

# ESET Cyber Security Pro

## Guia do Usuário

[Clique aqui para exibir a versão da Ajuda deste documento](#)

Direitos autorais ©2023 por ESET, spol. s r.o.

ESET Cyber Security Pro foi desenvolvido por ESET, spol. s r.o.

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

Todos os direitos reservados. Nenhuma parte desta documentação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravação, digitalização, ou de outra forma sem a permissão por escrito do autor.

A ESET, spol. s r.o. reserva-se o direito de alterar qualquer software aplicativo descrito sem prévio aviso.

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

REV. 19-03-2023

1 ESET Cyber Security Pro .....	1
<b>1.1 Novidades da versão 6</b> .....	1
<b>1.2 Requisitos do sistema</b> .....	1
2 Instalação .....	2
<b>2.1 Instalação típica</b> .....	3
<b>2.2 Instalação personalizada</b> .....	4
3 Ativação do produto .....	5
4 Desinstalação .....	6
5 Descrição básica .....	6
<b>5.1 Atalhos do teclado</b> .....	7
<b>5.2 Verificação do estado da proteção</b> .....	7
<b>5.3 O que fazer se o programa não funcionar corretamente</b> .....	8
6 Proteção do computador .....	8
<b>6.1 Proteção antivírus e antispware</b> .....	9
6.1 Geral .....	9
6.1 Exclusões .....	9
6.1 Proteção na inicialização .....	10
6.1 Proteção em tempo real do sistema de ficheiros .....	10
6.1 Opções avançadas .....	11
6.1 Quando modificar a configuração da Proteção em tempo real .....	11
6.1 Verificação da Proteção em tempo real .....	12
6.1 O que fazer se a Proteção em tempo real não funcionar .....	12
6.1 Análise do computador a pedido .....	12
6.1 Tipos de análise .....	13
6.1 Análise inteligente .....	13
6.1 Análise personalizada .....	14
6.1 Alvos de análise .....	14
6.1 Perfis de análise .....	14
6.1 Configuração dos parâmetros do mecanismo ThreatSense .....	15
6.1 Objetos .....	16
6.1 Opções .....	17
6.1 Limpeza .....	17
6.1 Exclusões .....	18
6.1 Limites .....	18
6.1 Outros .....	19
6.1 Foi detetada uma infiltração .....	19
<b>6.2 Análise e bloqueio do suporte amovível</b> .....	20
7 Antiphishing .....	21
8 Firewall .....	21
<b>8.1 Modos de filtragem</b> .....	22
<b>8.2 Regras da firewall</b> .....	23
8.2 Criação de novas regras .....	23
<b>8.3 Zonas da firewall</b> .....	24
<b>8.4 Perfis da firewall</b> .....	24
<b>8.5 Relatórios da firewall</b> .....	24
9 Proteção da Web e de e-mails .....	25
<b>9.1 Proteção Web</b> .....	25
9.1 Portas .....	25
9.1 Listas de URL .....	25
<b>9.2 Proteção de e-mail</b> .....	26

9.2 Verificação de protocolo POP3 .....	27
9.2 Verificação de protocolo IMAP .....	27
<b>10 Controlo parental .....</b>	<b>28</b>
<b>11 Atualizar .....</b>	<b>28</b>
<b>11.1 Configuração da atualização .....</b>	<b>29</b>
11.1 Opções avançadas .....	29
<b>11.2 Como criar tarefas de atualização .....</b>	<b>30</b>
<b>11.3 Atualizar o ESET Cyber Security Pro para uma nova versão .....</b>	<b>30</b>
<b>11.4 Atualizações do sistema .....</b>	<b>30</b>
<b>12 Ferramentas .....</b>	<b>31</b>
<b>12.1 Relatórios .....</b>	<b>32</b>
12.1 Manutenção de relatórios .....	32
12.1 Filtragem de relatórios .....	33
<b>12.2 Agenda .....</b>	<b>34</b>
12.2 Criação de novas tarefas .....	35
12.2 Analisar como proprietário de diretório .....	36
12.2 Criação de tarefas definidas pelo utilizador .....	36
<b>12.3 Quarentena .....</b>	<b>37</b>
12.3 Colocação de ficheiros em quarentena .....	38
12.3 Restauro da Quarentena .....	38
12.3 Envio de ficheiro da Quarentena .....	38
<b>12.4 Processos em execução .....</b>	<b>38</b>
<b>12.5 Ligações de rede .....</b>	<b>39</b>
<b>12.6 Live Grid .....</b>	<b>39</b>
12.6 Configuração do Live Grid .....	40
<b>13 Interface do utilizador .....</b>	<b>41</b>
<b>13.1 Alertas e notificações .....</b>	<b>41</b>
13.1 Mostrar alertas .....	42
13.1 Estados da proteção .....	42
<b>13.2 Privilégios .....</b>	<b>43</b>
<b>13.3 Menu de contexto .....</b>	<b>43</b>
<b>13.4 Importar e exportar definições .....</b>	<b>43</b>
<b>13.5 Configuração do servidor proxy .....</b>	<b>44</b>
<b>13.6 Tipos de infiltrações .....</b>	<b>44</b>
13.6 Vírus .....	44
13.6 Worms .....	45
13.6 Cavalos de troia (Trojans) .....	46
13.6 Rootkits .....	46
13.6 Adware .....	46
13.6 Spyware .....	47
13.6 Aplicações potencialmente inseguras .....	48
13.6 Aplicações potencialmente não desejadas .....	48
<b>13.7 Tipos de ataques remotos .....</b>	<b>50</b>
13.7 Ataques DoS .....	50
13.7 Envenenamento de DNS .....	50
13.7 Análise da porta .....	50
13.7 Dessincronização do TCP .....	51
13.7 Relé SMB .....	51
13.7 Ataques ICMP .....	52
<b>13.8 E-mail .....</b>	<b>52</b>

13.8 Publicidades .....	53
13.8 Hoaxes .....	53
13.8 Phishing .....	54
13.8 Reconhecer fraudes através de spam .....	54
<b>14 Contrato de Licença do Utilizador Final .....</b>	<b>54</b>
<b>15 Política de Privacidade .....</b>	<b>62</b>

# ESET Cyber Security Pro

O ESET Cyber Security Pro representa uma nova abordagem em relação à segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de análise ThreatSense®, em combinação com Proteção de cliente de e-mail, Firewall e Controlo parental, utiliza velocidade e precisão para manter o seu computador seguro. O resultado é um sistema inteligente que está constantemente em alerta, protegendo o seu computador de ataques e software malicioso.

O ESET Cyber Security Pro é uma solução de segurança completa produzida a partir do nosso esforço a longo prazo para combinar uma proteção máxima e um impacto mínimo no sistema. Com base em inteligência artificial, as tecnologias avançadas que compõem o ESET Cyber Security Pro são capazes de eliminar de forma proativa infiltrações de vírus, worms, cavalos de troia, spyware, adware, rootkits e outros ataques com origem na Internet sem prejudicar o desempenho do sistema.

## Novidades da versão 6

A versão 6 do ESET Cyber Security Pro introduz as seguintes atualizações e melhorias:

- **Suporte à arquitetura de 64 bits**
- **Antiphishing** - impede que Web sites falsos disfarçados de Web sites de confiança adquiram as suas informações pessoais
- **Atualizações do sistema** – a versão 6 do ESET Cyber Security Pro inclui várias correções e melhorias, incluindo notificações para atualizações do sistema operativo. Para saber mais sobre este assunto, consulte a secção [Atualizações do sistema](#).
- **Estados da proteção** – oculta notificações do ecrã Estado da proteção (Por exemplo, *Proteção de e-mail desativada* ou *É necessário reiniciar o computador*)
- **Suporte a analisar** – é possível excluir determinados suportes da Análise em tempo real (Unidades locais, Suportes amovíveis, Suportes em rede)
- **Ligações de rede** - apresenta ligações de rede no computador e permite-lhe criar regras para estas ligações.

## Requisitos do sistema

Para um desempenho ideal do ESET Cyber Security Pro, o sistema deve satisfazer ou exceder os seguintes requisitos de hardware e de software:

	Requisitos do sistema
Arquitetura do processador	Intel 64 bits
Sistema operativo	macOS 10.12 ou posterior
Memória	300 MB

Espaço livre em disco	200 MB
-----------------------	--------

## Instalação

Antes de iniciar o processo de instalação, feche todos os programas abertos no computador. O ESET Cyber Security Pro contém componentes que podem entrar em conflito com outros programas antivírus que já podem estar instalados no computador. A ESET recomenda vivamente que remova todos os outros programas antivírus para evitar possíveis problemas.

Para iniciar o assistente de instalação, execute uma das seguintes ações:

- Se instalar a partir de um ficheiro transferido do Web site da ESET, abra o ficheiro e clique duas vezes no ícone **Instalar**
- Se instalar a partir do CD/DVD de instalação, insira-o no computador, abra-o a partir do ambiente de trabalho ou da janela **Finder** e clique duas vezes no ícone **Instalar**



O assistente de instalação orientá-lo-á ao longo do processo de configuração básica. Durante a fase inicial da instalação, o instalador irá procurar automaticamente online a versão mais recente do produto. Se for encontrada uma versão mais recente, poderá optar por transferi-la antes de continuar o processo de instalação.

Após concordar com o Contrato de Licença do Utilizador Final, ser-lhe-á pedido para selecionar um dos seguintes modos de instalação:

- [Instalação típica](#)

- [Instalação personalizada](#)

## Instalação típica

O modo de instalação típica inclui opções de configuração apropriadas para a maioria dos utilizadores. Estas definições proporcionam segurança máxima em combinação com um excelente desempenho do sistema. A instalação típica é a opção predefinida e é recomendada caso não possua requisitos específicos para definições.

### ESET Live Grid

O Live Grid Early Warning System ajuda a garantir que a ESET é imediata e continuamente informada de novas infiltrações de forma a proteger rapidamente os nossos clientes. O sistema permite que novas ameaças sejam enviadas para o Threat Lab da ESET, onde estas são analisadas e processadas. Recomendamos que ative o ESET Live Grid. Clique em **Configurar** para modificar as definições para o envio de ficheiros suspeitos. Para mais informações, consulte o tópico [Live Grid](#). Se o ESET Live Grid estiver desativado, o ESET Cyber Security Pro apresenta um alerta de segurança.

### Aplicações potencialmente não desejadas

O próximo passo do processo de instalação é configurar a deteção de **Aplicações potencialmente não desejadas**. As aplicações potencialmente não desejadas não são necessariamente maliciosas, mas podem afetar negativamente o comportamento do sistema operativo. Estas aplicações estão frequentemente integradas noutros programas e podem ser difíceis de notar durante o processo de instalação. Apesar de estas aplicações apresentarem geralmente uma notificação durante a instalação, podem ser instaladas facilmente sem o seu consentimento.

Depois de instalar o ESET Cyber Security Pro pela primeira vez, irá receber a notificação **Extensão do sistema bloqueada** do próprio sistema e a notificação **O seu computador não está protegido** do ESET Cyber Security Pro. Para aceder a todas as funções do ESET Cyber Security Pro, terá de permitir extensões de kernel no dispositivo. Para permitir extensões de kernel no dispositivo, navegue para **Preferências do sistema > Segurança e privacidade** e clique em **Permitir** para permitir software do sistema do programador **ESET, spol. s.r.o.**

1. Receberá a notificação **Extensão do sistema bloqueada** do seu sistema e a notificação **O seu computador não está protegido** do ESET Cyber Security Pro. Para aceder a todas as funções do ESET Cyber Security Pro, tem de permitir as extensões kernel no seu dispositivo. Para permitir extensões kernel no seu dispositivo, navegue para **Preferências do sistema > Segurança e privacidade** e clique em **Permitir** para permitir software do sistema do programador **ESET, spol. s.r.o.** Para informações mais detalhadas, visite o nosso [artigo da base de dados de conhecimento](#).

2. Receberá a notificação **O seu computador está parcialmente protegido** do ESET Cyber Security Pro. Para aceder a todas as funções do ESET Cyber Security Pro, tem de permitir o **Acesso total ao disco** ao ESET Cyber Security Pro. Clique em **Abrir Preferências do sistema > Segurança e privacidade**. Aceda ao separador **Privacidade** e selecione a opção **Acesso total ao disco**. Clique no ícone de cadeado para permitir a edição. Clique no ícone de adição e selecione a aplicação ESET Cyber Security Pro. O seu computador apresentará uma notificação para reiniciar o seu computador. Clique em **Mais tarde**. Não reinicie agora o seu computador.

Clique em **Iniciar novamente** na janela de notificação do ESET Cyber Security Pro ou reinicie o seu computador. Para informações mais detalhadas, visite o nosso [artigo da base de dados de conhecimento](#).

Após instalar o ESET Cyber Security Pro, deve analisar o seu computador quanto à presença de códigos maliciosos. A partir da janela de programa principal, clique em **Análise do computador > Análise inteligente**. Para mais informações sobre análises de computador a pedido, consulte o tópico [Análise de computador a pedido](#).

## Instalação personalizada

O modo de instalação personalizada destina-se a utilizadores experientes que pretendem modificar as definições avançadas durante o processo de instalação.

### Servidor proxy

Se estiver a utilizar um servidor proxy, defina os respetivos parâmetros ao selecionar **Utilizo um servidor proxy**. Na próxima janela, introduza o endereço IP ou o URL do servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as ligações (3128 por predefinição). Caso o servidor proxy requeira autenticação, introduza um **Nome de utilizador** e uma **Palavra-passe** válidos para obter acesso ao servidor proxy. Se não utilizar um servidor proxy, selecione **Não utilizo um servidor proxy**. Se não tiver a certeza se está a utilizar um servidor proxy, selecione **Utilizar as definições do sistema (recomendado)** para utilizar as definições atuais do sistema.

### Privilégios

Neste passo, tem a possibilidade de definir utilizadores ou grupos privilegiados a quem serão concedidas permissões para editar a configuração do programa. Na lista de utilizadores, à esquerda, selecione os utilizadores e selecione **Adicionar** para incluí-los na lista **Utilizadores privilegiados**. Para visualizar todos os utilizadores do sistema, selecione **Mostrar todos os utilizadores**. Se deixar a lista de Utilizadores privilegiados vazia, todos os utilizadores são considerados privilegiados.

### ESET Live Grid

O Live Grid Early Warning System ajuda a garantir que a ESET é imediata e continuamente informada de novas infiltrações de forma a proteger rapidamente os nossos clientes. O sistema permite que novas ameaças sejam enviadas para o Threat Lab da ESET, onde estas são analisadas e processadas. Recomendamos que ative o ESET Live Grid (recomendado). Clique em **Configurar** para modificar as definições para o envio de ficheiros suspeitos. Para mais informações, consulte o tópico [Live Grid](#). Se o ESET Live Grid estiver desativado, o ESET Cyber Security Pro apresenta um alerta de segurança.

### Aplicações potencialmente não desejadas

O próximo passo do processo de instalação é configurar a deteção de **Aplicações potencialmente não desejadas**.

As aplicações potencialmente não desejadas não são necessariamente maliciosas, mas podem afetar negativamente o comportamento do sistema operativo. Estas aplicações estão frequentemente integradas noutros programas e podem ser difíceis de notar durante o processo de instalação. Apesar de estas aplicações apresentarem geralmente uma notificação durante a instalação, podem ser instaladas facilmente sem o seu consentimento.

## Firewall

No último passo, tem a possibilidade de seleccionar o modo de filtragem da Firewall. Para mais informações, consulte o tópico [Modos de filtragem](#).

Depois de instalar o ESET Cyber Security Pro pela primeira vez, irá receber a notificação **Extensão do sistema bloqueada** do próprio sistema e a notificação **O seu computador não está protegido** do ESET Cyber Security Pro. Para aceder a todas as funções do ESET Cyber Security Pro, terá de permitir extensões de kernel no dispositivo. Para permitir extensões de kernel no dispositivo, navegue para **Preferências do sistema > Segurança e privacidade** e clique em **Permitir** para permitir software do sistema do programador **ESET, spol. s.r.o.**

1.Receberá a notificação **Extensão do sistema bloqueada** do seu sistema e a notificação **O seu computador não está protegido** do ESET Cyber Security Pro. Para aceder a todas as funções do ESET Cyber Security Pro, tem de permitir as extensões kernel no seu dispositivo. Para permitir extensões kernel no seu dispositivo, navegue para **Preferências do sistema > Segurança e privacidade** e clique em **Permitir** para permitir software do sistema do programador **ESET, spol. s.r.o.** Para informações mais detalhadas, visite o nosso [artigo da base de dados de conhecimento](#).

2.Receberá a notificação **O seu computador está parcialmente protegido** do ESET Cyber Security Pro. Para aceder a todas as funções do ESET Cyber Security Pro, tem de permitir o **Acesso total ao disco** ao ESET Cyber Security Pro. Clique em **Abrir Preferências do sistema > Segurança e privacidade**. Aceda ao separador **Privacidade** e selecione a opção **Acesso total ao disco**. Clique no ícone de cadeado para permitir a edição. Clique no ícone de adição e selecione a aplicação ESET Cyber Security Pro. O seu computador apresentará uma notificação para reiniciar o seu computador. Clique em **Mais tarde**. Não reinicie agora o seu computador. Clique em **Iniciar novamente** na janela de notificação do ESET Cyber Security Pro ou reinicie o seu computador. Para informações mais detalhadas, visite o nosso [artigo da base de dados de conhecimento](#).

Após instalar o ESET Cyber Security Pro, deve analisar o seu computador quanto à presença de códigos maliciosos. A partir da janela de programa principal, clique em **Análise do computador > Análise inteligente**. Para mais informações sobre análises de computador a pedido, consulte o tópico [Análise de computador a pedido](#).

## Ativação do produto

Após a instalação, a janela Ativação do produto é apresentada automaticamente. Para aceder à caixa de diálogo de ativação do produto em qualquer altura, clique no ícone do ESET Cyber Security Pro <sup>®</sup> localizado na Barra de menu do macOS (parte superior do ecrã) e depois clique em **Ativação do produto....**

- **Chave de licença** – uma cadeia de caracteres exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXXX que é utilizada para identificar o proprietário da licença e ativar a licença. Se adquiriu uma versão em caixa a retalho do produto, ative o produto utilizando uma Chave de licença. Esta está geralmente localizada no interior ou na parte posterior da embalagem do produto.
- **Nome de utilizador e palavra-passe** – Se tiver um Nome de utilizador e palavra-passe e não souber como ativar o ESET Cyber Security Pro, clique em **O que faço com o Nome de utilizador e Palavra-passe?**. Será redirecionado para my.eset.com onde pode converter as suas credenciais numa Chave de licença.
- **Licença de avaliação gratuita** – seleccione esta opção se pretender avaliar o ESET Cyber Security Pro antes de efetuar uma compra. Preencha com o seu endereço de e-mail para ativar o ESET Cyber Security Pro durante um período limitado. A sua licença de teste ser-lhe-á enviada por e-mail. As licenças de avaliação apenas podem ser ativadas uma vez por cliente.
- **Comprar licença** – se não tem uma licença e gostaria de comprar uma, clique em Comprar licença. Isto irá redirecioná-lo para o Web site do distribuidor local da ESET.
- **Ativar mais tarde** – clique nesta opção se não pretender ativar neste momento.

## Desinstalação

Para desinstalar o ESET Cyber Security Pro, execute uma das seguintes ações:

- insira o CD/DVD de instalação do ESET Cyber Security Pro no computador, abra-o a partir do ambiente de trabalho ou da janela **Finder** e clique duas vezes em **Desinstalar**
- abra o ficheiro de instalação do ESET Cyber Security Pro (.dmg) e clique duas vezes em **Desinstalar**
- inicie o **Finder**, abra a pasta **Aplicações** no disco rígido, CTRL + clique no ícone **ESET Cyber Security Pro** e seleccione a opção **Mostrar conteúdo do pacote**. Abra a pasta **Contents > Helpers** e clique duas vezes no ícone **Uninstaller**.

## Descrição básica

A janela principal do ESET Cyber Security Pro está dividida em duas secções principais. A janela principal à direita apresenta informações correspondentes à opção selecionada no menu principal à esquerda.

As secções que se seguem podem ser acedidas a partir do menu principal:

- **Início** – fornece informações sobre o estado da proteção do seu Computador, Firewall, Proteção da Web e e-mail e Controlo parental.
- **Análise do computador** – esta secção permite configurar e iniciar a [Análise do computador a pedido](#).
- **Atualizar** – apresenta informações sobre as atualizações dos módulos de deteção.
- **Configurar** – seleccione esta secção para ajustar o nível de segurança do computador.

- **Ferramentas** – fornece acesso a [Relatórios](#), [Agenda](#), [Quarentena](#), [Processos em execução](#) e outras funcionalidades do programa.
- **Formação em cibersegurança** - curso de formação online gratuito para ajudá-lo a proteger os dados do seu computador e as informações pessoais.
- **Ajuda** – apresenta o acesso para ficheiros de ajuda, base de dados de conhecimento da Internet, formulário de pedido de suporte e informações adicionais do programa.

## Atalhos do teclado

Atalhos do teclado que podem ser utilizados ao trabalhar com o ESET Cyber Security Pro:

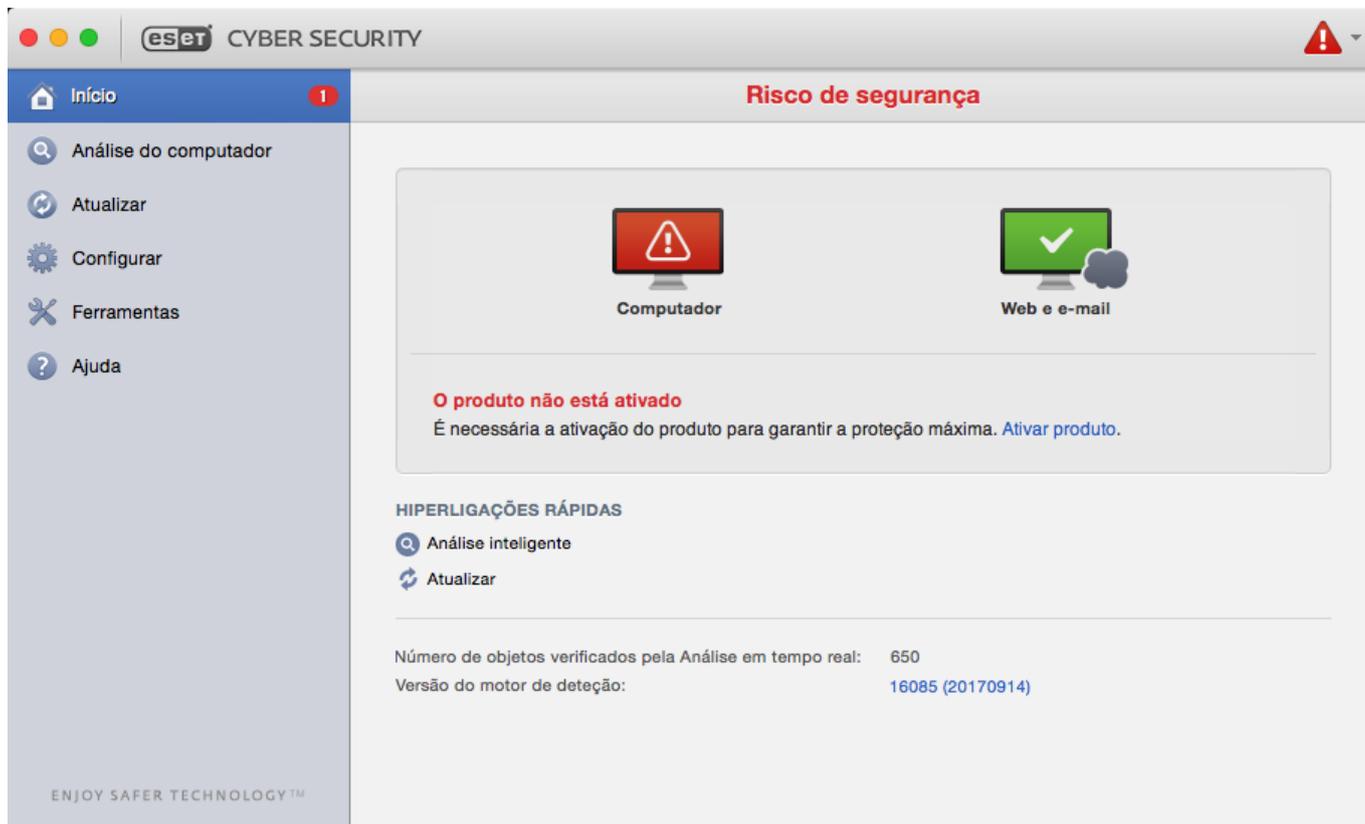
- *cmd+,* - apresenta as preferências do ESET Cyber Security Pro,
- *cmd+O* - redimensiona a janela da GUI principal do ESET Cyber Security Pro para o tamanho predefinido e move-a para o centro do ecrã,
- *cmd+Q* - oculta a janela da GUI principal do ESET Cyber Security Pro. Pode abri-la clicando no ícone do ESET Cyber Security Pro  na Barra de menu macOS (parte superior do ecrã),
- *cmd+W* - fecha a janela da GUI principal do ESET Cyber Security Pro.

Os seguintes atalhos do teclado apenas funcionam se **Usar menu padrão** estiver ativado em **Configurar > Introduzir preferências da aplicação... > Interface**:

- *cmd+alt+L* - abra a secção **Relatórios**,
- *cmd+alt+S* - abre a secção **Agenda**,
- *cmd+alt+Q* - abre a secção **Quarentena**.

## Verificação do estado da proteção

Para ver o estado da proteção, clique em **Início** no menu principal. Um resumo de estado sobre o funcionamento dos módulos do ESET Cyber Security Pro será apresentado na janela principal.



## O que fazer se o programa não funcionar corretamente

Se um módulo estiver a funcionar corretamente, é apresentado um ícone verde. Se um módulo não estiver a funcionar corretamente, será apresentado um ponto de exclamação vermelho ou um ícone de notificação laranja. Serão apresentadas informações adicionais sobre o módulo e uma solução sugerida para corrigir o problema. Para alterar o estado dos módulos individuais, clique na hiperligação azul por baixo de cada mensagem de notificação.

Se não conseguir resolver um problema utilizando as soluções sugeridas, pode pesquisar na [Base de dados de conhecimento da ESET](#) por uma solução ou contactar o [Suporte ao cliente da ESET](#). O Suporte ao cliente irá responder rapidamente às suas perguntas e ajudar a resolver qualquer problema com o ESET Cyber Security Pro.

## Proteção do computador

A configuração do computador pode ser encontrada em **Configuração > Computador**. Apresenta o estado de **Proteção em tempo real do sistema de ficheiros** e **Bloquear suporte amovível**. Para desativar módulos individuais, altere o botão do módulo pretendido para **DESATIVADO**. Tenha em atenção que isto poderá diminuir ao nível de proteção do seu computador. Para aceder às definições detalhadas para cada módulo, clique em **Configurar....**

# Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos, modificando ficheiros que representam ameaças internas. Se uma ameaça com código malicioso for detectada, o módulo antivírus poderá eliminá-la, bloqueando-a e, em seguida, limpando, eliminando ou movendo-a para a quarentena.

## Geral

Na secção **Geral (Configurar > Introduzir preferências da aplicação... > Geral)**, pode ativar a deteção dos seguintes tipos de aplicações:

- **Aplicações potencialmente não desejadas** - Estas aplicações não são necessariamente maliciosas, mas podem afetar negativamente o desempenho do computador. Tais aplicações exigem geralmente o consentimento para a instalação. Se estas aplicações estiverem presentes no computador, o sistema irá comportar-se de modo diferente (em comparação ao modo anterior à instalação destas aplicações). As alterações mais significativas incluem janelas pop-up não desejadas, ativação e execução de processos ocultos, aumento da utilização de recursos do sistema, alterações nos resultados de pesquisa e aplicações em comunicação com servidores remotos.
- **Aplicações potencialmente inseguras** - estas aplicações são softwares comerciais e legítimos que podem sofrer abusos por parte de atacantes caso tenham sido instaladas sem o consentimento do utilizador. Esta classificação inclui programas como ferramentas de acesso remoto, motivo pelo qual esta opção está desativada por predefinição.
- **Aplicações suspeitas** - estas aplicações incluem programas compactados com empacotadores ou protetores. Estes tipos de protetores são, muitas vezes, explorados por autores de malware para evitar a deteção. Um empacotador é um executável de autoextração em tempo real que reúne vários tipos de malware num único pacote. Os empacotadores mais comuns são o UPX, PE\_Compact, PKLite e ASPack. O mesmo malware pode ser detetado de forma diferente quando compactado com um empacotador diferente. Os empacotadores apresentam também a capacidade de alterar as respetivas "assinaturas" ao longo do tempo, tornando mais difícil a deteção e remoção de malware.

Para configurar as [Exclusões do Sistema de Ficheiros ou Web e E-mail](#), clique no botão **Configurar...**

## Exclusões

Na secção **Exclusões**, é possível excluir determinados ficheiros/pastas, aplicações ou endereços IP/IPv6 da análise.

Os ficheiros e pastas incluídos no separador **Sistema de ficheiros** serão excluídos de todas as análises: Inicialização, Tempo real e A pedido (Análise do computador).

- **Caminho** – caminho para ficheiros e pastas excluídos

- **Ameaça** – se houver um nome de uma ameaça junto a um ficheiro excluído, significa que o ficheiro só foi excluído para essa ameaça e não completamente. Se o ficheiro for infetado posteriormente com outro malware, será detetado pelo módulo antivírus.
-  – cria uma nova exclusão. Introduza o caminho para um objeto (também podem utilizar os caracteres universais \* e ?) ou selecionar a pasta ou ficheiro na estrutura em árvore.
-  – remove as entradas selecionadas
- **Padrão** – cancela todas as exclusões

No separador **Web e e-mail**, pode excluir determinadas **Aplicações** ou **Endereços IP/IPv6** da análise de protocolo.

## Proteção na inicialização

A análise de ficheiros na inicialização analisa automaticamente os ficheiros na inicialização do sistema. Por predefinição, esta análise é executada regularmente como tarefa agendada após o início de sessão de um utilizador ou após uma atualização dos módulos de deteção bem-sucedida. Para modificar as definições dos parâmetros do mecanismo ThreatSense aplicáveis à análise na inicialização, clique no botão **Configurar**. Para saber mais sobre a configuração do mecanismo ThreatSense, leia [esta secção](#).

## Proteção em tempo real do sistema de ficheiros

A Proteção em tempo real do sistema de ficheiros verifica todos os tipos de suporte e aciona uma análise com base em vários eventos. Utilizando tecnologia ThreatSense (descrita na secção denominada [Configuração dos parâmetros do mecanismo ThreatSense](#)), a proteção em tempo real do sistema de ficheiros pode variar para ficheiros recém-criados e ficheiros existentes. É possível controlar com mais precisão os ficheiros recém-criados.

Por predefinição, todos os ficheiros são analisados na **abertura de ficheiro**, **criação de ficheiro** ou **execução de ficheiro**. Recomendamos que mantenha estas predefinições, uma vez que fornecem o nível máximo de Proteção em tempo real ao seu computador. A Proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando análise ininterrupta. Em casos especiais (por exemplo, se houver um conflito com outra Análise em tempo real), é possível terminar a Proteção em tempo real, clicando no ícone do ESET Cyber Security Pro  localizado na Barra de menu (parte superior do ecrã) e selecionando **Desativar Proteção em Tempo Real do Sistema de Ficheiros**. A Proteção em tempo real do sistema de ficheiros também pode ser desativada a partir da janela principal do programa (clique em **Configurar > Computador** e altere **Proteção em tempo real do sistema de ficheiros** para **DESATIVADO**).

É possível excluir da análise Real-time os seguintes tipos de suporte:

- **Unidades locais** - unidades do disco do sistema
- **Suportes amovíveis** - CDs, DVDs, suportes USB, dispositivos Bluetooth, etc.
- **Suportes em rede** - todas as unidades mapeadas

Recomendamos que utilize as predefinições e que apenas modifique as exclusões da análise em casos específicos como, por exemplo, quando a análise de determinados suportes abrandar significativamente as transferências de dados.

Para modificar as definições avançadas da Proteção em tempo real do sistema de ficheiros, aceda a **Configurar > Introduzir preferências da aplicação ...** (ou prima *cmd+*) > **Proteção em tempo real** e clique em **Configurar...** junto das **Opções avançadas** (descritas em [Opções de análise avançadas](#)).

## Opções avançadas

Nesta janela pode definir que tipo de objetos são analisados pelo mecanismo ThreatSense. Para saber mais sobre **Arquivos compactados de auto-extração**, **Empacotadores em tempo real** e **Heurística avançada**, consulte [Configuração de parâmetros do mecanismo ThreatSense](#).

Não recomendamos que faça alterações na secção **Predefinições de ficheiros compactados**, a menos que seja preciso resolver um problema específico, uma vez que valores superiores de compactação de arquivos compactados podem impedir o desempenho do sistema.

**Parâmetros do ThreatSense para ficheiros executados** - por predefinição, a **Heurística avançada** é utilizada quando os ficheiros são executados. Recomendamos vivamente que mantenha a Otimização inteligente e a ESET Live Grid ativadas para mitigar o impacto no desempenho do sistema.

**Aumentar compatibilidade dos volumes de rede** - esta opção otimiza o desempenho ao aceder a ficheiros através da rede. A mesma deve ser ativada se detetar abrandamentos no acesso a unidades da rede. Esta funcionalidade utiliza o coordenador de ficheiros do sistema no macOS X 10.10 e posterior. Tenha em atenção que nem todas as aplicações suportam o coordenador de ficheiros, por exemplo, não é suportado pelo Microsoft Word 2011, mas é suportado pelo Word 2016.

## Quando modificar a configuração da Proteção em tempo real

A Proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro com o ESET Cyber Security Pro. Tenha cuidado ao modificar os parâmetros da Proteção em tempo real. Recomendamos que modifique estes parâmetros apenas em casos específicos. Por exemplo, uma situação em que existe um conflito com uma determinada aplicação.

Após instalar o ESET Cyber Security Pro, todas as definições serão otimizadas para proporcionar o nível máximo

de segurança do sistema aos utilizadores. Para restaurar as predefinições, clique no botão **Padrão** na parte inferior esquerda da janela **Proteção em tempo real (Configurar > Introduzir preferências da aplicação ... > Proteção em tempo real)**.

## Verificação da Proteção em tempo real

Para verificar se a Proteção em tempo real está a funcionar e a detetar vírus, transfira o ficheiro de teste [eicar.com](http://eicar.com) e verifique se ESET Cyber Security Pro o identifica como uma ameaça. Este ficheiro de teste é especial, inofensivo e detetável por todos os programas antivírus. O ficheiro foi criado pelo instituto EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus.

## O que fazer se a Proteção em tempo real não funcionar

Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos a Proteção em tempo real e como resolvê-las.

### A Proteção em tempo real está desativada

Se a Proteção em tempo real for inadvertidamente desativada por um utilizador, será necessário reativá-la. Para reativar a Proteção em tempo real, no menu principal clique em **Configurar > Computador** e altere **Proteção em tempo real do sistema de ficheiros** para **ATIVADO**. Em alternativa, pode ativar a Proteção em tempo real do sistema de ficheiros na janela preferências da aplicação, em **Proteção em tempo real**, selecionando **Ativar proteção em tempo real do sistema de ficheiros**.

### A Proteção em tempo real não deteta nem limpa infiltrações

Verifique se não existe outro programa antivírus instalado no computador. Se forem ativadas duas proteções em tempo real ao mesmo tempo, as mesmas poderão entrar em conflito. Recomendamos que desinstale todos os programas antivírus que possam estar instalados no sistema.

### A Proteção em tempo real não é iniciada

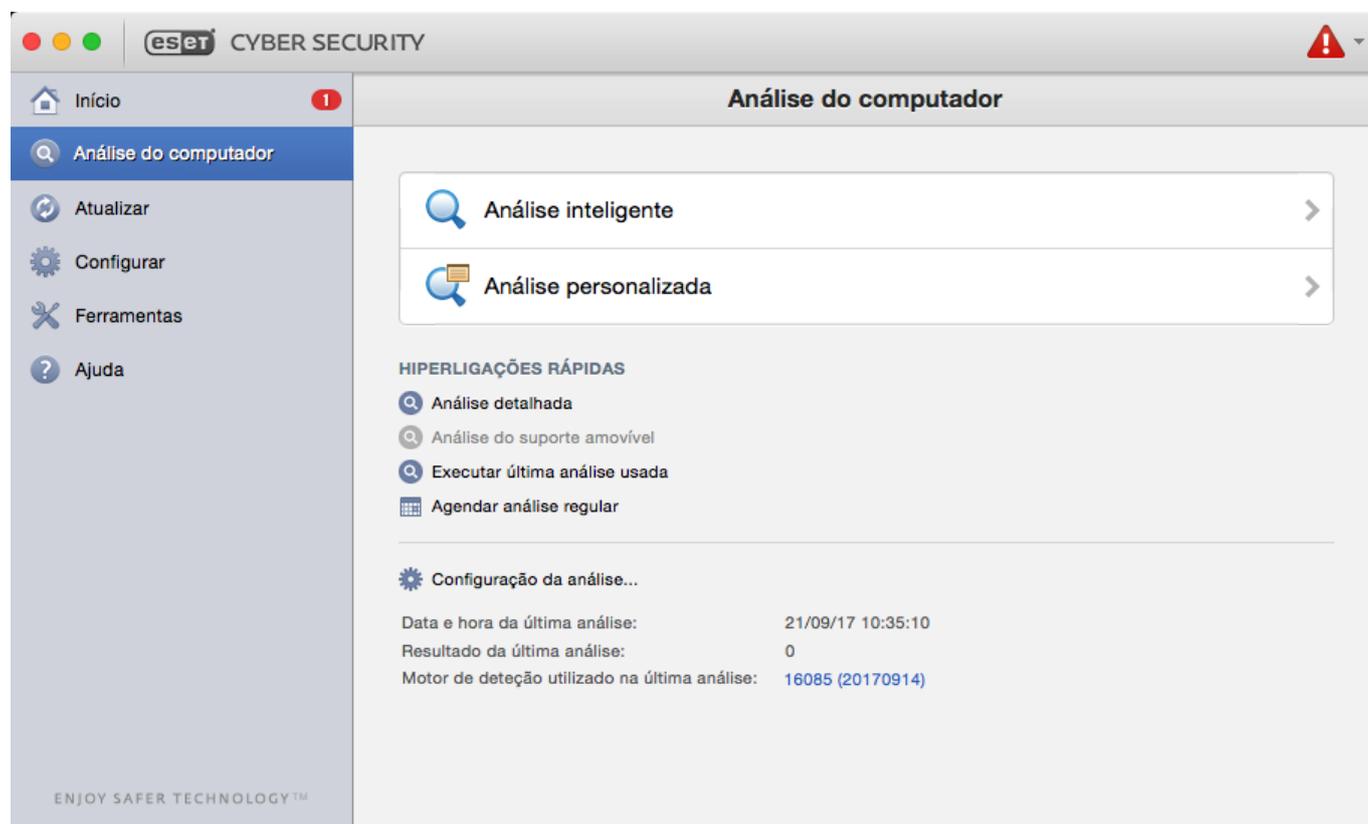
Se a Proteção em tempo real não for ativada na inicialização do sistema, talvez existam conflitos com outros programas. Se for este o caso, contacte o Suporte ao cliente da ESET.

## Análise do computador a pedido

Se suspeitar que o computador está infetado (se se comportar de modo anormal), execute uma **Análise inteligente** para examinar se existem infiltrações no computador. Para obter proteção máxima, as análises do computador devem ser executadas regularmente como parte das medidas usuais de segurança; não apenas quando suspeitar de uma infeção. A análise normal pode detetar infiltrações que não foram detetadas pela

Análise em tempo real quando foram guardadas no disco. Isto pode acontecer caso a Análise em tempo real esteja desativada no momento da infeção ou se os módulos de deteção não estiverem atualizados.

Recomendamos que execute uma Análise do computador a pedido pelo menos uma vez por mês. A análise pode ser configurada como uma tarefa agendada em **Ferramentas > Agenda**.



Recomendamos que execute uma Análise do computador a pedido pelo menos uma vez por mês. A análise pode ser configurada como uma tarefa agendada em **Ferramentas > Agenda**.

## Tipos de análise

Existem dois tipos disponíveis de análise do computador a pedido. A **Análise inteligente** analisa rapidamente o sistema sem necessidade de mais configurações dos parâmetros de análise. A **Análise personalizada** permite seleccionar qualquer perfil de análise predefinido, bem como escolher alvos de análise específicos.

## Análise inteligente

A análise inteligente permite-lhe iniciar rapidamente uma análise do computador e limpar ficheiros infetados, sem a necessidade de intervenção do utilizador. A sua principal vantagem é a operação fácil, sem configurações de análise detalhadas. A Análise inteligente verifica todos os ficheiros em todas as pastas e limpa ou elimina

automaticamente as infiltrações detetadas. O nível de limpeza é automaticamente definido para o valor predefinido. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a secção sobre [Limpeza](#).

## Análise personalizada

A **Análise personalizada** é ideal caso pretenda especificar parâmetros de análise, como alvos de análise e métodos de análise. A vantagem de executar a Análise personalizada é o facto de possibilitar a configuração dos parâmetros detalhadamente. Podem ser guardadas configurações diferentes nos perfis de análise definidos pelo utilizador, o que poderá ser útil se a análise for executada repetidas vezes utilizando os mesmos parâmetros.

Para seleccionar os alvos de análise, seleccione **Análise do computador > Análise personalizada** e, em seguida, seleccione **Alvos de análise** na estrutura em árvore. Um alvo de análise pode ser também especificado com mais exatidão através da introdução do caminho para a pasta ou ficheiro(s) que pretende incluir. Se estiver interessado apenas na análise do sistema, sem ações de limpeza adicionais, seleccione **Analisar sem limpar**. Além disso, pode seleccionar entre três níveis de limpeza clicando em **Configurar... > Limpeza**.



### Análise personalizada

A realização de análises de computador com a Análise personalizada é recomendada para utilizadores avançados com experiência anterior na utilização de programas antivírus.

## Alvos de análise

A estrutura em árvore de Alvos de análise permite-lhe seleccionar ficheiros e pastas que serão analisados quanto a vírus. As pastas também podem ser seleccionadas de acordo com as definições de um perfil.

Um alvo de análise pode ser definido com mais exatidão através da introdução do caminho para a pasta ou ficheiro(s) que pretende incluir na análise. Seleccione os alvos na estrutura em árvore que lista todas as pastas disponíveis no computador através da caixa de verificação que corresponde a um determinado ficheiro ou pasta.

## Perfis de análise

As suas definições de análise favoritas podem ser guardadas para análise futura. Recomendamos a criação de um perfil diferente (com diversos alvos de análise, métodos de análise e outros parâmetros) para cada análise utilizada regularmente.

Para criar um novo perfil, no menu principal, clique em **Configurar > Introduzir preferências da aplicação...** (ou prima *cmd-*) > **Análise do computador** e clique em **Editar...** junto à lista de perfis atuais.



Para ajudar a criar um perfil de análise de acordo com as suas necessidades, consulte a secção [Configuração de parâmetros do mecanismo ThreatSense](#) para obter uma descrição de cada parâmetro da configuração de análise.

Exemplo: Suponhamos que pretende criar o seu próprio perfil de análise e que a configuração de Análise inteligente é parcialmente adequada. Porém, não pretende analisar empacotadores em tempo real nem aplicações potencialmente inseguras e que pretende também aplicar a Limpeza rigorosa. Na janela **Lista de perfis da análise a pedido**, introduza o nome do perfil, clique no botão **Adicionar** e confirme clicando em **OK**. Ajuste os parâmetros de acordo com os seus requisitos, configurando o **Mecanismo ThreatSense** e os **Alvos de análise**.

Se pretender desligar o sistema operativo e encerrar o computador depois de a Análise a pedido terminar, utilize a opção **Encerrar computador após análise**.

## Configuração dos parâmetros do mecanismo ThreatSense

O ThreatSense é uma tecnologia proprietária da ESET, composta por vários métodos de deteção de ameaças complexos. Esta tecnologia é proativa, o que significa que também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genérica, etc.) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de análise é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de deteção. A tecnologia ThreatSense também evita com êxito os rootkits.

As opções de configuração da tecnologia ThreatSense permitem-lhe especificar diversos parâmetros de análise:

- Tipos e extensões de ficheiros que serão analisados
- A combinação de diversos métodos de deteção
- Níveis de limpeza, etc.

Para abrir a janela de configuração, clique em **Configurar > Introduzir preferências da aplicação** (ou prima *cmd+,*) e, em seguida, clique no botão **Configuração** do mecanismo ThreatSense localizado nos módulos **Proteção na inicialização, Proteção em tempo real e Análise do computador**, que utilizam a tecnologia ThreatSense (consultar abaixo). Cenários de segurança diferentes podem exigir configurações diferentes. Como tal, o ThreatSense é configurado individualmente para os seguintes módulos de proteção:

- **Proteção na inicialização** - Análise automática de ficheiros na inicialização
- **Proteção em tempo real** - Proteção em tempo real do sistema de ficheiros
- **Análise do computador** - Análise do computador a pedido
- **Proteção de acesso à Web**
- **Proteção de e-mail**

Os parâmetros do ThreatSense são especificamente otimizados para cada módulo e a respetiva modificação pode influenciar significativamente o funcionamento do sistema. Por exemplo, a alteração das definições para analisar sempre empacotadores em tempo real ou a ativação da heurística avançada no módulo de Proteção em tempo real do sistema de ficheiros pode resultar num sistema mais lento. Por conseguinte, recomendamos que mantenha os parâmetros predefinidos do ThreatSense inalterados para todos os módulos, à exceção da Análise do computador.

## Objetos

A seção **Objetos** permite definir os ficheiros a analisar quanto a infiltrações.

- **Hiperligações simbólicas** - (apenas Análise do computador) analisa ficheiros que contenham uma cadeia de caracteres de texto que seja interpretada e seguida pelo sistema operativo como um caminho para outro ficheiro ou diretório.
- **Ficheiros de e-mail** - (indisponível na Proteção em tempo real) analisa ficheiros de e-mail.
- **Caixas de correio** - (não disponível na Proteção em tempo real) analisa as caixas de correio do utilizador no sistema. A utilização incorreta desta opção pode resultar num conflito com o seu cliente de e-mail. Para saber mais sobre as vantagens e desvantagens desta opção, leia o seguinte [artigo da base de dados de conhecimento](#).
- **Arquivos compactados** - (não disponível na Proteção em tempo real) analisa ficheiros em arquivos compactados (.rar, .zip, .arj, .tar ,etc.).
- **Arquivos compactados de auto-extração** - (não disponível na Proteção em tempo real) analisa ficheiros

incluídos em arquivos compactados de auto-extração.

- **Empacotadores em tempo real** - ao contrário dos tipos de arquivo padrão, os empacotadores em tempo real são descompactados na memória. Quando esta opção está selecionada, os empacotadores estáticos padrão (por exemplo, UPX, yoda, ASPack, FGS) também são analisados.

## Opções

Na secção **Opções**, pode seleccionar os métodos utilizados durante uma análise do sistema. As opções disponíveis são:

- **Heurística** – A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detetar novos softwares maliciosos, que não existiam anteriormente.
- **Heurística avançada** – A heurística avançada é constituída por um algoritmo heurístico exclusivo, desenvolvido pela ESET, otimizado para a detecção de worms e cavalos de troia informáticos escritos em linguagens de programação de elevado nível. A capacidade de detecção do programa é significativamente superior devido à heurística avançada.

## Limpeza

As definições de limpeza determinam o modo como a análise limpa os ficheiros infetados. Existem 3 níveis de limpeza:

- **Sem limpeza** – Os ficheiros infetados não são limpos automaticamente. O programa irá apresentar uma janela de aviso e permitir-lhe escolher uma ação.
- **Limpeza padrão** – O programa tentará limpar ou eliminar automaticamente um ficheiro infetado. Se não for possível seleccionar a ação correta automaticamente, o programa irá possibilitar-lhe escolher as ações a seguir. A possibilidade de escolher as ações a seguir também será apresentada se não for possível concluir uma ação predefinida.
- **Limpeza rigorosa** – O programa irá limpar ou eliminar todos os ficheiros infetados (incluindo os arquivos compactados). As únicas exceções são os ficheiros do sistema. Se não for possível limpar um ficheiro, receberá uma notificação e ser-lhe-á pedido que selecione o tipo de ação a tomar.

Aviso: No modo de limpeza Padrão, os arquivos compactados serão eliminado na íntegra apenas se todos os ficheiros do arquivo compactado estiverem infetados. Se um arquivo compactado incluir ficheiros legítimos e ficheiros infetados, o mesmo não será eliminado. Se, no modo de Limpeza rigorosa, for detetado um ficheiro do arquivo compactado infetado, o arquivo compactado será eliminado na íntegra, mesmo se existirem ficheiros limpos.



#### Análise de arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão eliminados na íntegra apenas se todos os ficheiros do arquivo compactado estiverem infetados. Se um arquivo compactado incluir ficheiros legítimos e ficheiros infetados, o mesmo não será eliminado. Se, no modo de Limpeza rigorosa, for detetado um ficheiro do arquivo compactado infetado, o arquivo compactado será eliminado na íntegra, mesmo se existirem ficheiros limpos.

## Exclusões

Uma extensão é a parte do nome de um ficheiro delimitada por um ponto final. A extensão define o tipo e o conteúdo do ficheiro. Esta secção de configuração de parâmetros do ThreatSense permite definir os tipos de ficheiros a excluir da análise.

Por predefinição, todos os ficheiros são analisados, independentemente das respetivas extensões. Qualquer extensão pode ser adicionada à lista de ficheiros excluídos da análise. Com os botões + e -, pode ativar ou desativar a análise de extensões específicas.

A exclusão de ficheiros da análise é por vezes necessária caso a análise de determinados tipos de ficheiros impeça o funcionamento correto do programa. Por exemplo, poderá ser aconselhável excluir os ficheiros *log*, *cfg* e *tmp*. O formato de introdução de extensões de ficheiros correto é o seguinte:

*log*

*cfg*

*tmp*

## Limites

A secção **Limites** permite especificar o tamanho máximo de objetos e os níveis de arquivos compactados aninhados a analisar:

- **Tamanho máximo:** Define o tamanho máximo dos objetos a analisar. Assim que o tamanho máximo estiver definido, o módulo antivírus irá analisar apenas objetos com um tamanho inferior ao especificado. Esta opção deverá ser alterada apenas por utilizadores avançados que tenham motivos específicos para excluir objetos maiores da análise.
- **Tempo máximo da análise:** Define o tempo máximo designado para a análise de um objeto. Se um valor definido pelo utilizador for introduzido aqui, o módulo antivírus interromperá a análise de um objeto depois de decorrido o período especificado, independentemente de a análise ter ou não terminado.
- **Nível de compactação de ficheiros:** Especifica a profundidade máxima da análise de arquivos compactados aninhados. Não recomendamos que altere o valor predefinido de 10; em circunstâncias normais, não haverá motivo para modificá-lo. Se a análise for encerrada prematuramente devido ao número de arquivos compactados aninhados, o arquivo permanecerá sem verificação.

- **Tamanho máximo do ficheiro:** Esta opção permite especificar o tamanho máximo de ficheiro dos arquivos incluídos em arquivos compactados (quando são extraídos) a analisar. Se a análise for encerrada prematuramente devido a este limite, o arquivo compactado permanecerá sem verificação..

## Outros

### Ativar otimização inteligente

Com a Otimização Inteligente ativada, as definições são otimizadas para garantir o nível mais eficiente de análise, sem comprometer a respetiva velocidade. Os diversos módulos de proteção efetuam a análise de maneira inteligente, utilizando diferentes métodos de análise. A Otimização inteligente não é definida de modo rígido no produto. A equipa de desenvolvimento ESET está a implementar continuamente novas alterações que vão sendo integradas no ESET Cyber Security Pro através de atualizações regulares. Se a Otimização inteligente estiver desativada, apenas as definições configuradas pelo utilizador no núcleo do ThreatSense do módulo em questão serão aplicadas durante a realização de uma análise.

### Analisar fluxos dados alternativos (apenas a análise a pedido)

Os fluxos de dados alternativos utilizados pelo sistema de ficheiros são associações de ficheiros e pastas invisíveis às técnicas comuns de análise. Muitas infiltrações tentam evitar a deteção, disfarçando-se de fluxos de dados alternativos.

## Foi detetada uma infiltração

As infiltrações podem atingir o sistema a partir de vários pontos de entrada: páginas Web, pastas partilhadas, e-mail ou dispositivos de computador amovíveis (USB, discos externos, CDs, DVDs, etc.).

Se o computador estiver a apresentar sinais de infeção por malware, por exemplo, estiver mais lento, bloquear com frequência, etc., recomendamos que siga os seguintes passos:

1. Clique em **Análise do computador**.
2. Clique em **Análise inteligente** (para obter mais informações, consulte a secção [Análise inteligente](#)).
3. Após a análise ter terminado, reveja o relatório para verificar o número de ficheiros verificados, infetados e limpos.

Se pretende analisar apenas uma determinada parte do disco, clique em **Análise personalizada** e selecione os alvos a analisar quanto a vírus.

Como exemplo geral de como as infiltrações são tratadas pelo ESET Cyber Security Pro, suponha que uma infiltração é detetada pelo monitor do sistema de ficheiros em tempo real, que utiliza o nível de limpeza padrão.

A proteção em tempo real tentará limpar ou eliminar o ficheiro. Se não houver uma ação predefinida disponível para o módulo de proteção em tempo real, ser-lhe-á pedido que selecione uma opção numa janela de alertas. Geralmente as opções **Limpar**, **Eliminar** e **Nenhuma ação** estão disponíveis. A seleção da opção **Nenhuma ação** não é recomendada, visto que os ficheiro(s) infetado(s) se mantêm no estado não infetado. Esta opção destina-se a situações em que tenha a certeza de que o ficheiro é inofensivo e foi detetado por engano.

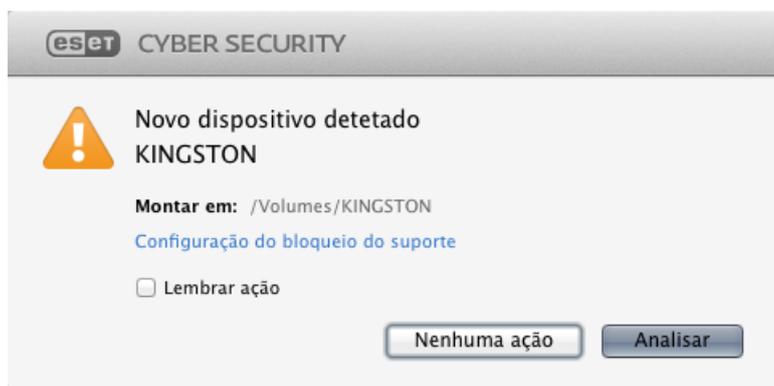
**Limpeza e eliminação** - Aplique a limpeza se um ficheiro tiver sido atacado por um vírus que anexou a esse ficheiro um código malicioso. Se esse for o caso, tente primeiro limpar o ficheiro infetado para restaurá-lo para o respetivo estado original. Se o ficheiro for constituído exclusivamente por código malicioso, o mesmo será eliminado.



**Eliminação de ficheiros em arquivos compactados** - No modo de limpeza padrão, os arquivos compactados serão eliminados apenas se contiverem ficheiros infetados e nenhum ficheiro limpo. Por outras palavras, os arquivos compactados não serão eliminados se contiverem também ficheiros limpos inofensivos. No entanto, tenha cuidado quando realizar uma análise de **Limpeza rigorosa**. Com este tipo de limpeza, o arquivo será eliminado se contiver, pelo menos, um ficheiro infetado, independentemente do estado dos restantes ficheiros incluídos no arquivo compactado.

## Análise e bloqueio do suporte amovível

O ESET Cyber Security Pro pode executar uma análise a pedido dos dispositivos multimédia amovíveis inseridos (CD, DVD, USB, dispositivo iOS, etc.).



O suporte amovível pode conter código malicioso e colocar o seu computador em risco. Para bloquear o suporte amovível, clique em **Configuração do bloqueio do suporte** (consulte a imagem acima) ou, no menu principal, clique em **Configurar > Introduzir preferências da aplicação... > Suporte** a partir da janela principal do programa e selecione **Ativar bloqueio de suporte amovível**. Para permitir o acesso a determinados tipos de suporte, desmarque os volumes de suporte pretendidos.



#### Acesso ao CD-ROM

Se pretender conceder a acesso a uma unidade de CD-ROM externa ligada ao seu computador através de um cabo USB, desmarque a opção **CD-ROM**.

## Antiphishing

O termo phishing define uma atividade criminosa que utiliza a engenharia social (a manipulação de utilizadores de forma a obter informações confidenciais). O phishing é utilizado, muitas vezes, para a obtenção de acesso a dados confidenciais, nomeadamente números de contas bancárias, números de cartões de crédito, PINs ou nomes de utilizador e palavras-passe.

Recomendamos que mantenha o Antiphishing (**Configurar > Introduzir preferências da aplicação... > Proteção Antiphishing**) ativado. Os potenciais ataques de phishing provenientes de Web sites ou domínios perigosos serão bloqueados e será apresentada uma notificação de aviso com a informação do ataque.

## Firewall

A firewall controla todo o tráfego de rede para e a partir do sistema ao permitir ou negar ligações de rede individuais com base em regras de filtragem especificadas. Fornece proteção contra ataques de computadores remotos e ativa o bloqueamento de alguns serviços. Também fornece proteção antivírus para protocolos HTTP, POP3 e IMAP.

A configuração da firewall pode ser encontrada em **Configuração > Firewall**. Permite-lhe ajustar o modo de filtragem, regras e definições detalhadas. Também pode aceder a definições mais detalhadas do programa a

partir daqui.

Se mudar **Bloquear todo o tráfego de rede: desligar rede** para **ATIVADO**, todas as comunicações de entrada e saída serão bloqueadas pela firewall. Utilize esta opção apenas se suspeitar de riscos de segurança críticos que exijam que o sistema seja desligado da rede.

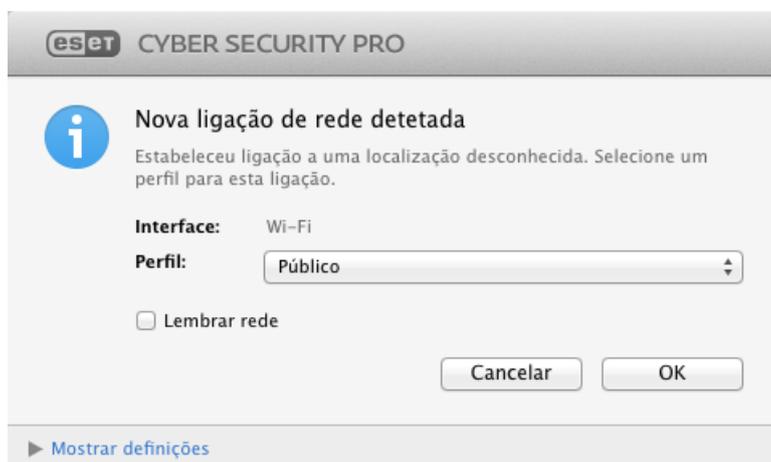
## Modos de filtragem

Estão disponíveis três modos de filtragem para a firewall do ESET Cyber Security Pro. As definições dos modos de filtragem podem ser encontradas nas preferências do ESET Cyber Security Pro (prima *cmd+*) > **Firewall**. O comportamento da firewall é alterado com base no modo selecionado. Os modos de filtragem também influenciam o nível de interação necessário por parte do utilizador.

**Todo tráfego bloqueado** - todas as ligações de entrada e saída serão bloqueadas.

**Auto com exceções** - o modo predefinido. Este modo é adequado para utilizadores que preferem uma utilização fácil e cómoda da firewall sem necessidade de definir regras. O modo automático permite que o tráfego de saída padrão para o sistema em questão e bloqueia todas as ligações não iniciadas a partir o lado da rede. Também pode adicionar regras personalizadas, definidas pelo utilizador.

**Modo interativo** – permite-lhe construir uma configuração personalizada da sua firewall. Quando é detetada uma comunicação e nenhuma das regras existentes se aplica a essa comunicação, é apresentada uma caixa de diálogo a informar sobre uma ligação desconhecida. A caixa de diálogo dá a opção de permitir ou negar a comunicação e a decisão de permitir ou negar pode ser lembrada com uma nova regra para a firewall. Se escolher criar uma nova regra neste momento, todas as futuras ligações deste tipo serão permitidas ou bloqueadas de acordo com a regra.



Para registar informações detalhadas sobre todas as ligações bloqueadas num relatório, selecione **Registar todas as ligações bloqueadas**. Para rever os relatórios da firewall, no menu principal, clique em **Ferramentas > Relatórios** e selecione **Firewall** no menu pendente **Relatório**.

## Regras da firewall

As regras da firewall são um conjunto de condições utilizadas para testar todas as ligações de rede e determinar as ações apropriadas a estas condições. Com as regras da firewall, pode definir o tipo de ação a tomar se for estabelecida uma ligação definida pela regra.

As ligações de entrada são iniciadas por um computador remoto que tenta estabelecer uma ligação com o sistema local. As ligações de saída trabalham da forma oposta – o sistema local contacta um computador remoto.

Se for detetada uma nova comunicação desconhecida, tem de considerar cuidadosamente se a permite ou nega. As ligações não solicitadas, não seguras ou desconhecidas representam um risco de segurança para o sistema. Se for estabelecida uma ligação desse género, recomendamos que preste particular atenção ao computador remoto e à aplicação que estão a tentar ligar-se ao seu computador. Muitas infiltrações tentam obter e enviar dados privados ou transferir aplicações maliciosas para estações de trabalho host. A firewall permite-lhe detetar e terminar essas ligações.

Por predefinição, as aplicações assinadas pela Apple podem aceder automaticamente à rede. Se pretender desativar esta opção, desmarque **Permitir que software assinado pela Apple aceda automaticamente à rede**.

## Criação de novas regras

O separador **Regras** contém uma lista de todas as regras aplicadas ao tráfego gerado por aplicações individuais. As regras são adicionadas automaticamente de acordo com as respostas do utilizador a uma nova comunicação.

1. Para criar uma nova regra, clique em **Adicionar**, introduza um nome para a regra e arraste e largue o ícone da aplicação no campo em branco ou clique em **Procurar** para procurar o programa na pasta */Applications*. Se aplicar a regra a todas as aplicações instaladas no seu computador, selecione a opção **Todas as aplicações**.
2. Na próxima janela, especifique a **Ação** (permitir ou negar a comunicação entre a aplicação e rede selecionadas) e **Direção** da comunicação (entrada, saída ou ambas). Pode gravar todas as comunicações relacionadas com esta regra num relatório. Para tal, selecione a opção **Registar regra**. Para rever os relatórios, clique em **Ferramentas > Relatórios** no menu principal do ESET Cyber Security Pro e selecione **Firewall** no menu pendente **Relatório**.
3. Na secção **Protocolo/Portas**, selecione o protocolo através do qual a aplicação comunica e os números de porta (se o protocolo TCP ou UDP estiver selecionado). A camada do protocolo de transporte fornece uma transferência de dados segura e eficiente.

4. Por último, especifique os critérios de **Destino** (endereço IP, intervalo, subrede, ethernet ou Internet) para a regra.

## Zonas da firewall

Uma zona representa um conjunto de endereços de rede que cria um grupo lógico. A cada endereço num determinado grupo são atribuídas regras semelhantes definidas centralmente para todo o grupo.

Estas zonas podem ser criadas clicando no botão **Adicionar....** Introduza um **Nome** e **Descrição** (opcional) para a zona, selecione um perfil ao qual irá pertencer esta zona e adicione um endereço IPv4/IPv6, intervalo de endereço, subrede, rede Wi-Fi ou uma interface.

## Perfis da firewall

Os **Perfis** permitem-lhe controlar o comportamento da firewall do ESET Cyber Security Pro. Ao criar ou editar uma regra da firewall, pode atribuí-la a um perfil específico. Quando seleciona um perfil, apenas são aplicadas as regras globais (nenhum perfil especificado) e as regras que foram atribuídas a esse perfil. Pode criar vários perfis com diferentes regras atribuídas para alterar facilmente o comportamento da firewall.

## Relatórios da firewall

A firewall do ESET Cyber Security Pro guarda todos os eventos importantes num relatório. Para aceder aos relatórios da firewall, no menu principal, clique em **Ferramentas > Relatórios** e selecione **Firewall** no menu pendente **Relatório**.

Os relatórios são uma ferramenta valiosa para detetar erros e revelar intrusões no seu sistema. Os relatórios da firewall da ESET contêm os seguintes dados:

- Data e hora do evento
- Nome do evento
- Origem
- Endereço de rede alvo
- Protocolo de comunicação de rede
- Regra aplicada
- Aplicação envolvida
- Utilizador

Uma análise minuciosa destes dados pode ajudar a detetar tentativas de comprometer a segurança do sistema. Muitos outros fatores indicam possíveis riscos de segurança e podem ser protegidos pela firewall, tais como: ligações frequentes de localizações desconhecidas, várias tentativas de estabelecer ligações, aplicações desconhecidas a comunicar ou números de porta pouco habituais.

## Proteção da Web e de e-mails

Para aceder à Proteção da Web e de e-mails a partir do menu principal, clique em **Configurar > Web e e-mail**. A partir daqui, também pode aceder a definições detalhadas de cada módulo, clicando em **Configurar....**

- **Proteção de acesso à Web** - monitoriza comunicações HTTP entre navegadores e servidores remotos.
- **Proteção de cliente de e-mail** - fornece controlo da comunicação por e-mail recebida via protocolos IMAP e POP3.
- **Proteção antiphishing** - bloqueia potenciais ataques de phishing provenientes de Web sites ou domínios.

## Proteção Web

A proteção de acesso à Web monitoriza comunicações entre navegadores e servidores remotos em conformidade com as regras HTTP (Protocolo de Transferência de Hipertexto).

Para conseguir a Filtragem da Web, defina [os números de porta para comunicação HTTP](#) e/ou [Endereços URL](#).

## Portas

No separador **Portas**, pode definir os números de porta utilizados para comunicação HTTP. Por predefinição, os números de porta 80, 8080 e 3128 estão predefinidos.

## Listas de URL

A secção **Listas de URL** permite-lhe especificar endereços HTTP para bloquear, permitir ou excluir da verificação. Os Web sites na lista de endereços bloqueados não estarão acessíveis. Os Web sites na lista de endereços excluídos são acedidos sem que sejam analisados quanto a código malicioso.

Para permitir o acesso apenas aos endereços URL indicados na lista **URL permitido**, seleccione a opção **Restringir endereços URL**.

Para ativar uma lista, seleccione **Ativado** junto ao nome da lista. Se pretender ser notificado quando introduz um endereço da lista atual, seleccione **Notificado**.

Em qualquer lista, é possível utilizar os símbolos especiais \* (asterisco) e ? (ponto de interrogação). O asterisco substitui qualquer cadeia de caracteres e o ponto de interrogação substitui qualquer símbolo. Deve prestar-se particular atenção ao especificar endereços excluídos, porque a lista deve conter apenas endereços de confiança e seguros. De forma semelhante, é necessário garantir que os símbolos \* e ? são utilizados corretamente nesta lista.

## Proteção de e-mail

A proteção de e-mail fornece controlo das comunicações por e-mail recebidas via protocolos POP3 e IMAP. Ao examinar mensagens a receber, o ESET Cyber Security Pro utiliza todos os métodos de análise avançados incluídos no mecanismo de análise ThreatSense. A análise de comunicações de protocolo POP3 e IMAP é independente do cliente de e-mail utilizado.

**Mecanismo ThreatSense: Configuração** – a avançada configuração da análise permite-lhe configurar alvos de análise, métodos de deteção, etc. Clique em **Configurar** para apresentar a janela de configuração detalhada da análise.

**Anexar mensagens de marca ao rodapé do e-mail** – após a análise de um e-mail, é possível anexar à mensagem uma notificação com os resultados da análise. As mensagens de marca são uma ferramenta útil, mas não devem ser utilizadas como a determinação final da segurança das mensagens, uma vez que estas podem ser omitidas em mensagens HTML problemáticas e podem ser adulteradas por algumas ameaças. As opções disponíveis são:

- **Nunca** – não serão adicionadas mensagens de marca a um e-mail
- **Apenas para e-mail infetado** – apenas e-mail com malware serão marcadas como verificadas
- **Para todos os e-mails analisados** – todos os e-mails analisados serão anexados com mensagens de marca

**Anexar nota ao assunto do e-mail infetado recebido e lido** – seleccione esta caixa de verificação se pretender que a proteção de e-mail inclua um aviso de ameaça no e-mail infetado. Esta funcionalidade permite uma filtragem simples de e-mails infetados. Também aumenta o nível de credibilidade para o destinatário e, no caso de ser detetada uma infiltração, disponibiliza informações valiosas sobre o nível de ameaça de um determinado e-mail ou remetente.

**Modelo adicionado ao assunto de e-mail infetado** – edite este modelo para modificar o formato do prefixo do assunto de um e-mail infetado.

- %avstatus% - Adiciona o estado de infeção do e-mail (por exemplo: limpo, infetado...)
- %virus% - Adiciona o nome da ameaça
- %aspmstatus% - Altera o assunto com base no resultado da análise antispam
- %product% - Adiciona o nome do seu produto ESET (neste caso: ESET Cyber Security Pro)
- %product\_url% - Adiciona a ligação do site da ESET ([www.eset.com](http://www.eset.com))

Na parte inferior desta janela, também pode ativar/desativar a verificação de comunicação por e-mail recebida via protocolos POP3 e IMAP. Para saber mais sobre este assunto, consulte os tópicos seguintes:

- [Verificação de protocolo POP3](#)
- [Verificação de protocolo IMAP](#)

## Verificação de protocolo POP3

O protocolo POP3 é o protocolo mais comum utilizado para receber comunicações por e-mail numa aplicação do cliente de e-mail. O ESET Cyber Security Pro proporciona proteção para este protocolo independentemente do cliente de e-mail utilizado.

O módulo de proteção que proporciona este controlo é automaticamente iniciado na inicialização do sistema e fica então ativo na memória. Certifique-se de que o módulo está ativado para a filtragem de protocolo para funcionar corretamente; a verificação do protocolo POP3 é executada automaticamente sem necessidade de reconfigurar o cliente de e-mail. Por predefinição, todas as comunicações na porta 110 são analisadas, mas é possível adicionar outras portas de comunicação caso seja necessário. Os números de porta são delimitados por uma vírgula.

Se a opção **Ativar verificação de protocolo POP3** estiver selecionada, todo o tráfego do POP3 é monitorizado quanto a software malicioso.

## Verificação de protocolo IMAP

O Protocolo de Acesso a Mensagens na Internet (IMAP) é outro protocolo Internet para recuperação de e-mail. O IMAP tem algumas vantagens em relação ao POP3, por exemplo, vários clientes podem ligar-se em simultâneo à mesma caixa de correio e manter as informações do estado da mensagem como, por exemplo, se a mensagem foi ou não lida, respondida ou eliminada. O ESET Cyber Security Pro proporciona proteção para este protocolo, independentemente do cliente de e-mail utilizado.

O módulo de proteção que proporciona este controlo é automaticamente iniciado na inicialização do sistema e fica então ativo na memória. Certifique-se de que a Verificação de protocolo IMPA se encontra ativada para que o módulo funcione corretamente; o controlo do protocolo IMAP é executado automaticamente sem necessidade de reconfigurar o cliente de e-mail. Por predefinição, todas as comunicações na porta 143 são analisadas, mas é possível adicionar outras portas de comunicação caso seja necessário. Os números de porta são delimitados por uma vírgula.

Se **Ativar verificação de protocolo IMAP** estiver selecionado, todo o tráfego através do IMAP é monitorizado quanto a software malicioso.

# Controlo parental

A secção **Controlo parental** permite-lhe configurar as definições de Controlo parental, que fornecem aos pais ferramentas automatizadas para ajudar a proteger os seus filhos. O objetivo é evitar que crianças e jovens adultos acessem a páginas que contenham conteúdo inadequado ou prejudicial. O Controlo parental permite-lhe bloquear páginas Web que podem conter material potencialmente ofensivo. Além disso, os pais podem proibir o acesso até 27 categorias de Web site predefinidas.

As suas contas do utilizador estão listadas na janela **Controlo parental (Configurar > Introduzir preferências da aplicação... > Controlo parental)**. Selecione aquela que pretende utilizar para controlo parental. Para especificar um nível de proteção para a conta selecionada, clique em **Configurar...** . Para criar uma nova regra, clique em **Adicionar...** . Isso irá redirecioná-lo para a janela de contas do sistema macOS.

Na janela **Configuração do Controlo parental**, selecione um dos perfis predefinidos no menu pendente **Configurar perfil** ou copie a configuração parental de outra conta de utilizador. Cada perfil contém uma lista modificada de categoria permitidas. Se uma categoria estiver marcada, esta é permitida. Movimentar o rato sobre uma categoria irá mostrar-lhe uma lista de páginas Web que pertencem a essa categoria.

Para modificar a lista de **Páginas Web permitidas e bloqueadas**, clique em **Configurar...** na parte inferior de uma janela e adicione um nome de domínio na lista pretendida. Não escreva *http://*. Não é necessário utilizar caracteres universais (\*). Se introduzir apenas um nome de domínio, todos os subdomínios serão incluídos. Por exemplo, se adicionar *google.com* à **Lista de páginas Web permitidas**, todos os subdomínios (*mail.google.com*, *news.google.com*, *maps.google.com* etc.) serão permitidos.



## Regras

Bloquear ou permitir uma página Web específica pode ser mais preciso do que bloquear ou permitir uma categoria completa de páginas Web.

# Atualizar

É necessário atualizar o ESET Cyber Security Pro com regularidade para manter o nível máximo de segurança. O módulo de atualização garante que o programa está sempre atualizado através da transferência dos módulos de deteção mais recentes.

Clique em **Atualizar** no menu principal para ver o estado atual da atualização do ESET Cyber Security Pro, incluindo o dia e a hora da última atualização bem-sucedida, e se será necessário efetuar uma atualização. Para iniciar o processo de atualização manualmente, clique em **Atualizar módulos**.

Em circunstâncias normais, quando as atualizações são transferidas corretamente, é apresentada a mensagem **Atualização não necessária – os módulos instalados são atuais** na janela Atualizar. Se não for possível atualizar os módulos, recomendamos que verifique as [definições de atualização](#). Regra geral, este erro ocorre devido à introdução incorreta dos dados de autenticação (Nome de utilizador e Palavra-passe) ou devido à configuração incorreta das [definições de ligação](#).

A janela Atualizar também contém informações sobre o número da versão do Motor de deteção. O número da versão está associado à página Web da ESET que lista as informações de atualização do Motor de deteção.

## Configuração da atualização

Para eliminar todos os dados de atualização armazenados temporariamente, clique em **Limpar** junto a **Limpar cache de atualização**. Utilize esta opção se estiver com dificuldades durante a atualização.

## Opções avançadas

Para desativar as notificações apresentadas após cada atualização bem sucedida, selecione **Não mostrar notificação sobre atualizações bem sucedidas**.

Ative **Modo de teste** para transferir módulos em desenvolvimento que ainda estejam em fases finais de teste. O Modo de teste inclui muitas vezes correções para problemas de produtos. **Atualização diferida** transfere atualizações algumas horas após serem disponibilizadas, para garantir que os clientes não irão receber atualizações até se confirmar de que estas estão isentas de quaisquer problemas não controlados.

O ESET Cyber Security Pro regista instantâneos dos módulos de deteção e do programa para utilizar com a funcionalidade **Inversão de atualização**. Mantenha **Criar instantâneos de ficheiros da atualização** ativado para que o ESET Cyber Security Pro registe estes instantâneos automaticamente. Se suspeitar que uma nova atualização dos módulos de deteção e /ou do programa possa ser instável ou estar corrompida, pode utilizar a funcionalidade de inversão para reverter para uma versão anterior e desativar as atualizações durante um período estabelecido. Em alternativa, pode ativar as atualizações anteriormente desativadas, caso as tenha adiado indefinidamente. Quando utilizar a funcionalidade Inversão de atualização para reverter para uma versão anterior, utilize o menu suspenso **Definir período de suspensão para** para especificar o período durante o qual pretende suspender as atualizações. Se selecionar **até à revogação**, as atualizações normais não serão retomadas até as restaurar manualmente. Tenha cuidado quando definir o período de suspensão das atualizações.

**Definir a idade máxima do motor de deteção automaticamente** – permite-lhe definir o tempo máximo (em dias) após o qual os módulos de deteção serão dados como desatualizados. O valor predefinido é de 7 dias.

# Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Atualizar** no menu principal e, em seguida, clicando em **Atualizar módulos**.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas > Agenda**. Por predefinição, as seguintes tarefas estão ativadas no ESET Cyber Security Pro:

- **Atualização automática de rotina**
- **Atualizar automaticamente após início de sessão do utilizador**

Cada uma das tarefas de atualização pode ser modificada para satisfazer as suas necessidades. Além das tarefas de atualização predefinidas, pode criar novas tarefas de atualização com uma configuração definida pelo utilizador. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a secção [Agenda](#).

## Atualizar o ESET Cyber Security Pro para uma nova versão

Para obter a máxima proteção, é importante utilizar a compilação mais recente do ESET Cyber Security Pro. Para verificar se existe uma nova versão, clique em **Início** no menu principal. Se estiver disponível uma nova compilação, será apresentada uma mensagem. Clique em **Saber mais...** para apresentar uma nova janela com o número da versão da nova compilação e o registo de alterações.

Clique em **Sim** para transferir a compilação mais recente ou clique em **Agora não** para fechar a janela e transferir a atualização mais tarde.

Se clicar em **Sim**, o ficheiro será transferido para a sua pasta de transferências (ou para a pasta predefinida definida pelo navegador). Quando a transferência do ficheiro terminar, inicie o ficheiro e siga as instruções de instalação. O seu Nome de utilizador e Palavra-passe serão automaticamente transferidos para a nova instalação. Recomenda-se que verifique regularmente a existência de atualizações, especialmente se instalar o ESET Cyber Security Pro através de um CD/DVD.

## Atualizações do sistema

A funcionalidade de atualizações do sistema macOS é um componente importante concebido para proteger os utilizadores contra software malicioso. Para obter a máxima segurança, recomendamos que instale estas

atualizações assim que elas ficarem disponíveis. O ESET Cyber Security Pro notificará-lo-á sobre atualizações em falta de acordo com o nível especificado. Pode ajustar a disponibilidade das notificações de atualização em **Configurar > Introduzir preferências da aplicação ...** (ou prima *cmd+*) > **Alertas e notificações > Configurar...** alterando as opções **Condições de apresentação** junto a **Atualizações do sistema operativo**.

- **Mostrar todas as atualizações** - será apresentada uma notificação sempre que faltar uma atualização do sistema
- **Mostrar apenas recomendadas** - será notificado apenas sobre atualizações recomendadas

Se não pretender ser notificado sobre atualizações em falta, desmarque a caixa de verificação junto de **Atualizações do sistema operativo**.

A janela de notificação fornece uma visão geral das atualizações disponíveis para o sistema operativo macOS e das aplicações atualizadas através da ferramenta nativa do macOS, Atualizações de software. Pode executar a atualização diretamente a partir da janela de notificação ou a partir da secção **Início** do ESET Cyber Security Pro, clicando em **Instalar a atualização em falta**.

A janela de notificação inclui o nome, a versão, o tamanho e as propriedades (sinalizadores) da aplicação, assim como informações adicionais sobre atualizações disponíveis. A coluna Sinalizadores inclui as seguintes informações:

- **[recomendado]** - o fabricante do sistema operativo recomenda a instalação desta atualização para aumentar a segurança e a estabilidade do sistema
- **[reiniciar]** - é necessário reiniciar o computador após a instalação
- **[encerrar]** - é necessário encerrar e voltar a ligar o computador após a instalação

A janela de notificação mostra as atualizações obtidas pela ferramenta da linha de comandos denominada "softwareupdate". As atualizações obtidas por esta ferramenta podem ser diferentes das atualizações apresentadas pela aplicação "Atualizações de software". Se pretender instalar todas as atualizações disponíveis apresentadas na janela "Atualizações do sistema em falta", assim como as atualizações não apresentadas pela aplicação "Atualizações de software", tem de utilizar a ferramenta da linha de comandos "softwareupdate". Para saber mais sobre esta ferramenta, leia o manual de "softwareupdate", escrevendo `man softwareupdate` numa Janela de terminal. Esta ação é recomendada apenas para utilizadores avançados.

## Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para utilizadores avançados.

# Relatórios

Os relatórios contêm informações sobre os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detetadas. O registo em relatório atua como uma ferramenta essencial na análise do sistema, na deteção de ameaças e na resolução de problemas. O registo em relatório é realizado ativamente em segundo plano, sem interação do utilizador. As informações são registadas com base nas definições atuais de detalhe do relatório. É possível ver mensagens de texto e relatórios diretamente do ambiente do ESET Cyber Security Pro, bem como arquivar relatórios.

Os relatórios podem ser acedidos a partir do menu principal do ESET Cyber Security Pro, clicando em **Ferramentas > Relatórios**. Selecione o tipo de relatório pretendido, utilizando o menu pendente **Relatório** na parte superior da janela. Estão disponíveis os seguintes relatórios:

1. **Ameaças detetadas** – Utilize esta opção para ver todas as informações sobre eventos relacionados com a deteção de infiltrações.
2. **Eventos** - esta opção destina-se a ajudar os administradores do sistema e os utilizadores a resolverem problemas. Todas as ações importantes executadas pelo ESET Cyber Security Pro são registadas nos relatórios de eventos.
3. **Análise do computador** - os resultados de todas as análises concluídas são apresentados neste relatório. Clique duas vezes em qualquer entrada para ver os detalhes da respetiva Análise do computador a pedido.
4. **Parental** - lista de todas as páginas Web bloqueadas pelo Controlo parental.
5. **Firewall** - este relatório contém os resultados de todos os eventos relacionados com a rede.
6. **Web sites filtrados** - esta lista é útil no caso de pretender ver uma lista de Web sites que foram bloqueados pela Proteção de acesso à Web. Nestes relatórios, pode ver a hora, o URL, o estado, o endereço IP, o utilizador e a aplicação que abriu uma ligação para um Web site específico.

Em cada secção, as informações apresentadas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão **Copiar**.

## Manutenção de relatórios

A configuração de relatórios do ESET Cyber Security Pro pode ser acedida a partir da janela principal do programa. Clique em **Configurar > Introduzir preferências da aplicação** (ou prima *cmd+,*) > **Relatórios**. Pode especificar as seguintes opções para os relatórios:

- **Eliminar relatórios antigos automaticamente** - as entradas de relatórios anteriores ao número de dias especificado são automaticamente eliminadas (por predefinição, 90 dias)
- **Otimizar automaticamente relatórios** - ativa a desfragmentação automática de relatórios se a percentagem especificada de registos não utilizados foi ultrapassada (por predefinição, 25%)

Todas as informações relevantes apresentadas na interface gráfica do utilizador, mensagens de eventos e ameaças podem ser armazenadas em formatos de texto legível humano, tais como, texto simples ou CSV (Comma-separated values). Se pretender tornar estes ficheiros disponíveis para processamento através de ferramentas de outros fabricantes, seleccione a caixa de verificação junto a **Ativar registo para ficheiros de texto**.

Para definir uma pasta onde os relatórios serão guardados, clique em **Configurar** junto a **Opções avançadas**.

Com base nas opções seleccionadas em **Relatórios de texto: Editar**, pode guardar relatórios com as seguintes informações escritas:

- Eventos, tais como *Nome de utilizador e palavra-passe inválidos*, *Não é possível atualizar os módulos* etc. são gravados no ficheiro eventslog.txt
- Ameaças detetadas pela Análise na inicialização, Proteção em tempo real ou Análise do computador são armazenadas no ficheiro denominado threatslog.txt
- Os resultados de todas as análises concluídas são guardados no formato scanlog.NUMBER.txt
- Todos os eventos relacionados com a comunicação através da Firewall são gravados em firewalllog.txt

Para configurar os filtros para **Registos de relatórios de análise do computador predefinidos**, clique em **Editar** e seleccione/desmarque os tipos de relatórios, consoante necessário. Pode encontrar uma explicação mais detalhada sobre estes tipos de relatórios em [Filtragem de relatórios](#).

## Filtragem de relatórios

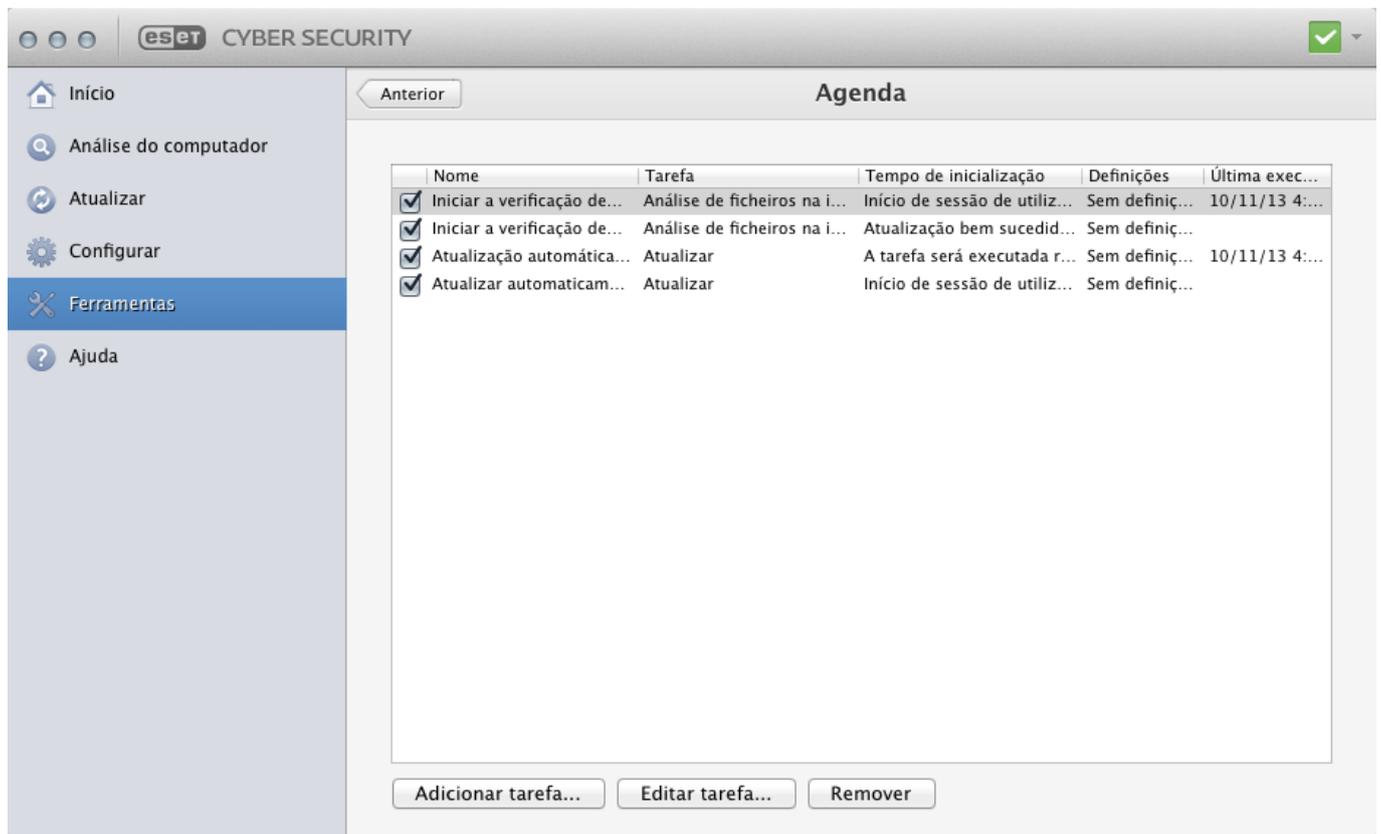
Regista em relatórios as informações de armazenamento sobre eventos importantes do sistema. A funcionalidade de filtragem de relatórios permite visualizar registos sobre um tipo específico de evento.

Os tipos de relatórios usados com frequência são listados a seguir:

- **Avisos críticos** - erros críticos do sistema (por exemplo, falha ao iniciar a proteção antivírus)
- **Erros** - mensagens de erro, como "*Erro ao transferir ficheiro*" e erros críticos
- **Avisos** - mensagens de aviso
- **Registos informativos** - mensagens informativas, incluindo atualizações bem sucedidas, alertas, etc.
- **Registos de diagnóstico** - informações necessárias para ajustar o programa e também todos os registos descritos acima.

# Agenda

Pode encontrar a **Agenda** no menu principal do ESET Cyber Security Pro em **Ferramentas**. A **Agenda** contém uma lista de todas as tarefas agendadas e propriedades de configuração, como a data e a hora predefinidas e o perfil de análise utilizado.



A Agenda gere e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e a hora, bem como os perfis especificados a utilizar durante a execução da tarefa.

Por predefinição, as seguintes tarefas agendadas são apresentadas na Agenda:

- Manutenção de relatórios (após a ativação da opção **Mostrar tarefas do sistema** na configuração da agenda)
- Análise de ficheiros na inicialização após início de sessão do utilizador
- Análise de ficheiros na inicialização após atualização bem sucedida dos módulos de deteção
- Atualização automática de rotina
- Atualizar automaticamente após início de sessão do utilizador

Para editar a configuração de uma tarefa agendada existente (tanto predefinida como definida pelo utilizador), CTRL +clique na tarefa que pretende modificar e seleccione **Editar** ou seleccione a tarefa e clique em **Editar tarefa**.

## Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique em **Adicionar tarefa...** ou faça CTRL+clique no campo em branco e seleccione **Adicionar...** no menu de contexto. Estão disponíveis cinco tipos de tarefas agendadas :

- Executar aplicação
- Atualizar
- Manutenção de relatórios
- Análise do computador a pedido
- Análise de ficheiros na inicialização do sistema



### Executar aplicação

Ao escolher **Executar aplicação**, pode executar programas como um utilizador do sistema denominado "nobody". As permissões para executar aplicações através da Agenda são definidas pelo macOS. Para alterar a predefinição do utilizador, escreva o nome de utilizador seguido de pontos pontos (:) à frente do comando. Também pode usar o utilizador **raiz** nesta funcionalidade.



### Exemplo: Executar tarefa como utilizador

Neste exemplo, iremos programar a aplicação da calculadora para iniciar à hora seleccionada como um utilizador denominado **UtilizadorUm**:

1. Na **Agenda**, seleccione **Adicionar tarefa**.
2. Escreva o nome da tarefa. Seleccione **Executar aplicação** como uma **Tarefa agendada**. Na janela **Executar tarefa**, seleccione **Uma vez** para executar esta tarefa uma única vez. Clique em **Seguinte**.
3. Clique em Procurar e seleccione a aplicação Calculadora.
4. Escreva **UtilizadorUm:** antes do caminho da aplicação (UtilizadorUm:'/Applications/Calculator.app/Contents/MacOs/Calculator') e clique em **Seguinte**.
5. Seleccione uma hora para executar a tarefa e clique em **Seguinte**.
6. Seleccione uma opção alternativa caso não seja possível executar a tarefa e clique em **Seguinte**.
7. Clique em **Concluir**.
8. O ESET Scheduler irá iniciar a aplicação Calculadora à hora seleccionada.



Exemplo: Tarefa de atualização

Pode analisar diretórios como proprietário do diretório:

1. A partir do menu pendente **Tarefa agendada**, selecione **Atualizar**.
2. Introduza o nome da tarefa no campo **Nome da tarefa**.
3. Selecione a frequência da tarefa a partir do menu pendente **Executar a tarefa**. Com base na frequência selecionada, ser-lhe-á solicitado que especifique diferentes parâmetros de atualização. Se seleccionar **Definido pelo utilizador**, ser-lhe-á solicitado que especifique a data/hora em formato cron (consulte a secção [Criar tarefa definida pelo utilizador](#) para obter mais informações).
4. No passo seguinte, defina a ação a realizar se a tarefa não puder ser realizada ou concluída à hora agendada.
5. No último passo, é apresentada uma janela de resumo com informações sobre a tarefa atualmente agendada. Clique em **Concluir**. A nova tarefa agendada será adicionada à lista de tarefas atualmente agendadas.

Por predefinição, o ESET Cyber Security Pro inclui tarefas agendadas predefinidas para garantir uma funcionalidade correta do produto. Estas tarefas não devem ser alteradas e estão ocultas por predefinição. Para as tornar visíveis, no menu principal, clique em **Configuração > Introduzir preferências da aplicação...** (ou prima *cmd+,*) > **Agenda** e selecione **Mostrar tarefas do sistema**.

## Analisar como proprietário de diretório

Pode analisar os diretórios como proprietário de diretório:

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

Também pode analisar a pasta /tmp como utilizador com sessão iniciada:

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

## Criação de tarefas definidas pelo utilizador

A data e a hora da tarefa **Definida pelo utilizador** têm de ser introduzidas no formato cron estendido por ano (uma cadeia composta por 6 campos separados por um espaço em branco):

```
minuto(0-59) hora(0-23) dia do mês(1-31) mês(1-12) ano(1970-2099) dia da  
semana(0-7) (Domingo = 0 ou 7)
```

Exemplo:

Caracteres especiais suportados nas expressões cron:

- asterisco (\*) - a expressão corresponderá a todos os valores do campo; por exemplo, asterisco no 3.º campo (dia do mês) significa todos os dias
- hífen (-) - define intervalos; por exemplo, 3-9
- vírgula (,) - separa itens de uma lista; por exemplo, 1,3,7,8
- barra (/) - define incrementos de intervalos; por exemplo, 3-28/5 no 3.º campo (dia do mês) significa 3.º dia do mês e depois de 5 em 5 dias.

Os nomes dos dias (Monday-Sunday) e os nomes dos meses (January-December) não são suportados.



#### Executar comandos

Se definir o dia do mês e o dia da semana, o comando será executado apenas quando ambos os campos corresponderem.

## Quarentena

O principal objetivo da quarentena é armazenar os ficheiros infetados em segurança. Os ficheiros devem ser colocados em quarentena se não for possível limpá-los, se não for seguro nem aconselhável eliminá-los ou se estiverem a ser falsamente detetados pelo ESET Cyber Security Pro.

Pode optar por colocar qualquer ficheiro em quarentena. Recomenda-se a colocação de um ficheiro em quarentena se se comportar de modo suspeito, mas não for detetado pela análise antivírus. Os ficheiros em quarentena podem ser enviados para análise para o Threat Lab da ESET.

Os ficheiros armazenados na pasta de quarentena podem ser visualizados numa tabela que apresenta a data e a hora da quarentena, o caminho da localização original do ficheiro infetado, o tamanho do ficheiro em bytes, o motivo (por exemplo, adicionado pelo utilizador...) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas infiltrações). A pasta de quarentena com ficheiros colocados em quarentena () permanece no sistema mesmo depois da desinstalação do ESET Cyber Security Pro. Os ficheiros em quarentena são armazenados num formato encriptado e podem ser restaurados novamente após a instalação do ESET Cyber Security Pro.

## Colocação de ficheiros em quarentena

O ESET Cyber Security Pro coloca automaticamente os ficheiros eliminados em quarentena (caso não tenha desmarcado esta opção na janela de alertas). É possível colocar manualmente em quarentena qualquer ficheiro suspeito clicando em **Quarentena...**. O menu de contexto pode ser utilizado também para esta finalidade, CTRL + clique no campo em branco, selecione **Quarentena...**, selecione um ficheiro que pretende colocar em quarentena e clique em **Abrir**.

## Restauração da Quarentena

Os ficheiros colocados em quarentena podem também ser restaurados para o local original. Para tal, selecione um ficheiro colocado em quarentena e clique em **Restaurar**. A opção Restaurar também está disponível no menu de contexto, CTRL+clique num determinado ficheiro na janela Quarentena e, em seguida, clique em **Restaurar**. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um ficheiro para uma localização diferente da localização original da qual foi eliminado.

## Envio de ficheiro da Quarentena

Se colocou em quarentena um ficheiro suspeito não detetado pelo programa, ou se um ficheiro foi avaliado incorretamente como infetado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o ficheiro para o Threat Lab da ESET. Para enviar um ficheiro da quarentena, CTRL + clique no ficheiro e selecione **Enviar ficheiro para análise** no menu de contexto.

## Processos em execução

A lista de **Processos em execução** apresenta os processos em execução no computador. O ESET Cyber Security Pro fornece informações detalhadas sobre a execução de processos para proteger os utilizadores com a tecnologia ESET Live Grid.

- **Processo** - nome do processo em execução no computador atualmente. Para ver todos os processos em execução, também pode utilizar o Monitor de Atividade (em */Aplicações/Utilitários*).
- **Nível de risco** - na maioria dos casos, o ESET Cyber Security Pro e a tecnologia ESET Live Grid atribuem níveis de risco a objetos (ficheiros, processos, etc.) através de uma série de regras da heurística, que examinam as características de cada objeto e avaliam o seu potencial para atividades maliciosas. Com base nesta heurística, é atribuído um nível de risco aos objetos. As aplicações conhecidas marcadas a verde estão seguramente limpas (na lista de permissões) e serão excluídas da análise. Isto melhora a velocidade da análise a pedido e em Tempo real. Se uma aplicação for marcada como desconhecida (amarelo), não significa que seja, necessariamente, software malicioso. Normalmente, trata-se apenas de uma aplicação mais recente. Se não tiver a certeza em relação a um ficheiro, pode enviá-lo para o Threat Lab da ESET para análise. Se o ficheiro for, efetivamente, uma aplicação maliciosa, a sua assinatura será adicionada a uma das atualizações futuras.
- **Número de utilizadores** - o número de utilizadores de uma determinada aplicação. Esta informação é reunida pela tecnologia ESET Live Grid.
- **Hora da descoberta** - período de tempo desde que a aplicação foi descoberta pela tecnologia ESET Live Grid.

- **ID do conjunto de aplicações** - nome do fornecedor ou do processo da aplicação.

Ao clicar num determinado processo, serão apresentadas as seguintes informações na parte inferior da janela:

- **Ficheiro** - localização de uma aplicação no computador
- **Tamanho do ficheiro** - tamanho físico do ficheiro no disco
- **Descrição do ficheiro** - características do ficheiro baseadas na descrição do sistema operativo
- **ID do conjunto de aplicações** - nome do fornecedor ou do processo da aplicação
- **Versão do ficheiro** - informações sobre o editor da aplicação
- **Nome do produto** - nome da aplicação e/ou nome da empresa

## Ligações de rede

As Ligações de rede são uma lista de ligações de rede ativas presentes no computador. O ESET Cyber Security Pro fornece informações detalhadas sobre cada ligação e permite-lhe criar uma regra para bloquear estas ligações.

### Criar uma regra de bloqueio para esta ligação

O ESET Cyber Security Pro permite-lhe criar uma regra de bloqueio para cada ligação no gestor de **Ligações de rede**. Para criar uma regra de bloqueio, clique com o botão direito do rato e selecione **Criar regra de bloqueio para esta ligação**.

1. Selecione o **Perfil** da ligação para a qual pretende criar a regra e introduza o nome da regra. Selecione a aplicação à qual se aplica a regra ou selecione a caixa de verificação para que a regra se aplique a todas as aplicações.
2. Selecione uma ação para a ligação, quer para recusar (bloquear) a ligação, quer para permitir a mesma. Selecione a direção da comunicação que deverá aplicar-se à regra. Pode criar um relatório para a regra ao clicar em **Registar regra**.
3. Selecione o protocolo da ligação e os tipos de porta. Selecione a porta para o serviço ou especifique um intervalo de portas com o formato: from-to.
4. Selecione o destino e introduza as informações no campo em questão, consoante o destino.

## Live Grid

O Live Grid Early Warning System mantém a ESET imediata e continuamente informada de novas infiltrações. O Live Grid Early Warning System bidirecional tem um único objetivo: melhorar a proteção que podemos oferecer. A melhor forma de garantir que detetamos novas ameaças logo que estas aparecem é "ligar" tantos dos nossos clientes quanto possível e utilizá-los como os nossos batedores de ameaças. Existem duas opções:

1. Pode escolher não ativar o Live Grid Early Warning System. Não irá perder qualquer funcionalidade no software e irá ainda receber a melhor proteção que oferecemos.

2. Pode configurar o Live Grid Early Warning System para enviar informações anónimas sobre novas ameaças e onde está incluído o novo código de ameaça. Esta informação pode ser enviado para a ESET para uma análise detalhada. Estudar estas ameaças pode ajudar a ESET a atualizar o seu motor de deteção e melhorar a capacidade de deteção de ameaças do programa.

O Live Grid Early Warning System irá recolher informações sobre o seu computador relacionadas com ameaças recentemente detetadas. Estas informações podem incluir uma amostra ou cópia do ficheiro onde apareceu a ameaça, o caminho para esse ficheiro, o nome do ficheiro, a data e hora, o processo através do qual a ameaça apareceu no seu computador e informações sobre o sistema operativo do seu computador.

Apesar de haver uma possibilidade de esta situação divulgar ocasionalmente algumas informações sobre si ou o seu computador (nomes de utilizador num caminho de diretório, etc.) para o Threat Lab da ESET, estas informações não serão utilizadas para QUALQUER efeito que não o de nos ajudar a responder imediatamente a novas ameaças.

Para aceder à configuração do Live Grid a partir do menu principal, clique em **Configurar > Introduzir preferências da aplicação ...** (ou prima *cmd+,*) > **Live Grid**. Selecione **Ativar Live Grid Early Warning System** para ativar o Live Grid e, em seguida, clique em **Configurar...** junto a **Opções avançadas**.

## Configuração do Live Grid

Por predefinição, o ESET Cyber Security Pro está configurado para enviar ficheiros suspeitos para o Threat Lab da ESET para uma análise detalhada. Se não pretender enviar estes ficheiros automaticamente, desmarque **Enviar ficheiros**.

Se encontrar um ficheiro suspeito, pode enviá-lo para os nossos Threat Labs para análise. Para tal, clique em **Ferramentas > Enviar amostra para análise** a partir da janela principal do programa. Se se tratar de uma aplicação maliciosa, a respetiva deteção será adicionada a atualização futura.

**Enviar estatísticas anónimas** – o ESET Live Grid Early Warning System recolhe informações anónimas sobre o seu computador relacionadas com ameaças recentemente detetadas. Estas informações poderão incluir o nome da infiltração, a data e hora em foi detetada, a versão do produto de segurança da ESET, a versão do seu sistema operativo e a definição de localização. Estas estatísticas são normalmente entregues aos servidores da ESET, uma ou duas vezes por dia.

**Filtro de exclusões** – esta opção permite-lhe excluir determinados tipos de ficheiro do envio. Por exemplo, poderá ser útil para excluir ficheiros que possam conter informações confidenciais, tais como documentos ou folhas de cálculo. Por predefinição, são excluídos os tipos de ficheiros mais comuns (.doc, etc.). Pode adicionar tipos de ficheiros à lista de ficheiros excluídos.

**E-mail de contacto (opcional)** – o seu endereço de e-mail poderá ser utilizado se forem necessárias mais informações para análise. Tenha em atenção que não irá receber uma resposta da ESET exceto se forem necessárias mais informações.

## Interface do utilizador

As opções de configuração da interface do utilizador permitem-lhe ajustar o ambiente de trabalho de acordo com as suas necessidades. É possível aceder a estas opções a partir do menu principal, clicando em **Configurar** > **Introduzir preferências da aplicação ...** (ou prima *cmd+,*) > **Interface**.

- Para apresentar o ecrã inicial do ESET Cyber Security Pro na inicialização do sistema, seleccione **Mostrar ecrã inicial na inicialização**.
- **Aplicação presente no Dock** permite-lhe apresentar o ícone  do ESET Cyber Security Pro no Dock do macOS e mudar entre o ESET Cyber Security Pro e outras aplicações em execução premindo *cmd+tab*. As alterações são implementadas depois de reiniciar o ESET Cyber Security Pro (ação geralmente acionada pela reinicialização do computador).
- A opção **Usar menu padrão** permite-lhe utilizar determinados atalhos do teclado (consulte [Atalhos do teclado](#)) e ver os itens do menu padrão (Interface do utilizador, Configuração e Ferramentas) na Barra de menu do macOS (parte superior do ecrã).
- Para ativar sugestões para determinadas opções do ESET Cyber Security Pro, seleccione **Mostrar sugestões**.
- **Mostrar ficheiros ocultos** permite-lhe visualizar e seleccionar ficheiros ocultos na configuração **Alvos de análise** de uma **Análise do computador**.
- Por predefinição, o ícone  do ESET Cyber Security Pro é apresentado nos Extras da Barra de menu que aparecem à direita da Barra de menu do macOS (parte superior do ecrã). Para desativar esta opção, desmarque **Mostrar ícone nos extras da barra de menu**. Esta alteração é implementada depois de reiniciar o ESET Cyber Security Pro (ação geralmente acionada pela reinicialização do computador).

## Alertas e notificações

A secção **Alertas e notificações** permite-lhe configurar o modo como os alertas de ameaças e as notificações do sistema são tratados pelo ESET Cyber Security Pro.

A desativação de **Mostrar alertas** irá cancelar todas as janelas de alertas e será recomendada apenas em situações específicas. Para a maioria dos utilizadores, recomendamos que a predefinição desta opção seja mantida (ativada). As opções avançadas são descritas [neste capítulo](#).

A seleção de **Mostrar notificações no ambiente de trabalho** irá ativar as janelas de alertas que não requeiram a interação do utilizador para serem apresentadas no ambiente de trabalho (por predefinição, no canto superior direito do ecrã). Pode definir o período durante o qual a notificação será apresentada, ajustando o valor **Fechar notificações automaticamente depois de X segundos** (por predefinição, 5 segundos).

Desde a versão 6.2 do ESET Cyber Security Pro que é possível impedir que determinados **Estados da proteção** sejam apresentados no ecrã principal do programa (janela **Estado da proteção**). Para saber mais sobre este assunto, consulte [Estados da proteção](#).

## Mostrar alertas

O ESET Cyber Security Pro apresenta caixas de diálogo de alerta a informar sobre uma nova versão do programa, atualizações do sistema operativo, desativação de determinados componentes do programa, eliminação de relatórios, etc. Pode suprimir cada notificação individualmente selecionando **Não mostrar esta caixa de diálogo novamente**.

A **Lista de caixas de diálogo** (**Configuração > Introduzir preferências da aplicação... > Alertas e notificações > Configuração...**) mostra a lista de todas as caixas de diálogo de alerta acionadas pelo ESET Cyber Security Pro. Para ativar ou suprimir cada notificação, seleccione a caixa de verificação à esquerda **Nome da caixa de diálogo**. Além disso, pode definir **Condições de apresentação** onde serão apresentadas as notificações sobre novas versões do programa e atualizações do sistema operativo.

## Estados da proteção

É possível alterar o estado da proteção atual do ESET Cyber Security Pro através da ativação ou desativação dos estados em **Configurar > Introduzir preferências da aplicação... > Alertas e notificações > Mostrar no ecrã Estado da proteção: Configurar**. O estado das diversas funcionalidades do programa será apresentado ou ocultado no ecrã principal do ESET Cyber Security Pro (janela **Estado da proteção**).

Pode ocultar o estado da proteção das seguintes funcionalidades do programa:

- Firewall
- Antiphishing
- Proteção de acesso à Web
- Proteção do cliente de email
- Atualização do sistema operativo
- Expiração da licença

- É necessário reiniciar o computador

## Privilégios

As definições do ESET Cyber Security Pro podem ser muito importantes para a política de segurança da organização. As modificações não autorizadas podem pôr em risco a estabilidade e a proteção do seu sistema. Por este motivo, pode definir os utilizadores que têm permissão para editar a configuração do programa.

Para especificar os utilizadores privilegiados, aceda a **Configurar > Introduzir preferências da aplicação ...** (ou prima *cmd+*) > **Privilégios**. Selecione os utilizadores ou grupos da lista à esquerda e clique em **Adicionar**. Para visualizar todos os utilizadores/grupos do sistema, selecione **Mostrar todos os utilizadores/grupos**. Para remover um utilizador, basta seleccionar um nome na lista **Utilizadores seleccionados** do lado direito e clicar em **Remover**.



Acerca da atualização

Se deixar a lista Utilizadores seleccionados vazia, todos os utilizadores são considerados privilegiados.

## Menu de contexto

A integração do menu de contexto pode ser ativada clicando em **Configurar > Introduzir preferências da aplicação ...** (ou prima *cmd+*) > secção **Menu de contexto** seleccionando a caixa de verificação **Integrar ao menu de contexto**. É necessário terminar sessão ou reiniciar o computador para que as alterações sejam implementadas. As opções do menu de contexto ficam disponíveis na janela do **Finder** ao fazer CTRL+clique em qualquer ficheiro.

## Importar e exportar definições

Para importar uma configuração existente ou exportar a configuração do ESET Cyber Security Pro, clique em **Configurar > Importar ou exportar definições**.

A importação e a exportação são úteis caso seja necessário fazer uma cópia de segurança da configuração atual do ESET Cyber Security Pro para posterior utilização. Exportar definições também é prático para utilizadores que pretendam utilizar as suas configurações preferenciais do ESET Cyber Security Pro em diversos sistemas. Pode importar facilmente um ficheiro de configuração para transferir as definições pretendidas.



Para importar uma configuração, selecione **Importar definições** e clique em **Procurar** para navegar até ao ficheiro de configuração que pretende importar. Para exportar, selecione **Exportar definições** e utilize o navegador para selecionar uma localização no computador para guardar o ficheiro de configuração.

## Configuração do servidor proxy

As definições do servidor proxy podem ser configuradas em **Configurar > Introduzir preferências da aplicação...** (ou prima *cmd-*) > **Servidor Proxy**. A especificação do servidor proxy neste nível define as definições globais do servidor proxy para todas as funções do ESET Cyber Security Pro. Os parâmetros definidos aqui serão utilizados por todos os módulos que necessitem de ligação à Internet. O ESET Cyber Security Pro suporta os tipos de autenticação de Acesso Básico e NTLM (NT LAN Manager).

Para especificar as definições do servidor proxy para este nível, selecione **Usar servidor proxy** e introduza o endereço IP ou o URL do servidor proxy no campo **Servidor proxy**. No campo Porta, especifique a porta em que o servidor proxy aceita as ligações (3128 por predefinição). Também pode clicar em **Detetar** para deixar o programa preencher os dois campos.

Se a comunicação com o servidor proxy requerer autenticação, introduza um **Nome de utilizador** e **Palavra-passe** válidos nos respetivos campos.

## Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta aceder e/ou danificar o computador de um utilizador.

## Vírus

Um vírus informático é uma infiltração que corrompe os ficheiros existentes no computador. O nome vírus é proveniente dos vírus biológicos, uma vez que utilizam técnicas semelhantes para se propagarem de um computador para outro.

Os vírus informáticos atacam normalmente ficheiros executáveis, scripts e documentos. Para se replicar, um vírus anexa o seu "corpo" ao fim de um ficheiro de destino. Em resumo, um vírus informático funciona da seguinte maneira: após a execução do ficheiro infetado, o vírus ativa-se a si próprio (antes da aplicação original) e realiza a sua tarefa predefinida. Só depois disso, a aplicação original pode ser executada. Um vírus só pode infetar um computador se um utilizador (acidental ou deliberadamente) executar ou abrir o programa malicioso.

Os vírus informáticos podem variar em termos de finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de eliminar propositadamente ficheiros de um disco rígido. Porém, alguns vírus não causam quaisquer danos; apenas servem para aborrecer o utilizador e demonstrar as capacidades técnicas dos respetivos autores.

É importante salientar que os vírus (quando comparados com os cavalos de troia ou spyware) estão a tornar-se cada vez mais raros, uma vez que não são comercialmente atrativos para os autores de software malicioso. Além disso, o termo "vírus" é frequentemente utilizado de modo incorreto para abranger todos os tipos de infiltrações. Esta utilização está gradualmente a ser ultrapassada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador for infetado por um vírus, será necessário restaurar os ficheiros infetados para o estado original, normalmente limpando-os utilizando um programa antivírus.

## Worms

Um worm informático é um programa que contém código malicioso que ataca os computadores host e se propaga através de uma rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; estes não dependem dos ficheiros host (ou dos setores de inicialização). Os worms são propagados através dos endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança das aplicações de rede.

Os worms são, por conseguinte, muito mais viáveis que os vírus informáticos. Devido à ampla disponibilidade da Internet, os worms podem propagar-se por todo o globo em horas após a sua libertação, em alguns casos, até em minutos. Esta capacidade de se replicarem de forma autónoma e rápida torna-os mais perigosos que outros tipos de malware.

Um worm ativado num sistema pode causar muitos transtornos: Pode eliminar ficheiros, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm informático qualifica-o como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador for infectado por um worm, recomendamos que elimine os ficheiros infetados porque

provavelmente contêm código malicioso.

## Cavalos de troia (Trojans)

Historicamente, os cavalos de troia informáticos foram definidos como uma classe de infiltrações que tenta apresentar-se como programas úteis, enganando assim os utilizadores que permitem a respetiva execução. Atualmente, deixou de ser necessário disfarçar os cavalos de troia. O seu único propósito é infiltrar-se o mais facilmente possível e atingir os seus objetivos maliciosos. O "cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não pertença a nenhuma classe específica de infiltração.

Uma vez que esta é uma categoria muito abrangente, é frequentemente dividida em muitas subcategorias:

- Downloader – Um programa malicioso com a capacidade de fazer a transferência de outras infiltrações da Internet
- Dropper – Um tipo de cavalo de troia criado para instalar outros tipos de malware em computadores comprometidos
- Backdoor – Uma aplicação que se comunica com atacantes remotos e que permite que obtenham acesso a um sistema e assumam o controlo do mesmo.
- Keylogger – (keystroke logger) – Um programa que regista cada toque de tecla do utilizador e envia as informações para os atacantes remotos
- Dialer – Dialers são programas criados para estabelecerem ligação com os números premium-rate. É quase impossível para um utilizador notar que foi criada uma nova ligação. Os dialers apenas podem causar danos aos utilizadores com modems de ligação telefónica, que deixaram de ser utilizados com tanta frequência.

Os cavalos de troia geralmente tomam a forma de ficheiros executáveis. Se um ficheiro no computador for detetado como um cavalo de troia, recomenda-se que o elimine, uma vez que é muito provável que contenha código malicioso.

## Rootkits

Os rootkits são programas maliciosos que concedem aos atacantes pela Internet acesso ilimitado a um sistema, enquanto ocultam a sua presença. Depois de acederem a um sistema (explorando, normalmente, a vulnerabilidade de um sistema), os rootkits utilizam funções integradas no sistema operativo para evitar que sejam detetados por software antivírus: este ocultam processos e ficheiros. Por este motivo, é praticamente impossível detetá-los utilizando técnicas de teste comuns.

## Adware

Adware é a abreviatura de "advertising-supported software" (software suportado por publicidade). Os programas que apresentam material publicitário pertencem a esta categoria. Geralmente, as aplicações adware abrem automaticamente uma nova janela pop-up com publicidade num navegador da Internet, ou mudam a home page

do mesmo. O adware está frequentemente integrado em programas freeware, permitindo que os criadores de programas freeware cubram os custos de programação das suas aplicações (normalmente úteis).

O adware por si só não é perigoso; os utilizadores serão apenas incomodados pela publicidade. O perigo está no facto de o adware também poder realizar funções de análise (à semelhança do spyware).

Se decidir utilizar um produto freeware, preste especial atenção ao programa de instalação. É muito provável que o instalador o notifique sobre a instalação de um programa adware extra. Normalmente, poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware, caso contrário as respetivas funcionalidades ficarão limitadas. Isto muitas vezes significa que o adware poderá aceder com frequência ao sistema "legalmente", uma vez que os utilizadores assim o concordaram. Neste caso, é melhor prevenir do que remediar. Se um ficheiro for detetado como adware no computador, recomenda-se que o elimine, uma vez que há uma grande probabilidade de conter código malicioso.

## Spyware

Esta categoria abrange todas as aplicações que enviam informações privadas sem o consentimento/conhecimento do utilizador. Os spywares utilizam as funções de análise para enviar diversos dados estatísticos, como listas dos Web sites visitados, endereços de email da lista de contactos do utilizador ou uma lista das teclas registadas.

Os autores de spyware alegam que estas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos utilizadores e permitir um melhor direcionamento da publicidade. O problema é que não existe uma distinção clara entre as aplicações maliciosas e as úteis, e ninguém pode assegurar que as informações recebidas não serão utilizadas indevidamente. Os dados obtidos pelas aplicações spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O spyware é frequentemente integrado em versões gratuitas de um programa pelo seu autor com a finalidade de gerar receitas ou incentivar à aquisição do software. Geralmente, os utilizadores são informados da presença do spyware durante a instalação do programa no sentido de os incentivar a atualizar para uma versão paga sem o mesmo.

Exemplos de produtos freeware bem conhecidos que vêm integrados com spyware são as aplicações cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; parecem ser programas antispyware, mas são, na verdade programas spyware.

Se um ficheiro for detectado como spyware no computador, recomenda-se que o elimine, uma vez que há uma grande probabilidade de conter código malicioso.

## Aplicações potencialmente inseguras

Existem muitos programas legítimos cuja função é a de simplificar a administração dos computadores ligados em rede. No entanto, nas mãos erradas, estes podem ser utilizados indevidamente para fins maliciosos. O ESET Cyber Security Pro fornece a opção de detetar tais ameaças.

Normalmente, as aplicações potencialmente inseguras são softwares comerciais e legítimos. Esta classificação inclui programas como ferramentas de acesso remoto, aplicações para desbloquear palavras-passe e keyloggers (um programa que regista cada toque de tecla do utilizador).

## Aplicações potencialmente não desejadas

As aplicações potencialmente não desejadas não são necessariamente maliciosas, mas podem afetar negativamente o desempenho do computador. Tais aplicações exigem geralmente o consentimento para a instalação. Se estas aplicações estiverem presentes no computador, o sistema irá comportar-se de modo diferente (em comparação ao modo como se comportava antes da instalação destas aplicações). As alterações mais significativas são:

As categorias que podem ser consideradas grayware incluem: software de apresentação de publicidade, wrappers de transferência, várias ferramentas de browser, software com comportamento enganoso, bundleware, trackware, limpadores de registo ou qualquer outro software de borderline ou software que recorre a práticas comerciais ilícitas ou, pelo menos, não éticas (apesar da sua aparência legítima) e que possa ser considerado indesejável por um utilizador final que conheça as consequências da instalação desse tipo de software.

Uma Aplicação Potencialmente Insegura é um software legítimo (possivelmente de finalidade comercial) que pode ser utilizado de forma abusiva por um atacante. A deteção destes tipos de aplicação pode ser ativada ou desativada pelos utilizadores do software ESET.

Existem situações em que um utilizador pode sentir que as vantagens de uma aplicação potencialmente não desejada se sobrepõem aos riscos. Por esse motivo, a ESET atribui essas aplicações a uma categoria de risco inferior em comparação com outros tipos de software malicioso, como cavalos de Troia ou worms.

- [Aviso - Aplicação potencialmente não desejada detetada](#)
- [Aplicações potencialmente não desejadas - Definições](#)
- [Aplicações potencialmente não desejadas - Wrappers de software](#)
- [Aplicações potencialmente não desejadas - Limpadores de registo](#)
- [Conteúdo potencialmente não desejado](#)

## Aviso - Aplicação potencialmente não desejada detetada

Quando é detetada uma aplicação potencialmente não desejada, pode decidir a ação a realizar:

1. **Limpar/Desligar:** Esta opção termina a ação e impede que a PUA entre no seu sistema.
2. **Ignorar:** Esta opção permite a entrada de uma PUA no seu sistema.

3. Para permitir a execução da aplicação no seu computador futuramente e sem interrupção, clique em **Opções avançadas** e, em seguida, selecione a caixa de verificação junto a **Excluir da detecção** e clique em **Ignorar**.

## ativação e execução de processos ocultos

Ao instalar o seu produto ESET, pode decidir se pretende ativar a detecção de aplicações potencialmente não desejadas, conforme indicado a seguir:



### Aviso

As aplicações potencialmente não desejadas podem instalar adware, ferramentas de browser ou incluir outras funções de programa não desejadas e inseguras.

Estas definições podem ser modificadas em qualquer momento no seu programa. Para ativar ou desativar a detecção de aplicações potencialmente não desejadas, inseguras ou suspeitas, siga estas instruções:

1. Abra o seu produto ESET. [Como abrir o meu produto ESET?](#)
2. Acesse a **Configuração** e clique em **Introduzir preferências da aplicação** para aceder às preferências do ESET Cyber Security Pro.
3. Clique em **Geral** e ative ou desative as opções **Ativar detecção de aplicações potencialmente não desejadas**, **Ativar detecção de aplicações potencialmente inseguras** e **Ativar detecção de aplicações suspeitas** de acordo com as suas preferências. Confirme clicando em **OK**.

## aumento da utilização de recursos do sistema

Um wrapper de software é um tipo especial de modificação de aplicação utilizado por determinados Web sites de alojamento de ficheiros. Trata-se de uma ferramenta de terceiros que instala o programa que pretende transferir, mas que adiciona software adicional, como ferramentas de browser ou adware. O software adicional pode também efetuar alterações na página inicial do browser e nas definições de pesquisa. Além disso, os Web sites de alojamento de ficheiros, frequentemente, não notificam o fornecedor do software ou destinatário das transferências de que foram efetuadas modificações e ocultam frequentemente as opções de recusa. Por esses motivos, a ESET classifica os wrappers de software como um tipo de aplicação potencialmente não desejada de forma a permitir aos utilizadores aceitar ou recusar a transferência.

## Aplicações potencialmente inseguras

Existem diversos programas legítimos cuja função é simplificar a administração de computadores ligados em rede. No entanto, nas mãos erradas, podem ser utilizados abusivamente para fins maliciosos. O ESET Cyber Security Pro oferece a opção de detecção desse tipo de ameaças.

As aplicações potencialmente inseguras são tipicamente software legítimo, com fins comerciais. Esta classificação inclui programas como ferramentas de acesso remoto, ferramentas de decifragem e keyloggers (um programa que grava cada acionamento de tecla do utilizador).

## Aplicações suspeitas

Se a detecção de PUA estiver ativada no seu produto ESET, os Web sites com reputação de promoverem PUAs ou de enganarem os utilizadores, incentivando-os a realizar ações com implicações negativas nos seus sistemas ou

na sua experiência de navegação serão bloqueados como conteúdo potencialmente não desejado. Se receber a notificação de que um site que está a tentar visitar está classificado como conteúdo potencialmente não desejado, pode clicar em **Voltar** para sair da página web bloqueada ou clicar em **Ignorar e continuar** para permitir que o site carregue.

Consulte este [artigo da base de dados de conhecimento ESET](#) para obter uma versão atualizada desta página de ajuda.

## Tipos de ataques remotos

Existem várias técnicas especiais que permitem aos atacantes comprometer sistemas remotos. Estas estão divididas em várias categorias.

## Ataques DoS

DoS, ou Denial of Service, é uma tentativa de tornar um computador ou rede indisponível para os seus utilizadores pretendidos. A comunicação entre utilizadores afetados é obstruída e não pode continuar de uma forma funcional. O computadores expostos a ataques DoS precisam geralmente de ser reiniciados para funcionar adequadamente.

Na maioria dos casos, os alvos são servidores Web e o objetivo é torná-los indisponíveis para os utilizadores durante um determinado período de tempo.

## Envenenamento de DNS

Ao utilizar o envenenamento de DNS (Servidor de Nomes de Domínio), os hackers podem enganar o servidor DNS de qualquer computador de forma a acreditar que os dados falsos que forneceram são legítimos e autênticos. As informações falsas são colocadas em cache durante um determinado período de tempo, permitindo aos atacantes reescrever respostas DNS de endereços IP. Consequentemente, os utilizadores que tentam aceder a Web sites da Internet irão transferir vírus informáticos ou worms em vez do seu conteúdo original.

## Análise da porta

A análise da porta é utilizada para determinar que portas do computador estão abertas num host de rede. Um scanner de portas é um software concebido para encontrar essas portas.

A porta de um computador é um ponto virtual que lida com dados de entrada e saída, o que é crucial do ponto de vista da segurança. Numa rede de grandes dimensões, as informações reunidas por scanners de portas podem ajudar a identificar possíveis vulnerabilidades. Essa utilização é legítima.

No entanto, a análise de portas é muitas vezes utilizada por hackers que tentam comprometer a segurança. O seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar que

portas estão em utilização. A própria análise não provoca danos, mas tenha em atenção que esta atividade pode revelar possíveis vulnerabilidades e permitir que atacantes assumam o controlo de computadores remotos.

É aconselhável que os administradores de rede bloqueiem todas as portas não utilizadas e protejam as que estão em utilização de acesso não autorizado.

## Dessincronização do TCP

A dessincronização do TCP é uma técnica utilizada em ataques de sequestro de ligações TCP. Esta é acionada por um processo em que o número sequencial em pacotes de entrada difere do número sequencial esperado. Os pacotes com um número sequencial inesperado são dispensados (ou guardados no armazenamento da memória intermédia, se estiverem presentes na atual janela de comunicação).

Na dessincronização, ambos os pontos de comunicação dispensam os pacotes recebidos, altura em que os atacantes remotos podem infiltrar-se e fornecer aos pacotes um número sequencial correto. Os atacantes podem até manipular ou modificar comunicações.

Os ataques de sequestro de ligações TCP têm como objetivo interromper as comunicações servidor-cliente ou peer-to-peer. Muitos ataques podem ser evitados utilizando autenticação para cada segmento TCP. É também aconselhável utilizar as configurações recomendadas para os seus dispositivos de rede.

## Relé SMB

O relé SMB e relé SMB 2 são programas especiais capazes de executar ataques contra computadores remotos. Estes programas tiram proveito do protocolo de partilha de ficheiros do Bloco de Mensagem de Servidor (SMB), que está sobreposto no NetBIOS. Um utilizador que partilhe qualquer pasta ou diretório numa LAN utiliza muito provavelmente este protocolo de partilha de ficheiros.

Na comunicação de rede local, os hashes das palavras-passe são trocados.

O relé SMB recebe uma ligação na porta UDP 139 e 445, reencaminha os pacotes trocados pelo cliente e servidor e modifica-os. Depois da ligação e autenticação, o cliente é desligado. O relé SMB cria um novo endereço IP virtual. O relé SMB reencaminha as comunicações do protocolo SMB, exceto para negociação e autenticação. Os atacantes remotos podem utilizar o endereço IP, desde que o computador cliente esteja ligado.

O relé SMB 2 funciona com base no mesmo princípio que o relé SMB, com a exceção de utilizar nomes do NetBIOS em vez de endereços IP. Ambos podem executar ataques "intermediários". Estes ataques permitem aos atacantes remotos ler, introduzir e modificar mensagens trocadas entre dois pontos de comunicação sem serem detetados. Os computadores expostos a esses ataques deixam muitas vezes de responder ou reiniciam

inesperadamente.

Para evitar ataques, recomendamos que utilize palavras-passe ou chaves de autenticação.

## Ataques ICMP

O ICMP (Protocolo de Mensagens de Controlo da Internet) é um protocolo popular e largamente utilizado. É utilizado sobretudo por computadores ligados em rede para enviar várias mensagens de erro.

Os atacantes remotos tentam explorar as fraquezas do protocolo ICMP. O protocolo ICMP foi concebido para comunicação unidirecional, não necessitando de autenticação. Isto permite que os atacantes remotos acionem ataques DoS (Denial of Service) ou ataques que dão acesso a indivíduos não autorizados a pacotes de entrada e saída.

Os exemplos típicos de um ataque ICMP são ataques ping floods, floods de ICMP\_ECHO e smurf. Os computadores expostos a um ataque ICMP são significativamente mais lentos (isso aplica-se a todas as aplicações que utilizam a Internet) e têm problemas de ligação à Internet.

## E-mail

E-mail, ou correio eletrónico, é uma forma moderna de comunicação com diversas vantagens. É flexível, rápido e direto e desempenhou um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com um grande nível de anonimato, o e-mail e a Internet dão azo a atividades ilegais como, por exemplo, o spam. O spam inclui publicidades não solicitadas, hoaxes e proliferação de software malicioso - malware. A inconveniência e perigo para si aumentam com o facto de o custo de enviar spam ser mínimo e os autores de spam têm muitas ferramentas para adquirir novos endereços de e-mail. Para além disso, o volume e a variedade do spam torna-o difícil de regular. Quanto mais tempo utilizar o seu endereço de e-mail, maior é a probabilidade de acabar numa base de dados de mecanismo de spam. Algumas sugestões de prevenção:

- Se possível, não publique o seu endereço de e-mail na Internet
- dê apenas o seu endereço de e-mail a pessoas de confiança
- se possível, não utilize aliases comuns. Com aliases mais complicados, a probabilidade de rastreamento é menor
- não responda a spam que já tenha chegado à sua caixa de entrada
- tenha cuidado ao preencher formulários da Internet; tenha especial cuidado com opções como *Sim, pretendo receber informações*
- utilize endereços de e-mail "especializados", por exemplo, um para o trabalho, um para comunicar com os

seus amigos, etc.

- esporadicamente, altere o seu endereço de e-mail
- utilize uma solução antispam

## Publicidades

A publicidade na Internet é uma das formas de publicidade que tem crescido mais rapidamente. As suas principais vantagens de marketing são custos mínimos e um elevado nível de objetividade; para além disso, as mensagens são entregues praticamente de imediato. Muitas empresas utilizam ferramentas de marketing através de e-mail para comunicar com os seus atuais e potenciais clientes.

Este tipo de publicidade é legítimo, uma vez que pode estar interessado em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em massa não solicitadas. Nesses casos, a publicidade através de e-mail é exagerada e passa a considerar-se spam.

A quantidade de e-mails não solicitados tornou-se num problema e não há sinais de abrandamento. Os autores de e-mails não solicitados tentam muitas vezes disfarçar spam como mensagens legítimas.

## Hoaxes

Um hoax é uma informação errada que é espalhada pela Internet. Os hoaxes são geralmente enviados através de e-mail ou ferramentas de comunicação como o ICQ e Skype. A mensagem em si é muitas vezes uma piada ou um mito urbano.

O hoaxes de vírus informáticos tentam incutir medo, incerteza e dúvida nos destinatários, fazendo-os acreditar que existe um "vírus indetetável" a eliminar ficheiros e a obter palavras-passe ou a executar alguma outra atividade prejudicial no seu sistema.

Alguns hoaxes funcionam pedindo aos destinatários para encaminhar as mensagens para os seus contactos, perpetuando o hoax. Existem hoaxes para telemóveis, pedidos de ajuda, pessoas que lhe oferecem dinheiro do estrangeiro, etc. É muitas vezes impossível determinar o intuito do criador.

Se vir uma mensagem a solicitar que a encaminhe para toda a gente que conhece, pode muito bem ser um hoax. Existem vários Web sites na Internet que podem verificar se um e-mail é legítimo. Antes de encaminhar, faça uma pesquisa na Internet relativamente a qualquer mensagem que suspeite ser um hoax.

# Phishing

O termo phishing define uma atividade criminal que utiliza técnicas de engenharia social (manipular os utilizadores de forma a obter informações confidenciais). O seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos PIN, etc.

O acesso é geralmente alcançado enviando um e-mail, fazendo-se passar por uma pessoa ou empresa de confiança (p. ex., instituição financeira, companhia de seguros). O e-mail pode parecer muito genuíno e irá incluir imagens e conteúdo que poderão ter sido originalmente retirados da fonte que estão a imitar. Ser-lhe-á pedido para introduzir, mediante vários pretextos (verificação de dados, operações financeiras), alguns dos seus dados pessoais, como números de contas bancárias ou nomes de utilizador e palavras-passe, etc. Todos esses dados, se enviados, podem ser facilmente roubados e utilizados indevidamente.

Bancos, companhias de seguros e outras empresas legítimas nunca lhe pedirão nomes de utilizador e palavras-passe num e-mail não solicitado.

## Reconhecer fraudes através de spam

Geralmente, existem poucos indicadores que o podem ajudar a identificar spam (e-mails não solicitados) na sua caixa de correio. Se uma mensagem preencher, pelo menos, alguns dos critérios seguintes, o mais provável é tratar-se de uma mensagem de spam.

- O endereço do remetente não pertence a alguém na sua lista de contactos
- é-lhe oferecida uma grande quantia de dinheiro, mas tem de fornecer primeiro uma pequena quantia
- é-lhe pedido para introduzir, mediante vários pretextos (verificação de dados, operações financeiras), alguns dos seus dados pessoais como, por exemplo, números de contas bancárias, nomes de utilizador e palavras-passe, etc.
- está escrito numa língua estrangeira
- é-lhe pedido para comprar um produto no qual não está interessado. Se decidir comprar mesmo assim, verifique se o remetente da mensagem é um vendedor fiável (consulte o fabricante do produto original)
- algumas palavras têm erros gramaticais numa tentativa de enganar o seu filtro de spam. Por exemplo *vaigra* em vez de *viagra*, etc.

## Contrato de Licença do Utilizador Final para Utilização de Software.

**IMPORTANTE:** Leia cuidadosamente os termos e condições da aplicação do produto definidos abaixo antes de proceder à respetiva transferência, instalação, cópia ou utilização. **AO TRANSFERIR, INSTALAR, COPIAR OU UTILIZAR O SOFTWARE ESTARÁ A EXPRESSAR A SUA ACEITAÇÃO DOS PRESENTES TERMOS E CONDIÇÕES E**

## DECLARA TER TOMADO CONHECIMENTO DA [POLÍTICA DE PRIVACIDADE](#).

### Contrato de Licença do Utilizador Final

Ao abrigo dos termos do presente Contrato de Licença do Utilizador Final do Software (doravante designado por "Contrato") assinado por, e celebrado entre a ESET, spol. s r. o., com sede social em Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita na Conservatória do Registo Comercial administrada pelo Tribunal Distrital de Bratislava I, Secção Sro, Inscrição N.º 3586/B, sob o Número de Registo de Sociedade 31333532 (doravante designada por "ESET" ou "Fornecedor") e o cliente, sendo este uma pessoa singular ou uma pessoa coletiva (doravante designada por "Cliente" ou "Utilizador Final"), o Cliente terá o direito de utilizar o Software conforme definido no Artigo 1.º do presente Contrato. O Software descrito no Artigo 1.º do presente Contrato poderá ser armazenado num suporte de dados, enviado através de correio eletrónico, descarregado da Internet, transferido a partir dos servidores do Fornecedor ou obtido junto de outras fontes, ficando sujeito aos termos e condições abaixo especificados.

O PRESENTE DOCUMENTO CONSTITUI UM ACORDO RELATIVO AOS DIREITOS DO UTILIZADOR FINAL E NÃO UM ACORDO DE VENDA. O Fornecedor continuará a ser o proprietário da cópia do Software e dos meios físicos contidos no pacote de venda, bem como de quaisquer outras cópias que o Utilizador Final esteja autorizado a efetuar em conformidade com o disposto no presente Contrato.

Ao clicar em "Aceito" ou "Eu Aceito..." no decorrer da instalação, transferência, cópia ou utilização do Software, o Cliente estará a manifestar a sua concordância relativamente aos termos e condições do presente Contrato. Caso não esteja de acordo com todos os termos e condições do presente Contrato, deverá clicar de imediato na opção de cancelar, a fim de suspender a instalação ou a transferência, ou proceder à destruição ou à devolução do Software, dos meios de instalação, da documentação que acompanha o Software e do recibo comprovativo da venda, ao Fornecedor ou à loja junto da qual efetuou a aquisição do Software.

O CLIENTE RECONHECE QUE A SUA UTILIZAÇÃO DO SOFTWARE SIGNIFICA QUE LEU O PRESENTE CONTRATO, TENDO TOMADO CONHECIMENTO DO MESMO E ACEITANDO FICAR VINCULADO AOS SEUS TERMOS E CONDIÇÕES.

**1. Software.** O Software neste Contrato significará: (i) o programa de computador ESET Cybersecurity, incluindo todas as respetivas partes; (ii) o conteúdo dos discos, CD-ROMs, DVDs, relatórios de e-mail e todos os seus anexos, se existirem, ou outro suporte ao qual este Contrato seja anexado, incluindo o Software fornecido na forma de um código de objeto num CD-ROM, DVD ou por correio eletrónico através da Internet; (iii) qualquer material de instrução e documentação relacionados com o Software, incluindo, mas não se limitando a, qualquer descrição do Software, respetivas especificações, descrição das propriedades, descrição da utilização, descrição da interface na qual o Software é usado, um manual ou guia de instalação do Software ou qualquer descrição da utilização correta do Software ("Documentação"); (iv) cópias do Software, reparações de erros, se existirem, do Software, acréscimos ao Software, extensões do Software, versões modificadas do Software, novas versões do Software e todas as atualizações das partes do Software, se fornecidas, em relação às quais o Fornecedor lhe concede a Licença de acordo com o Artigo 3 deste documento. O Software deverá ser fornecido exclusivamente sob a forma de código-objeto executável.

**2. Instalação, Computador e Chave de Licença.** O Software fornecido num suporte de dados, enviado por correio eletrónico, descarregado da Internet, transferido a partir dos servidores do Fornecedor, ou obtido junto de outras fontes, requer uma instalação. Deverá instalar o Software num Computador corretamente configurado, que cumpra pelo menos os requisitos estipulados na Documentação. O método de instalação está descrito na Documentação. O Computador no qual o Software irá ser instalado não deverá conter quaisquer programas informáticos ou componentes de hardware suscetíveis de afetar negativamente o referido Software. O termo Computador entende-se por hardware, incluindo, mas não se limitando a, computadores pessoais, laptops, estações de trabalho, smartphones, dispositivos eletrónicos portáteis, ou outros dispositivos eletrónicos para os quais o Software tenha sido concebido, ou nos quais o Software irá ser instalado e/ou utilizado. O termo Chave de

Licença refere-se à sequência única, composta por símbolos, letras, números ou sinais especiais, que é fornecida ao Utilizador Final de modo a permitir a utilização legal do Software ou da sua versão específica, ou a extensão do prazo de validade da Licença em conformidade com o disposto no presente Contrato.

3. **Licença.** Sujeito à aceitação dos termos do presente Contrato por parte do Cliente, e na medida em que este último se comprometa a respeitar todos os termos e condições nele estipulados, o Fornecedor deverá atribuir-lhe os seguintes direitos (doravante conjuntamente designados por "Licença"):

a) **Instalação e utilização.** O Cliente tem o direito intransmissível e não exclusivo de proceder à instalação do Software no disco rígido de um Computador ou outro suporte permanente de armazenamento de dados, ou à instalação e armazenamento do Software na memória de um sistema informático, bem como de implementar, armazenar e visualizar o Software.

b) **Número de licenças estipulado.** O direito de utilização do Software ficará condicionado ao número de Utilizadores Finais. O termo Utilizador Final deverá ser entendido como referindo-se ao seguinte: (i) instalação do Software num sistema de computador; ou (ii) se a extensão de uma licença estiver vinculada ao número de caixas de correio eletrónico, um Utilizador Final será nesse caso entendido como um utilizador de computador que aceite receber correio eletrónico por intermédio de um Mail User Agent (doravante designado por "MUA"). Se o MUA aceitar o correio eletrónico e em seguida distribuí-lo automaticamente por vários utilizadores, tal significa que o número de Utilizadores Finais deverá ser determinado em função do número efetivo de utilizadores aos quais é distribuído o correio eletrónico. Se um servidor de correio eletrónico desempenhar a função de uma porta de correio, o número de Utilizadores Finais deverá ser igual ao número de utilizadores do servidor de correio aos quais é prestado um serviço pela referida porta. Caso um número indeterminado de endereços de correio eletrónico seja dirigido a, e aceite por, um mesmo utilizador (por exemplo, através do recurso a pseudónimos) e as mensagens não sejam automaticamente distribuídas pelo cliente a um maior número de utilizadores, será necessária uma Licença para um computador. A mesma Licença não poderá ser utilizada simultaneamente em mais do que um computador. O Utilizador Final encontra-se autorizado a introduzir a Chave de Licença no Software unicamente na medida em que lhe assista o direito de utilizar o Software de acordo com a limitação resultante do número de Licenças concedidas pelo Fornecedor. A Chave de Licença é considerada como sendo confidencial, pelo que o Cliente deverá abster-se de partilhar a Licença com terceiros, não devendo permitir que terceiros utilizem a Chave de Licença, salvo se autorizados para esse efeito pelo Fornecedor ou pelo presente Contrato. Caso a confidencialidade da sua Chave de Licença tenha ficado comprometida, deverá notificar de imediato o Fornecedor.

c) **Edição Empresarial.** Deverá ser obtida uma versão da Edição Empresarial do Software, caso este se destine a ser utilizado no âmbito de servidores de correio, relays de correio, gateways de correio eletrónico ou gateways de Internet.

d) **Prazo de validade da Licença.** O seu direito a utilizar o Software limitar-se-á a um determinado período de tempo.

e) **Software OEM.** O Software OEM (Fabricante do Equipamento Original) deverá limitar-se a ser utilizado apenas no Computador juntamente com o qual foi fornecido. Não poderá ser transferido para um outro Computador.

f) **Software de TESTE e NFR.** O Software classificado como "Não destinado a revenda" (NFR) ou de TESTE não poderá ser disponibilizado mediante um pagamento, devendo ser utilizado unicamente para fins de demonstração ou teste das funcionalidades do Software.

d) **Término da Licença.** A Licença expira automaticamente após decorrido o período pelo qual foi concedida. No caso de o Cliente não cumprir qualquer uma das disposições do presente Contrato, o Fornecedor terá o direito de rescindir o Contrato, sem prejuízo do exercício de qualquer direito ou do recurso a qualquer meio legal que seja aplicável ao Fornecedor numa tal eventualidade. Em caso de cancelamento da Licença, o Cliente deverá de

imediatamente proceder à eliminação, destruição ou devolução, a suas expensas próprias, do Software e de todas as cópias de segurança à ESET ou à loja junto da qual obteve o Software. Uma vez expirada a Licença, o Fornecedor terá ainda o direito de cancelar o acesso do Utilizador Final à utilização das funções do Software para as quais seja necessária uma ligação aos servidores do Fornecedor ou a servidores de terceiros.

**4. Funções com requisitos de ligação à Internet e recolha de dados.** Para funcionar corretamente, o Software requer ligação à Internet, necessitando ainda de se ligar regularmente aos servidores do Fornecedor ou aos servidores de terceiros, para efetuar a recolha de dados aplicáveis em conformidade com a Política de Privacidade. A Ligação à Internet e a recolha de dados aplicáveis são necessárias para que as seguintes funções do Software sejam executadas:

a) **Atualizações do Software.** O Fornecedor terá o direito de lançar atualizações do Software (doravante designadas por "Atualizações"), mas não ficará obrigado a disponibilizar tais Atualizações. Esta função encontra-se ativada segundo as definições-padrão do Software, pelo que as Atualizações serão assim instaladas automaticamente, exceto se o Utilizador Final tiver desativado a instalação automática de Atualizações. Para fins de disponibilização de Atualizações, é necessária uma verificação da autenticidade da Licença, incluindo informação sobre o Computador e/ou a plataforma onde o Software está instalado em conformidade com o disposto na Política de Privacidade.

b) **Encaminhamento de infiltrações e informações para o Fornecedor.** O Software possui funções que permitem recolher amostras de vírus informáticos e outros programas maliciosos, bem como objetos suspeitos, problemáticos, potencialmente indesejados ou desprovidos de segurança, tais como ficheiros, URLs, pacotes IP e pacotes ethernet (doravante conjuntamente designados por "Infiltrações") e em seguida enviá-las para o Fornecedor, incluindo, mas não se limitando a, informação sobre o processo de instalação, o Computador e/ou a plataforma onde o Software está instalado, informação acerca das operações e funcionalidades do Software, e elementos sobre os dispositivos existentes na rede local, tal como o tipo, o fornecedor, o modelo e/ou a designação do dispositivo (doravante designados por "Informação"). A Informação e as Infiltrações poderão conter dados (incluindo dados pessoais obtidos aleatoriamente ou inadvertidamente) sobre o Utilizador Final ou outros utilizadores do Computador no qual está instalado o Software, e ficheiros afetados por Infiltrações com os respetivos metadados associados.

A Informação e as Infiltrações poderão ser recolhidas pelas seguintes funções do Software:

i. A função LiveGrid Reputation System inclui a recolha e o envio de hashes unidirecionais relacionados com as Infiltrações para o Fornecedor. Esta função encontra-se ativada segundo as definições padrão do Software.

ii. A função LiveGrid Feedback System inclui a recolha e o envio de Infiltrações com metadados associados e Informação para o Fornecedor. Esta função poderá ser ativada pelo Utilizador Final durante o processo de instalação do Software.

O Fornecedor deverá utilizar a Informação e as Infiltrações recebidas somente para fins de análise e pesquisa de Infiltrações, melhoramento do Software e verificação de autenticidade da Licença, devendo tomar as medidas adequadas no sentido de garantir que a Informação e as Infiltrações recebidas são mantidas em segurança. Ao ativar esta função do Software, a Informação e as Infiltrações podem ser recolhidas e processadas pelo Fornecedor conforme especificado na Política de Privacidade e de acordo com os regulamentos legais aplicáveis. Poderá desativar estas funções a qualquer momento.

Para os fins do presente Contrato, será necessário recolher, processar e armazenar dados que permitam ao Fornecedor identificar o Cliente em conformidade com o disposto na Política de Privacidade. O Cliente declara ter tomado conhecimento de que o Fornecedor verifica pelos seus próprios meios se o Cliente está a utilizar o Software de acordo com as disposições constantes do presente Contrato. O Cliente declara por este meio aceitar que, para os fins do presente Contrato, é necessário que os seus dados sejam transferidos, durante a comunicação entre o Software e os sistemas informáticos do Fornecedor, ou os dos seus parceiros comerciais

como parte da rede de assistência e distribuição do Fornecedor, a fim de garantir a operacionalidade do Software e a autorização de utilização do Software, bem como para efeitos de proteção dos direitos do Fornecedor.

Após a celebração do presente Contrato, o Fornecedor, ou qualquer um dos parceiros comerciais que integram a rede de assistência e distribuição do Fornecedor, terá o direito de transferir, processar e armazenar dados essenciais que identifiquem o Cliente para fins de faturação, execução do Contrato e envio de notificações relativas ao seu Computador. Ao abrigo do presente Contrato, o Cliente aceita receber notificações e mensagens incluindo, mas não se limitando a, informação de marketing.

**Poderá encontrar informações detalhadas acerca da privacidade, da proteção de dados pessoais e dos seus direitos enquanto titular dos dados, na Política de Privacidade que está disponível no site de Internet do Fornecedor e à qual poderá aceder diretamente a partir do processo de instalação. Poderá ainda consultá-la a partir da secção de ajuda do Software.**

**5. Exercício dos Direitos do Utilizador Final.** Deverá exercer, pessoalmente ou por intermédio dos seus colaboradores, os direitos que lhe assistem na qualidade de Utilizador Final. O Cliente somente terá o direito de utilizar o Software para salvaguardar as suas operações e proteger os Computadores ou sistemas informáticos para os quais tenha sido obtida a Licença.

**6. Restrições aplicáveis aos direitos.** Deverá abster-se de copiar, distribuir, extrair componentes ou criar trabalhos derivados do Software. Ao utilizar o Software, o Cliente deverá respeitar as seguintes restrições:

(a) Poderá efetuar uma cópia do Software num suporte de armazenamento permanente como uma cópia de segurança para arquivo, desde que esta última não se encontre instalada nem seja utilizada em nenhum Computador. Quaisquer outras cópias que o Cliente efetue do Software serão consideradas como constituindo uma violação ao presente Contrato.

(b) Não está autorizado a utilizar, modificar, traduzir ou reproduzir o Software, nem a transferir os direitos de utilização do Software ou as cópias do Software, sob forma alguma à exceção do disposto no presente Contrato.

(c) Não deverá vender, conceder uma sublicença, alugar ou pedir emprestado o Software, nem utilizar o Software para efeitos da prestação de serviços comerciais.

(d) Não deverá proceder a engenharia inversa, descompilar ou desmontar o Software, ou de qualquer outro modo tentar descobrir o código fonte do Software, salvo na medida em que tal restrição seja expressamente proibida por lei.

(e) O Cliente compromete-se a utilizar o Software de forma a agir em conformidade com todas as leis aplicáveis na jurisdição na qual o Software é utilizado, incluindo, mas não se limitando a, restrições relativas a direitos de autor e outros direitos de propriedade intelectual.

(f) O Cliente compromete-se a utilizar o Software e as suas funções unicamente de uma forma que não limite a possibilidade de outros Utilizadores Finais acederem a estes serviços. O Fornecedor reserva-se o direito de limitar o âmbito dos serviços prestados a Utilizadores Finais com carácter individual, de modo a permitir a utilização dos serviços pelo maior número possível de Utilizadores Finais. Limitar o âmbito dos serviços poderá implicar igualmente a suspensão completa da possibilidade de utilizar qualquer uma das funções do Software, bem como a eliminação de Dados e informações, nos servidores do Fornecedor e nos servidores de terceiros, relativamente a uma função específica do Software.

(g) O Cliente compromete-se a não realizar quaisquer atividades que envolvam uma utilização da Chave de Licença que se afigure contrária ao disposto no presente Contrato ou que seja conducente à disponibilização da Chave de Licença a qualquer pessoa não autorizada a utilizar o Software, tal como a transferência da Chave de Licença usada ou não usada sob qualquer forma, bem como a abster-se da reprodução não autorizada, ou da

distribuição de Chaves de Licença geradas ou duplicadas, ou da utilização do Software em resultado da utilização de uma Chave de Licença obtida junto de outra fonte que não o Fornecedor.

**7. Direitos de Autor.** O Software e todos os direitos que lhe são inerentes, incluindo, sem carácter limitativo, os direitos patenteados e os direitos de propriedade intelectual, são detidos pela ESET e/ou pelos seus licenciantes. Os referidos direitos são protegidos ao abrigo das disposições contidas nos tratados internacionais e de todas as outras leis nacionais aplicáveis no país onde o Software é utilizado. A estrutura, a organização e o código do Software constituem elementos valiosos de segredo comercial e informação confidencial da ESET e/ou dos seus licenciantes. O Cliente não está autorizado a copiar o Software, excepto nos moldes estipulados na alínea (a) do Artigo 6.º. Quaisquer cópias que lhe seja permitido efetuar em conformidade com os termos do presente Contrato deverão apresentar os mesmos direitos de autor e avisos de propriedade que figuram no Software. Caso proceda a engenharia reversa, descompilação, desmontagem, ou de outro modo tente descobrir o código fonte do Software, cometendo assim uma violação do disposto no presente Contrato, o Cliente declara pela presente aceitar que toda e qualquer informação obtida por essa via será, automaticamente e irrevogavelmente, considerada como sendo transferida para o Fornecedor e por este último detida na íntegra, a partir do momento em que a referida informação passe a existir, não obstante o exercício, por parte do Fornecedor, de quaisquer direitos que lhe assistam no que diz respeito à violação da cláusula contratual.

**8. Direitos reservados.** O Fornecedor reserva-se todos os direitos sobre o Software, à exceção dos direitos que, nos termos do presente Contrato, sejam expressamente atribuídos ao Cliente na sua qualidade de Utilizador Final do Software.

**9. Versões em vários idiomas, software dual media, várias cópias.** Na eventualidade de o Software suportar múltiplas plataformas ou idiomas, ou se receber várias cópias do Software, o Cliente somente poderá utilizar o Software para o número de sistemas informáticos e para as versões em relação às quais obteve a Licença. O Cliente deverá abster-se de vender, alugar, conceder sublicenças, emprestar ou transferir versões ou cópias do Software que não utilize.

**10. Entrada em vigor e rescisão do Contrato.** O presente Contrato produzirá os seus efeitos na data à qual o Cliente manifeste o seu acordo relativamente aos termos contratuais. O Cliente poderá rescindir o presente Contrato a qualquer momento, bastando para tal proceder, com carácter permanente, à desinstalação, destruição ou devolução do Software, ficando os respetivos custos a seu cargo, bem como de todas as cópias de segurança e quaisquer materiais relacionados que lhe tenham sido facultados pelo Fornecedor ou pelos seus parceiros comerciais. Independentemente da forma de rescisão do presente Contrato, as disposições contidas nos Artigos 7.º, 8.º, 11.º, 13.º, 19.º e 21.º continuarão a considerar-se aplicáveis por tempo ilimitado.

**11. DECLARAÇÕES DO UTILIZADOR FINAL.** NA QUALIDADE DE UTILIZADOR FINAL, O CLIENTE RECONHECE QUE O SOFTWARE É FORNECIDO "TAL COMO ESTÁ", SEM GARANTIAS DE QUALQUER TIPO, QUER EXPRESSAS OU IMPLÍCITAS, E DE ACORDO COM O MÁXIMO PERMITIDO PELA LEGISLAÇÃO APLICÁVEL. NEM O FORNECEDOR, OS SEUS LICENCIANTES OU AS SUAS FILIAIS, NEM OS TITULARES DOS DIREITOS DE AUTOR PRESTAM QUAISQUER DECLARAÇÕES OU GARANTIAS, EXPRESSAS OU IMPLÍCITAS, NOMEADAMENTE, MAS SEM CARÁCTER LIMITATIVO, GARANTIAS DE COMERCIALIZAÇÃO OU DE ADEQUABILIDADE PARA UM DETERMINADO FIM, ASSIM COMO NÃO DECLARAM NEM PRESTAM QUAISQUER GARANTIAS DE QUE O SOFTWARE NÃO IRÁ INFRINGIR PATENTES, DIREITOS DE AUTOR, MARCAS REGISTRADAS OU OUTROS DIREITOS DE TERCEIROS. NÃO EXISTE QUALQUER GARANTIA POR PARTE DO FORNECEDOR OU DE UM TERCEIRO, DE QUE AS FUNÇÕES CONTIDAS NO SOFTWARE IRÃO SATISFAZER OS SEUS REQUISITOS OU DE QUE O FUNCIONAMENTO DO SOFTWARE SERÁ ISENTO DE ERROS OU INTERRUPTÕES. O CLIENTE DEVERÁ ASSUMIR PLENAMENTE O RISCO E A RESPONSABILIDADE NO QUE TOCA AO SOFTWARE SELECIONADO PODER NÃO ATINGIR OS RESULTADOS PRETENDIDOS, BEM COMO PELA SUA INSTALAÇÃO E UTILIZAÇÃO E PELOS RESULTADOS EFETIVAMENTE OBTIDOS COM O SOFTWARE.

**12. Inexistência de outras obrigações.** Do presente Contrato não advêm quaisquer outras obrigações para o Fornecedor e para os seus licenciantes, que não aquelas especificamente definidas neste documento.

**13. LIMITAÇÃO DE RESPONSABILIDADE.** NO ÂMBITO MÁXIMO PERMITIDO PELA LEI APLICÁVEL, SOB CIRCUNSTÂNCIA ALGUMA SERÁ IMPUTÁVEL AO FORNECEDOR, OU AOS SEUS FUNCIONÁRIOS OU LICENCIANTES, A RESPONSABILIDADE POR QUAISQUER PERDAS DE LUCROS, RENDIMENTOS, VENDAS, DADOS, OU POR QUAISQUER CUSTOS DE ABASTECIMENTO DE BENS OU SERVIÇOS DE SUBSTITUIÇÃO, OU A TÍTULO DE DANOS PATRIMONIAIS, DANOS PESSOAIS, SUSPENSÃO DE ATIVIDADE, PERDA DE INFORMAÇÃO COMERCIAL, OU AINDA QUAISQUER DANOS ESPECIAIS, DIRETOS, INDIRETOS, INCIDENTAIS, ECONÓMICOS, INDEMNIZATÓRIOS, PUNITIVOS, ESPECÍFICOS OU CONSEQUENTES, QUE TENHAM SIDO CAUSADOS POR QUALQUER MEIO E NÃO OBSTANTE SEREM DECORRENTES DO CONTRATO, OU DE DELITO, NEGLIGÊNCIA OU OUTRA TEORIA DE RESPONSABILIDADE, OU RESULTANTES DA UTILIZAÇÃO OU DA INCAPACIDADE DE UTILIZAR O SOFTWARE, AINDA QUE O FORNECEDOR OU OS SEUS LICENCIANTES OU FILIAIS TENHAM SIDO ALERTADOS PARA A POSSIBILIDADE DE OCORRÊNCIA DE TAIS DANOS. ATENDENDO A QUE ALGUNS PAÍSES E ALGUMAS JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO DE RESPONSABILIDADE, MAS PODERÃO PERMITIR UMA LIMITAÇÃO DA RESPONSABILIDADE, EM TAIS CASOS, A RESPONSABILIDADE DO FORNECEDOR, DOS SEUS FUNCIONÁRIOS, LICENCIANTES OU FILIAIS, DEVERÁ SER LIMITADA AO MONTANTE QUE O CLIENTE PAGOU PELA LICENÇA.

14. Nenhuma das cláusulas do presente Contrato deverá ser susceptível de prejudicar os direitos legais que assistam a um terceiro na qualidade de consumidor, caso este atue de forma contrária ao mesmo.

**15. Suporte técnico.** A ESET, ou terceiros cujos serviços lhes sejam delegados pela ESET, deverão proporcionar uma assistência técnica de acordo com os seus critérios, sem que sejam prestadas quaisquer garantias ou declarações. Caberá ao Utilizador Final efetuar cópias de segurança de todos os dados existentes e dos programas informáticos instalados, antes da prestação da referida assistência técnica. A ESET e/ou os terceiros delegados pela ESET declinam toda e qualquer responsabilidade pela eventual perda de dados, bens, software ou hardware, assim como pela perda de lucros, em consequência da prestação de suporte técnico. A ESET e/ou os terceiros delegados pela ESET reservam-se o direito de decidir que a resolução do problema ultrapassa o âmbito do suporte técnico. A ESET reserva-se o direito de recusar, suspender ou cessar a prestação de suporte técnico, a seu próprio critério. Para os fins da prestação de suporte técnico, poderão ser-lhe solicitadas as informações relativas à Licença, a Informação e outros dados em conformidade com a Política de Privacidade

**16. Transferência da Licença.** O Software poderá ser transferido de um Computador para outro, salvo em caso de indicação expressa em contrário nos termos do presente Contrato. Caso não se afigure contrário aos termos do presente Contrato, o Utilizador Final apenas terá o direito de transferir, a título permanente, a Licença e todos os direitos que advêm do presente Contrato para outro Utilizador Final, mediante o consentimento do Fornecedor e sujeito às seguintes condições (i) o primeiro Utilizador Final não deverá conservar quaisquer cópias do Software; (ii) a transmissão dos direitos deverá ser direta, i.e., do primeiro Utilizador Final para o novo Utilizador Final; (iii) o novo Utilizador Final deverá assumir todos os direitos e obrigações que incumbem ao primeiro Utilizador Final nos termos do presente Contrato; (iv) o primeiro Utilizador Final deverá facultar ao novo Utilizador Final a documentação que permite a verificação da autenticidade do Software conforme especificado no Artigo 17.º.

**17. Verificação da autenticidade do Software.** O Utilizador Final poderá fazer prova do seu direito a utilizar o Software de uma das seguintes formas: (i) através de um certificado emitido pelo Fornecedor ou por um terceiro por aquele nomeado; (ii) através de um contrato de licença exposto por escrito, caso tenha sido assinado algum contrato; (iii) através da apresentação de um e-mail enviado pelo Fornecedor e do qual constem os dados detalhados da licença (nome de utilizador e palavra-passe). Para fins de verificação da autenticidade do Software, poderá ser solicitada a informação relativa à Licença e os dados de identificação do Utilizador Final, em conformidade com a Política de Privacidade.

**18. Concessão de Licenças para autoridades públicas e Governo dos EUA.** O Software deverá ser facultado às autoridades públicas, nomeadamente ao Governo dos Estados Unidos, com os direitos e as restrições aplicáveis à licença, conforme descrito no presente Contrato.

**19. Conformidade com o controlo comercial.**

(a) O Cliente não poderá, de forma direta ou indireta, exportar, reexportar, transferir ou, de outra forma, disponibilizar o Software a qualquer pessoa, assim como utilizá-lo de qualquer maneira, ou estar envolvido em qualquer ato que coloque a ESET ou as empresas sob o seu controle, as suas empresas subsidiárias ou qualquer subsidiária das empresas sob o seu controle, assim como entidades controladas pelas empresas sob o seu controle (doravante referidas como "Afiliadas") em violação ou sujeitas às consequências negativas das Leis de Controlo do Comércio, nas quais se incluem

i. quaisquer leis que controlem, restrinjam ou imponham requisitos de licenciamento à exportação, reexportação ou transferência de bens, software, tecnologias ou serviços, emitidas ou adotadas por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Singapura, Reino Unido, União Europeia ou qualquer um dos seus Estados-membros, ou por qualquer país no qual as obrigações impostas pelo presente Contrato devam ser executadas, ou no qual a ESET ou qualquer uma das suas Afiliadas estejam constituídas ou operem (doravante referidas como "Leis de Controlo de Exportação") e

ii. quaisquer medidas económicas, financeiras, de comércio ou outras, de limitação, embargo, interdição de importação ou exportação, proibição de transferências de fundos ou ativos ou de execução de serviços, ou quaisquer outras medidas equivalentes impostas por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Singapura, Reino Unido, União Europeia ou qualquer um dos seus Estados-membros, ou por qualquer país no qual as obrigações impostas pelo presente Contrato devam ser executadas, ou no qual a ESET ou qualquer uma das suas Afiliadas estejam constituídas ou operem (doravante referidas como "Leis Restritivas").

(b) A ESET tem o direito de suspender ou terminar, com efeitos imediatos, as suas obrigações ao abrigo dos presentes Termos no caso de:

i. a ESET determinar, na sua razoável opinião, que o Utilizador violou ou poderá violar o disposto na Cláusula 19.a do presente Contrato; ou

ii. o Utilizador Final e/ou o Software estarem sujeitos às Leis de Controlo do Comércio e, como consequência, a ESET determinar, na sua razoável opinião, que a manutenção do exercício das suas obrigações ao abrigo do presente Contrato possa resultar na ESET ou nas suas Afiliadas se encontrarem em violação ou estarem sujeitas às consequências negativas das Leis de Controlo do Comércio.

(c) Nenhuma disposição do presente Contrato pretende induzir ou exigir a tomada de ação ou a abstenção de qualquer ato (ou a aceitação da tomada de ação ou da abstenção de tal ato) de qualquer uma das partes de qualquer forma que seja contraditória, penalizada ou proibida ao abrigo de quaisquer Leis de Controlo do Comércio aplicáveis, nem deve ser interpretada como tal.

**20. Notificações.** Quaisquer comunicações, e a devolução do Software e da Documentação, deverão ser endereçadas a: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

**21. Legislação aplicável.** O presente Contrato deverá reger-se e ser interpretado de acordo com as leis da República Eslovaca. O Utilizador Final e o Fornecedor acordam por este meio que os princípios relativos ao conflito de leis e a Convenção das Nações Unidas sobre os Contratos de Venda Internacional de Mercadorias não serão aplicáveis. O Cliente aceita expressamente que a resolução de quaisquer litígios ou reivindicações decorrentes do presente Contrato em relação ao Fornecedor, ou de quaisquer litígios ou reivindicações relacionados com a utilização do Software, será da competência do Tribunal Distrital de Bratislava I, manifestando assim expressamente o seu acordo no que respeita ao referido tribunal exercer a sua jurisdição.

**22. Disposições gerais.** Se uma ou mais cláusulas deste Contrato for inválida ou não aplicável, isso não deverá afetar a validade ou aplicação de qualquer uma das cláusulas restantes do Contrato. Essas deverão permanecer válidas e vigentes de acordo com os termos e condições estipulados neste documento. Em caso de discrepância entre versões do presente Contrato em diferentes línguas, deverá prevalecer a versão em inglês. O presente

Contrato somente poderá ser modificado por escrito e se assinado por um representante autorizado do Fornecedor ou por uma pessoa expressamente autorizada a agir nessa qualidade ao abrigo de uma procuração.

O presente documento constitui o Contrato integral firmado entre o Fornecedor e o Cliente no que diz respeito ao Software, devendo o presente Contrato prevalecer sobre quaisquer anteriores declarações, conversações, compromissos, comunicações ou campanhas publicitárias referentes ao Software.

EULA ID: HOM-ECS-20-01

## Política de Privacidade

A ESET, spol. s r. o., com sede social em Einsteinova 24, 851 01 Bratislava, República Eslovaca, inscrita na Conservatória do Registo Comercial administrada pelo Tribunal Distrital de Bratislava I, Secção Sro, Inscrição N.º 3586/B, sob o Número de Registo de Sociedade: 31 333 535, na qualidade de Responsável pelo Tratamento dos Dados (doravante designada por "ESET" ou "Nós") gostaria de ser transparente no que diz respeito ao tratamento de dados pessoais e privacidade dos nossos clientes. Para cumprir esse objetivo, estamos a publicar esta Política de Privacidade com a única finalidade de informar o nosso cliente ("Utilizador Final" ou o "Cliente") sobre os seguintes tópicos:

- Tratamento de Dados Pessoais,
- Confidencialidade dos Dados,
- Direitos do Titular dos Dados.

### Tratamento de Dados Pessoais

Os serviços fornecidos pela ESET implementados no nosso produto são fornecidos de acordo com os termos do Contrato de Licença do Utilizador Final ("EULA"), mas alguns destes serviços podem exigir uma atenção específica. Gostaríamos de lhe fornecer mais detalhes sobre a recolha de dados associada ao fornecimento dos nossos serviços. Prestamos vários serviços descritos no EULA e na documentação do produto, como um serviço de atualização, Livegrid®, proteção contra utilização indevida de dados, suporte, etc. Para garantir um bom serviço, necessitamos de recolher as seguintes informações:

- Atualização e outras estatísticas relacionadas com informação sobre o processo de instalação e o seu computador, incluindo a plataforma em que está instalado o nosso produto e informações sobre as operações e a funcionalidade dos nossos produtos, como o sistema operativo, informação de hardware, ID de instalação, ID de licença, endereço IP, endereço MAC e definições de configuração de produto.
- Hashes unidirecionais relacionados com infiltrações, como parte do Sistema de Reputação ESET LiveGrid®, que melhora a eficiência das soluções antimalware da ESET ao comparar os ficheiros analisados com uma base de dados de itens permitidos e proibidos na nuvem.
- Amostras e metadados suspeitos e não controlados que fazem parte do Sistema de Feedback ESET LiveGrid® que permitem à ESET reagir imediatamente às necessidades dos nossos utilizadores finais e manter a capacidade de resposta da ESET às mais recentes ameaças. A ESET requer que o Cliente nos envie

o infiltrações como amostras potenciais de vírus e outros programas maliciosos e objetos suspeitos, problemáticos, potencialmente não desejados ou potencialmente inseguros, como ficheiros executáveis, mensagens de e-mail sinalizadas pelo Cliente como spam ou sinalizadas pelo nosso produto;

o informação sobre dispositivos em rede local, como tipo, vendedor, modelo e/ou nome do dispositivo;

Informação sobre a utilização da Internet, como endereço IP e informação geográfica, pacotes IP, URLs e pacotes Ethernet;

Oficheiros de crash dump e informação incluída.

Não desejamos recolher os seus dados fora deste âmbito, mas, por vezes, é impossível evitá-lo. Os dados recolhidos acidentalmente podem ser incluídos no malware (recolhidos sem o seu conhecimento ou aprovação) ou como parte de nomes de ficheiros ou URLs e a ESET não pretende que sejam integrados nos nossos sistemas nem processar esses dados para a finalidade declarada na presente Política de Privacidade.

- A informação de licenciamento, tal como ID de licença e dados pessoais, como o nome, apelido, endereço ou endereço de e-mail, é necessária para fins de faturação, verificação de autenticidade de licença e fornecimento dos nossos serviços.
- Pode ser solicitada informação de contacto e dados incluídos nos seus pedidos de suporte para efeitos de fornecimento do serviço de suporte. Com base no canal escolhido pelo Cliente para nos contactar, poderemos recolher o seu endereço de e-mail, número de telefone, informação de licença, detalhes do produto e descrição do seu caso de suporte. Além disso, poder-lhe-á ser solicitado o fornecimento de outras informações para facilitar a prestação do serviço de suporte.

## **Confidencialidade dos Dados**

A ESET é uma empresa que opera internacionalmente através de entidades ou parceiros afiliados, como parte da nossa rede de distribuição, serviço e assistência. As informações processadas pela ESET podem ser transferidas para e partir de entidades ou parceiros afiliados para o desempenho do EULA, como por ex., para o fornecimento de serviços, suporte técnico ou para fins de faturação. Com base na localização e no serviço que o Cliente escolher, podemos ser obrigados a transferir os seus dados para um país sem decisão de adequabilidade da Comissão Europeia. Mesmo neste caso, cada transferência de informação está sujeita a legislação relativa à regulamentação da proteção de dados e apenas ocorre se exigido. Devem ser implementados sem qualquer exceção mecanismos de Escudo de Proteção, Cláusulas Contratuais Padrão, Regras Empresariais Vinculativas ou outra proteção adequada.

Estamos a fazer o nosso melhor para evitar que os dados sejam armazenados durante um período superior ao necessário durante a prestação dos serviços no âmbito do EULA. O período de retenção pode exceder o período de validade da sua licença de forma a proporcionar-lhe tempo para realizar uma renovação fácil e confortável. As estatísticas e outros dados minimizados e anonimizados do ESET LiveGrid® podem continuar a ser processados para fins de estatística.

A ESET implementa as medidas técnicas e de organização adequadas para garantir um nível de segurança que seja apropriado para os potenciais riscos. Estamos a fazer o nosso melhor para garantir a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e dos serviços de tratamento. No entanto, no caso de uma violação dos dados que resulte num risco para os seus direitos e liberdades, estamos preparados para notificar a autoridade de supervisão e os titulares dos dados. Enquanto titular dos dados, o Cliente tem o direito de submeter uma reclamação junto de uma autoridade de supervisão.

## **Direitos do Titular dos Dados**

A ESET está sujeita à regulamentação das leis da Eslováquia e está vinculada pela legislação relativa à proteção de dados enquanto Estado-Membro da União Europeia. Enquanto titular dos dados, pode exercer os seguintes direitos:

- direito de solicitar à ESET o acesso aos seus dados pessoais,
- direito de retificação dos seus dados pessoais caso não estejam corretos (bem como direito de alteração de dados pessoais incompletos),
- direito de solicitar a eliminação dos seus dados pessoais,
- direito de solicitar a restrição do processamento dos seus dados pessoais
- direito de objeção ao tratamento e
- direito de portabilidade dos dados.

Caso pretenda exercer o seu direito como titular dos dados ou tenha qualquer questão, envie-nos uma mensagem para:

ESET, spol. s r.o.  
Data Protection Officer (Responsável pela proteção de dados)  
Einsteinova 24  
85101 Bratislava  
República Eslovaca  
dpo@eset.sk