAS PODEM PERMITIR A SUA LIMITAÇÃO, A RESPONSABILIDADE DO PROVEDOR, SEUS FUNCIONÁRIOS OU LICENCIADORES OU AFILIADOS, NESSES CASOS, DEVERÁ ESTAR LIMITADA À SOMA QUE VOCÊ PAGOU PELA LICENÇA.

14. Nada contido neste Contrato deverá prejudicar os direitos legais de qualquer parte que atua como um consumidor se estiver executando o contrariem.

15. **Suporte técnico**. A ESET ou terceiros comissionados pela ESET deverão fornecer suporte técnico a seu critério, sem quaisquer garantias ou declarações. O Usuário final deverá ser solicitado a fazer backup de todos os dados, software e recursos de programa existentes antes do fornecimento de suporte técnico. A ESET e/ou terceiros comissionados pela ESET não pode aceitar responsabilidade por danos ou perda de dados, de propriedade, de software ou hardware ou perda de lucros devido ao fornecimento de suporte técnico. A ESET e/ou terceiros comissionados pela ESET reserva-se o direito de decidir que a solução do problema está além do escopo de suporte técnico. A ESET reserva-se o direito de recusar, suspender ou terminar o fornecimento de suporte técnico a seu critério. Informações de licença, Informações e outros dados em conformidade com a Política de

Privacidade podem ser necessários para o fornecimento de suporte técnico.

16. **Transferência da licença**. O Software pode ser transferido de um sistema computacional para outro, a não ser que seja contrário aos termos do Contrato. Se não for contrário aos termos do Contrato, o Usuário Final somente será autorizado a transferir permanentemente a Licença e todos os direitos decorrentes deste Contrato para outro Usuário final com o consentimento do Provedor, desde que (i) o Usuário final original não retenha nenhuma cópia do Software, (ii) a transferência de direitos seja direta, ou seja, do Usuário final original para o novo Usuário final; (iii) o novo Usuário final tenha assumido todos os direitos e obrigações incumbidos ao Usuário final original, nos termos deste Contrato; (iv) o Usuário final original tenha fornecido ao novo Usuário final a documentação que permite a verificação da autenticidade do Software, como especificado no Artigo 17.

17. **Verificação da autenticidade do Software**. O Usuário final pode demonstrar direito de usar o Software em uma das seguintes formas: (i) por meio de um certificado de licença emitido pelo Provedor ou por um terceiro indicado pelo Provedor, (ii) por meio de um acordo de licença por escrito, se tal acordo foi concluído, (iii) por meio do envio de um email enviado para o Provedor contendo detalhes do licenciamento (nome de usuário e senha). Informações de licença e dados de identificação do Usuário Final em conformidade com a Política de Privacidade podem ser necessários para a verificação de legitimidade do Software.

18. **Licenciamento para as autoridades públicas e para o governo dos EUA**. O Software deve ser fornecido às autoridades públicas, incluindo o governo dos Estados Unidos com os direitos de licença e as restrições descritas neste Contrato.

19. **Conformidade com o controle comercial**.

a) Você não vai, direta ou indiretamente, exportar, reexportar, transferir ou disponibilizar o Software a qualquer pessoa, nem utilizá-lo de qualquer maneira ou estar envolvido em qualquer ação que possa resultar na ESET ou em suas empresas proprietárias, subsidiárias e as subsidiárias de qualquer uma de suas proprietárias, bem como entidades controladas por suas proprietárias (doravante as "Filiais"), violando ou sujeitas a consequências negativas sob as Leis de Controle Comercial, que incluem

i. quaisquer leis que controlem, restrinjam ou imponham requisitos de licenciamento para a exportação, reexportação ou transferência de bens, software, tecnologia ou serviços, emitidos ou adotados por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Cingapura, Reino Unido, União Europeia ou qualquer um de seus Estados-Membros ou qualquer país no qual as obrigações sob o Contrato sejam executadas, ou no qual a ESET ou qualquer uma de suas Filiais seja incorporada ou onde opere (doravante "Leis de Controle de Exportação") e

ii. quaisquer sanções, restrições, embargos econômicos, financeiros, comerciais ou outros, proibição de importação ou exportação, proibição da transferência de fundos ou ativos ou da realização de serviços, ou medidas equivalentes importas por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Cingapura, Reino Unido, União Europeia ou qualquer um de seus Estados Membros, ou qualquer país no qual as obrigações sob o Contrato sejam executadas, ou no qual a ESET ou qualquer uma de suas Filiais seja incorporada ou onde opere (doravante "Leis de Sanção").

b) A ESET terá o direito de suspender suas obrigações sob, ou rescindir, esses Termos com efeito imediato no caso de:

i. A ESET determinar que, em sua opinião razoável, o Usuário infringiu ou provavelmente vai infringir a disposição do Artigo 19.a do Contrato; ou

ii. o Usuário Final e/ou o Software se tornar sujeito às Leis de Controle Comercial e, como resultado, a ESET determinar que, em sua opinião razoável, o desempenho contínuo de suas obrigações sob o Contrato poderia resultar na ESET ou suas Filiais violarem, ou estarem sujeitas a consequências negativas sob, as Leis de Controle

Comercial.

c) Nada no Contrato tem a intenção de, e nada deve ser interpretado ou construído, para induzir ou requerer que qualquer uma das partes aja ou não aja (ou concorde em agir ou não agir) de qualquer maneira que não seja consistente com, que seja penalizada por ou proibida sob qualquer Lei de Controle Comercial aplicável.

20. **Avisos**. Todos os avisos e a devolução do Software e a Documentação devem ser entregues a: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Legislação aplicável**. Este Contrato deverá ser interpretado e regido segundo as leis da República Eslovaca. O Usuário final e o Provedor concordam que os princípios do conflito da legislação e a Convenção das Nações Unidas sobre Contratos de Venda Internacional de Bens não se aplicam a este Contrato. Você concorda expressamente que quaisquer disputas ou reclamações decorrentes deste Contrato com relação ao Provedor ou quaisquer disputas ou reivindicações relativas ao uso do Software serão resolvidos pelo Tribunal Regional de Bratislava I e Você concorda expressamente com o referido tribunal que exerce a jurisdição.

22. **Disposições gerais**. Se uma ou mais cláusulas deste Contrato forem inválidas ou não aplicáveis, isso não deverá afetar a validade das outras cláusulas restantes do Contrato, que deverão permanecer válidas e vigentes de acordo com as condições estipuladas neste documento. No caso de discrepâncias entre as versões de idioma desse Contrato, a versão em inglês prevalecerá. Este Contrato só poderá ser modificado por escrito, assinado por um representante autorizado do Provedor ou uma pessoa expressamente autorizada a agir nessa capacidade, nos termos de uma procuração.

Este é todo o acordo entre o Provedor e Você em relação ao Software e anula qualquer declaração, discussão, acordo, comunicação ou propaganda anterior em relação ao Software.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

Em conformidade com os requisitos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/EC (referido doravante como "GDPR"), o Provedor (referido doravante como o "Processador") e Você (referido doravante como "Controlador") estão entrando no relacionamento contratual de processamento de dados para definir os termos e condições para o processamento de dados pessoais, a maneira de sua proteção, e também para definir outros direitos e obrigações de ambas as partes no processamento de dados pessoais de titulares de dados em nome do Controlador durante o curso da execução do objeto destes Termos como o contrato principal.

1. **Tratamento de dados pessoais.** Os serviços prestados em conformidade com estes Termos incluem o tratamento de informações relacionadas a uma pessoa física identificada ou identificável listada na Política de Privacidade (doravante os "Dados Pessoais").

2. **Autorização.** O Responsável pelo Tratamento autoriza o Subcontratante para processar Dados Pessoais, incluindo as instruções a seguir:

(i) "Finalidade do processamento" significa a prestação de serviços em conformidade com estes Termos. O Subcontratante só pode processar Dados Pessoais em nome do Responsável pelo Tratamento em relação à prestação de serviços solicitados pelo Responsável pelo Tratamento. Todas as informações coletadas para fins adicionais serão processadas fora da relação contratual Responsável pelo Tratamento-Subcontratante.

(ii) período de processamento significa o período iniciado quando se inicia a cooperação sob estes Termos e

terminando na rescisão dos serviços,

(iii) Escopo e Categorias de Dados pessoais. Os Serviços são pretendidos apenas para o tratamento de dados pessoais. Porém, o Responsável pelo Tratamento é o único responsável pela determinação do escopo de dados pessoais.

(iv) “Titular dos dados” significa a pessoa física como usuário autorizado dos dispositivos do Controlador,

(v) operações de processamento são todas e quaisquer operações necessárias para o processamento,

(vi) “Instruções documentadas” significa instruções descritas nestes Termos, seus Anexos, na Política de Privacidade e na documentação do serviço. O Responsável pelo Tratamento será responsável pela responsabilidade legal do processamento de Dados Pessoais pelo Subcontratante em relação às respectivas disposições aplicáveis da lei de proteção de dados.

3. **Obrigações do Subcontratante.** O Processador será obrigado a:

(i) processar Dados Pessoais apenas com base nas Instruções documentadas e para os fins definidos nos Termos, seus Anexos, na Política de Privacidade e na documentação de serviço,

(ii) instruir as pessoas autorizadas a processar os Dados Pessoais (doravante as "Pessoas Autorizadas") sobre seus direitos e deveres de acordo com o GDPR, sobre sua responsabilidade em caso de violação e garantir que as Pessoas Autorizadas comprometeram-se a manter a confidencialidade e a seguir as instruções Documentadas,

(iii) implementar e seguir as medidas descritas nos Termos, seus Anexos, na Política de Privacidade e na documentação de serviço,

(iv) auxiliar o Responsável pelo Tratamento a responder a solicitações dos Titulares dos Dados relacionadas aos seus direitos. O Subcontratante não deve corrigir, remover ou restringir o tratamento de Dados Pessoais sem as instruções do Responsável pelo Tratamento. Todas as solicitações do Titular dos Dados relacionadas a Dados Pessoais processados em nome do Responsável pelo Tratamento serão encaminhadas ao Responsável pelo Tratamento sem atraso.

(v) auxiliar o Responsável pelo Tratamento com a notificação de violação de dados pessoais à autoridade supervisora e ao Titular dos Dados, O Subcontratante notificará o Responsável pelo Tratamento sobre qualquer violação do processamento de dados pessoais ou da segurança dos dados pessoais imediatamente após tal descoberta. O Subcontratante deve cooperar de forma razoável em uma investigação e correção de tal violação e tomar medidas razoáveis para limitar outras implicações negativas.

(vi) por escolha do Responsável pelo Tratamento remover ou devolver todos os Dados Pessoais ao Responsável pelo Tratamento após o fim do Período de Tratamento. O Responsável pelo Tratamento se compromete a informar o Subcontratante sobre sua decisão no prazo de dez (10) dias após o término do Período de Processamento. Essa disposição não afetará o direito do Subcontratante de manter os Dados Pessoais na extensão necessária para fins de arquivamento no interesse público, fins de pesquisa científica, fins estatísticos ou para o estabelecimento, exercício ou defesa de reivindicações judiciais.

(vii) manter um registro atualizado de todas as categorias de atividades de processamento que ele realizou em nome do Controlador,

(viii) disponibilizar todas as informações necessárias para demonstrar conformidade como parte dos Termos, seus Anexos, da Política de Privacidade e da documentação de serviço disponíveis ao Responsável pelo Tratamento. No caso de auditoria ou controle do processamento de Dados Pessoais do lado do Responsável pelo Tratamento, o Responsável pelo Tratamento será obrigado a informar o Subcontratante por escrito pelo menos dez (30) dias antes da auditoria ou controle planejado.

4. **Contratação de outro Subcontratante.** O Subcontratante tem o direito de contratar outro subcontratante para realizar atividades de tratamento específicas, como o fornecimento de armazenamento em nuvem e infraestrutura para o serviço, em conformidade com estes Termos, seus Anexo, a Política de Privacidade e a documentação do serviço. Atualmente, a Microsoft fornece armazenamento em nuvem e infraestrutura como parte do Azure Cloud Service. Mesmo neste caso, o Processador permanecerá o único ponto de contato e a parte responsável pela conformidade. O Subcontratante se compromete a informar o Responsável pelo Tratamento sobre qualquer adição ou substituição de outro subcontratante para fins da possibilidade de contestar tal alteração.

5. **Território de processamento.** O Processador garante que o processamento ocorra no Espaço Econômico Europeu ou em um país designado como seguro por decisão da Comissão Europeia, com base na decisão do Controlador. As Cláusulas Contratuais Padrão serão aplicadas em caso de transferências e tratamentos localizados fora do Espaço Econômico Europeu ou de um país designado como seguro por decisão da Comissão Europeia, por solicitação do Responsável pelo Tratamento.

6. **Segurança.** O Processador é certificado pela ISO 27001:2013 e usa a estrutura da ISO 27001 para implementar uma estratégia de defesa de segurança em camadas ao aplicar controles de segurança na camada de rede, sistemas operacionais, bancos de dados, aplicativos, pessoal e processos operacionais. A conformidade com os requisitos regulatórios e contratuais é regularmente avaliada e revisada de maneira semelhante a outras infraestruturas e operações do Processador, e as medidas necessárias são realizadas continuamente para garantir a conformidade. O Subcontratante organizou a segurança de dados usando ISMS com base em ISO 27001. A documentação de segurança inclui principalmente documentos de política para segurança da informação, segurança física e segurança de equipamentos, gerenciamento de incidentes, tratamento de vazamentos de dados e incidentes de segurança, etc.

7. **Medidas Técnicas e Organizacionais**. O Subcontratante deve proteger os Dados Pessoais contra danos e destruição casuais e ilegais, perda casual, mudança, acesso não autorizado e divulgação. Para cumprir este objetivo, o Subcontratante deverá adotar as medidas técnicas e organizativas adequadas ao modo de tratamento e ao risco que representa o tratamento dos direitos dos Titulares dos Dados em conformidade com os requisitos do GDPR. Uma descrição detalhada das medidas técnicas e organizacionais consta da Política de Segurança.

8. **Informações de contato do Subcontratante.** Todas as notificações, solicitações, demandas e outras comunicações relacionadas à proteção de dados pessoais devem ser endereçadas à ESET, spol. s.r.o., aos cuidados de: 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.

Política de Privacidade

Em vigor a partir de 21º de março de 2023 | Ver uma versão anterior da Política de Privacidade | Comparar alterações

A proteção de dados pessoais é de importância particular para a ESET, spol. s r. o., com sede em Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada no Registro Comercial administrado pela Corte Distrital Bratislava I, Seção Sro, Registro Nº. 3586/B, Número de Registro Comercial: 31333532 como um Responsável pelo Tratamento de Dados ("ESET" ou "Nós"). Queremos cumprir com o requisito de transparência conforme legalmente protegido pelo Regulamento Geral de Proteção de Dados ("RGPD") da UE. Para isso, estamos publicando essa Política de Privacidade com o objetivo exclusivo de informar nosso cliente ("Usuário Final" ou "Você") como titular dos dados sobre os tópicos de dados pessoais a seguir:

- Base jurídica do tratamento de dados pessoais,
- Compartilhamento de dados e confidencialidade,
- Segurança de dados,
- Seus direitos como titular dos dados,
- Tratamento de seus Dados pessoais
- Informações de contato.

Base jurídica do tratamento de dados pessoais

Existem apenas algumas bases jurídicas para o tratamento de dados que Nós usamos de acordo com a estrutura legislativa aplicável relacionada à proteção de dados pessoais. O tratamento de dados pessoais na ESET é principalmente necessário para o desempenho do Termos de uso ("Termos") com o Usuário Final (Art. 6 (1) (b) LGPD), que é aplicável para o fornecimento de produtos ou serviços ESET, a menos que explicitamente declarado o contrário, por exemplo:

- Base jurídica de interesse legítimo (Art. 6 (1) (f) LGPD), que nos permite processar dados sobre como nossos clientes usam nossos Serviços e sua satisfação para fornecer aos nossos usuários a melhor proteção, suporte e experiência que podemos oferecer. Mesmo o marketing é reconhecido pela legislação aplicável como um interesse legítimo, portanto normalmente contamos com isso para a comunicação de marketing com nossos clientes.
- Consentimento (Art. 6 (1) (a) LGPD), que podemos solicitar de Você em situações específicas quando consideramos essa base jurídica como a mais adequada ou se for exigido por lei.

- Conformidade com obrigações legais (Art. 6 (1) (c) LGPD), por exemplo estipulando requisitos para comunicação eletrônica, retenção para faturamento ou documentos de cobrança.

Compartilhamento de dados e confidencialidade

Não compartilhamos seus dados com terceiros. Porém, a ESET é uma empresa que opera no mundo todo através de empresas afiliadas ou parceiros como parte de nossa rede de vendas, serviço e suporte. Informações de licenciamento, cobrança e suporte técnico processadas pela ESET podem ser transferidas de e para afiliadas ou parceiros com o objetivo de cumprir com o Acordo de Licença para o Usuário Final, como o fornecimento de serviços ou suporte.

A ESET prefere processar seus dados na União Europeia (UE). Porém, dependendo de sua localização (uso de nossos produtos e/ou serviços fora da UE) e/ou do serviço escolhido por você, pode ser necessário transferir seus dados para um país fora da UE. Por exemplo, usamos serviços de terceiros em conexão com a computação em nuvem. Nesses casos, selecionamos cuidadosamente nossos provedores de serviço e garantimos um nível apropriado de proteção de dados através de medidas contratuais, técnicas e organizacionais. Como regra, concordamos com as cláusulas contratuais padrão da UE, se necessário, com regulamentos contratuais suplementares.

Para alguns países fora da UE, como o Reino Unido e Suíça, a UE já determinou um nível de proteção de dados comparável. Devido ao nível comparável de proteção de dados, a transferência de dados para esses países não requer qualquer autorização ou acordo especial.

Contamos com serviços de terceiros relacionados à computação em nuvem fornecida pela Microsoft como um provedor de serviços de nuvem.

Segurança de dados

A ESET implementa medidas técnicas e organizacionais adequadas para garantir um nível de segurança que seja apropriado para os riscos potenciais. Estamos fazendo nosso melhor para garantir a confidencialidade, integridade, disponibilidade e resiliência constante de sistemas de processamento e serviços. Porém, em caso de violação de dados resultando em um risco aos seus direitos e liberdades, estamos prontos para notificar uma autoridade supervisora relevante, assim como os Usuários Finais afetados como titulares dos dados.

Direitos do sujeito dos dados

Os direitos de todos os Usuários Finais são importantes e gostaríamos de informar que todos os Usuários Finais (de qualquer país da UE ou que não da UE) têm os seguintes direitos garantidos na ESET. Para exercer seus direitos de titular dos dados, você pode entrar em contato conosco através do formulário de suporte ou por e-mail em dpo@eset.sk. Para fins de identificação, pedimos as informações a seguir: Nome, endereço de e-mail e, se disponível, chave de licença ou número do cliente e filiação da empresa. Não envie nenhum outro dado pessoal, como a data de nascimento. Destacamos que, para ser capaz de processar sua solicitação, assim como para fins de identificação, vamos processar seus dados pessoais.

Direito de retirar o consentimento. O direito de retirar o consentimento é aplicável no caso de tratamento baseado apenas no consentimento. Se processarmos seus dados pessoais com base em seu consentimento, você tem o direito de retirar o consentimento a qualquer momento sem dar motivos. A retirada do seu consentimento só é eficaz para o futuro e não afeta a legalidade dos dados processados antes da retirada.

Direito a uma objeção. O direito de objeção ao tratamento é aplicável no caso de tratamento com base no interesse legítimo da ESET ou de terceiros. Se tratarmos seus dados pessoais para proteger um interesse legítimo,

Você como o titular dos dados tem o direito de objeção aos interesses legítimos nomeados por Nós e ao tratamento de seus dados pessoais a qualquer momento. Sua objeção só é eficaz para o futuro e não afeta a legalidade dos dados processados antes da objeção. Se processarmos seus dados pessoais para fins de marketing direto, não é necessário dar motivos para sua objeção. Isso também se aplica a criação de perfis, na medida em que está conectado a tal marketing direto. Em todos os outros casos, solicitamos que você nos informe brevemente sobre suas queixas contra o interesse legítimo da ESET para tratar seus dados pessoais.

Observe que, em alguns casos, apesar de sua retirada de consentimento, temos o direito de continuar com o tratamento de seus dados pessoais com base em outra base jurídica, por exemplo, para a execução de um contrato.

Direito de acesso. Como um titular dos dados, você tem o direito de obter informações sobre seus dados armazenados pela ESET gratuitamente a qualquer momento.

Direito a retificação. Se inadvertidamente tratarmos dados pessoais incorretos sobre você, você tem o direito de corrigir isso.

Direito a exclusão e direito a restrição do tratamento. Como um titular dos dados, você tem o direito de solicitar a exclusão ou restrição do tratamento de seus dados pessoais. Se tratarmos seus dados pessoais, por exemplo, com seu consentimento, você retirará esse consentimento e se não houver outra base jurídica, por exemplo, um contrato, removeremos seus dados pessoais imediatamente. Seus dados pessoais também serão removidos assim que não forem mais necessários para os fins declarados para eles no final do nosso período de retenção.

Se usarmos seus dados pessoais com o objetivo exclusivo de marketing direto e você tiver revogado seu consentimento ou feito uma objeção ao interesse legítimo subjacente da ESET, restringiremos o tratamento de seus dados pessoais na medida em que incluirmos seus dados de contato em nossa lista de proibições interna para evitar contato não solicitado. Caso contrário, seus dados pessoais serão removidos.

Note que Nós podemos ser obrigados a armazenar seus dados até a expiração das obrigações de retenção e períodos emitidos pelas autoridades legisladoras ou supervisoras. Obrigações e períodos de retenção também podem ser resultado da legislação eslovaca. Depois disso, os dados correspondentes serão removidos rotineiramente.

Direito à portabilidade de dados. Será um prazer fornecer a Você, como um titular dos dados, os dados pessoais processados pela ESET no formato xls.

Direito de fazer uma queixa. Como um titular dos dados, Você tem o direito de enviar uma queixa à autoridade supervisora a qualquer momento. A ESET é sujeita ao regulamento das leis eslovacas e estamos vinculados pela legislação de proteção de dados como parte da União Europeia. A autoridade supervisora de dados relevante é o Gabinete de Proteção de Dados Pessoais da República Eslovaca, localizado em Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Tratamento de seus Dados pessoais

Serviços fornecidos pela ESET implementados em nosso produto baseado na web são oferecidos sob os Termos de Uso (“ToU”), mas alguns deles podem precisar de uma atenção específica. Gostaríamos de fornecer a Você mais detalhes sobre o processamento de dados em relação ao fornecimento de nossos produtos e prestação de nossos serviços. Prestamos vários serviços descritos no Termos Especiais e no produto documentação. Para que tudo funcione, precisamos coletar as informações a seguir:

Dados de licenciamento e cobrança. O nome, endereço de e-mail, chave de licença e (se aplicável), endereço, filiação da empresa e dados de pagamento são coletados e processados pela ESET para facilitar a ativação da

licença, entrega de chaves de licença, lembretes sobre a expiração, solicitações de suporte, verificação da autenticidade da licença, fornecimento de nosso serviço e outras notificações, inclusive mensagens de marketing de acordo com a legislação aplicável ou com o Seu consentimento. A ESET é legalmente obrigada a manter as informações de cobrança pelo período de 10 anos, mas as informações de licenciamento serão transformadas em anônimas no máximo 12 meses depois da expiração da licença.

Atualização e outras estatísticas. As informações processadas incluem informações sobre o processo de instalação e seu computador, incluindo a plataforma na qual seu produto está instalado e informações sobre as operações e funcionalidades de seus produtos, como o sistema operacional, informações de hardware, IDs de instalação, ID de licença, endereço IP, endereço MAC, definições de configuração do produto são processadas para fins de fornecimento de serviços de atualização e manutenção, segurança e melhoria de nossa infraestrutura de backend.

Essas informações são mantidas além das informações de identificação necessárias para os fins de licenciamento e cobrança, já que não requerem a identificação do Usuário Final. O período de retenção é de até 4 anos.

ESET LiveGrid® Sistema de reputação. Hashes de via única relacionados a infiltrações são processados para os fins do Sistema de Reputação ESET LiveGrid®, o que melhora a eficiência de nossas soluções antimalware ao comparar os arquivos escaneados com um banco de dados de itens na lista de permissões e na lista de proibições na nuvem. O Usuário Final não é identificado durante esse processo.

ESET LiveGrid® Sistema de feedback. Amostras suspeitas e metadados originais como parte do Sistema de Feedback ESET LiveGrid® permite que a ESET reaja imediatamente às necessidades de nossos usuários finais e nos mantém sensível às ameaças mais recentes. Nós dependemos de Você enviando

- Infiltrações como amostras potenciais de vírus e outros programas nocivos e suspeitos; objetos problemáticos, potencialmente indesejados ou potencialmente inseguros como arquivos executáveis, mensagens de email reportadas por Você como spam ou marcadas pelo nosso produto;
- Informações sobre o uso da internet como endereço IP e informações geográficas, pacotes de IP, URL e quadros ethernet;
- Arquivos de despejo de parada e informações contidas neles.

Não queremos coletar seus dados além desse escopo, mas isso pode ser impossível de impedir algumas vezes. Dados coletados acidentalmente podem estar incluídos no próprio malware (coletados sem seu conhecimento ou aprovação) ou como parte de nomes de arquivos ou URL e não pretendemos que eles façam parte de nossos sistemas ou processos para os fins declarados nessa Política de Privacidade.

Todas as informações obtidas e processadas através do Sistema de feedback ESET LiveGrid® são feitas para serem usadas sem a identificação do Usuário Final.

Suporte técnico. As informações de contato e licenciamento e dados contidos em suas solicitações de suporte podem ser necessários para o serviço de suporte. Com base no canal escolhido por Você para entrar em contato conosco, podemos coletar seu endereço de email, número de telefone, informações de licença, detalhes do produto e a descrição do seu caso de suporte. Podemos solicitar que você forneça outras informações para facilitar o serviço de suporte. Os dados processados para suporte técnico são armazenados por 4 anos.

Observe que, se a pessoa usando nossos produtos e serviços não for o Usuário Final que comprou o produto ou serviço e concordou nos Termos conosco (por exemplo, um funcionário do Usuário Final, um membro da família ou uma pessoa autorizada a usar o produto ou serviço pelo Usuário Final de acordo com o Acordo de Licença para o Usuário Final), o tratamento dos dados é realizado no interesse legítimo da ESET, dentro do significado do Art. 6 (1) (f) LGPD para permitir ao usuário autorizado pelo Usuário Final usar os produtos e serviços fornecidos por Nós de acordo com o Acordo de Licença para o Usuário Final.

Informações de contato

Se Você quiser exercer seus direitos como sujeito de dados ou se tiver uma pergunta ou dúvida, envie uma mensagem para:

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