



VISÃO GERAL

# PROTECT

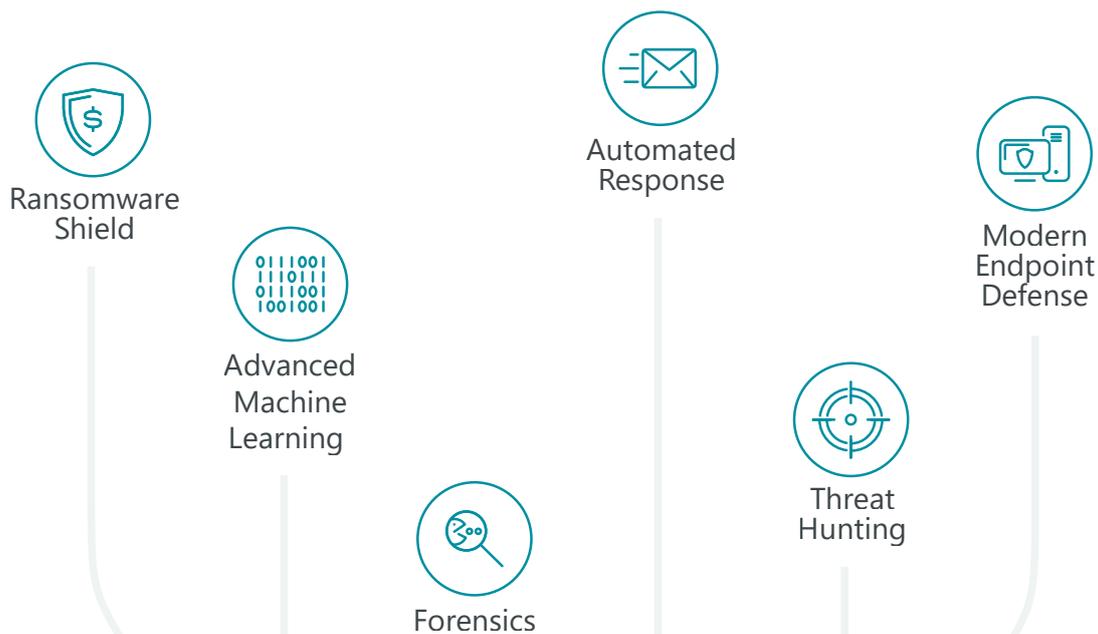
Uma plataforma de gerenciamento de segurança unificada que oferece uma visibilidade superior da rede

Progress. Protected.

# O que é um console de gerenciamento de segurança de endpoints?

O ESET PROTECT é um console UEM (Unified Endpoint Management) versátil, que fornece acesso à potente plataforma ESET PROTECT. É implementável no local ou a partir da nuvem e garante visibilidade em tempo real para endpoints remotos e no local, bem como relatórios completos e gerenciamento de segurança para todos os sistemas operacionais.

É um único painel de controle para todas as soluções de segurança da ESET implementadas na rede. É possível controlar as camadas de prevenção, detecção e resposta de endpoints em todas as plataformas, abrangendo desktops, servidores, máquinas virtuais e até mesmo dispositivos móveis gerenciados.



# O diferencial da ESET

## DA PREVENÇÃO À RESPOSTA

Em um único console, o ESET PROTECT combina o gerenciamento de diferentes soluções de segurança da ESET. Da prevenção de ameaças até a detecção e resposta, ele abrange toda a sua organização em múltiplas camadas, obtendo o melhor nível de proteção.

## REMEDIAÇÕES DE INCIDENTES COM UM CLIQUE

No painel principal, é possível a um administrador de TI avaliar rapidamente a situação e responder aos problemas. Ações como criar uma exclusão, enviar arquivos para análise posterior ou iniciar uma varredura estão disponíveis com um único clique. As exclusões podem ser realizadas por nome de ameaça, URL, hash ou combinação.

## RBAC AVANÇADO

Começando com o acesso protegido por MFA, o console está equipado com um sistema avançado de controle de acesso baseado em funções (RBAC). Atribua administradores e usuários do console a ramificações de rede e grupos de objetos específicos e detalhe conjuntos de permissões com alto grau de granularidade.

## PRONTO PARA MSP

Caso você seja um provedor de serviços gerenciados (MSP) que cuida das redes de seus clientes, você apreciará as capacidades completas de multilocalização do ESET PROTECT. As licenças do MSP são automaticamente detectadas e sincronizadas com o servidor de licenças, e o console permite realizar ações avançadas, como instalar/remover qualquer aplicativo de terceiros, executar scripts e comandos remotos, listar processos em execução, configurações de hardware, entre outros.

## COMPROVADA E CONFIÁVEL

A ESET está presente no setor de segurança há mais de 30 anos e seguimos aprimorando nossa tecnologia para nos mantermos preparados para as mais recentes ameaças. Como resultado, contamos com a confiança de mais de 110 milhões de usuários em todo o mundo. Nossa tecnologia é constantemente examinada e validada por testes de terceiros que comprovam a eficácia da nossa abordagem contra as ameaças mais recentes.

## RELATÓRIOS DINÂMICOS E PERSONALIZADOS

O ESET PROTECT oferece mais de 170 relatórios integrados e permite criar relatórios personalizados a partir de mais de mil pontos de dados. Assim, as organizações conseguem criar relatórios como desejarem. Uma vez criados, os relatórios podem ser configurados para serem gerados e enviados por e-mail em intervalos programados.

## FRAMEWORK DE AUTOMAÇÃO

Os grupos dinâmicos podem classificar dispositivos com base no seu status atual ou nos critérios de inclusão definidos. As tarefas podem, então, ser configuradas para acionar atividades como varreduras, alterações de política ou instalações/desinstalações de software, com base nas alterações dos membros do grupo dinâmico.

## SUORTE VDI TOTALMENTE AUTOMATIZADO

Um algoritmo abrangente de detecção de hardware é utilizado para determinar a identidade do dispositivo com base em seu hardware, permitindo a recriação de imagens e clonagem automatizadas de ambientes de hardware não persistentes. Assim, o suporte VDI da ESET não requer interação manual e é totalmente automatizado.

## SISTEMA DE NOTIFICAÇÕES TOTALMENTE PERSONALIZÁVEL

O sistema de notificações inclui um editor completo de "o que você vê é o que você obtém", que permite configurar as notificações para ter alertas de acordo com as informações específicas que deseja ser alertado.



# Recursos técnicos

## PAINEL DE CONTROLE ÚNICO

Todos os produtos de endpoints da ESET podem ser gerenciados a partir de um único console ESET PROTECT. Estão incluídos estações de trabalho, celulares, servidores e máquinas virtuais e os seguintes sistemas operacionais: Windows, macOS, Linux e Android.

## SUPORTE PARA XDR

Para melhorar ainda mais a consciência situacional e fornecer visibilidade em toda a sua rede, o ESET PROTECT trabalha em conjunto com o ESET Inspect, o componente de habilitação de XDR da plataforma ESET PROTECT. O ESET Inspect é multiplataforma (Windows, macOS e Linux), permite uma busca avançada e remediação de ameaças, e pode ser integrado perfeitamente ao seu centro de operações de segurança.

## FULL-DISK ENCRYPTION (FDE)

O Full Disk Encryption é parte do ESET PROTECT, gerenciando a criptografia de dados em endpoints Windows e Mac (FileVault), aprimorando a segurança dos dados e auxiliando as organizações a resolver a questão da conformidade com a regulamentação de dados.

## DEFESA AVANÇADA CONTRA AMEAÇAS

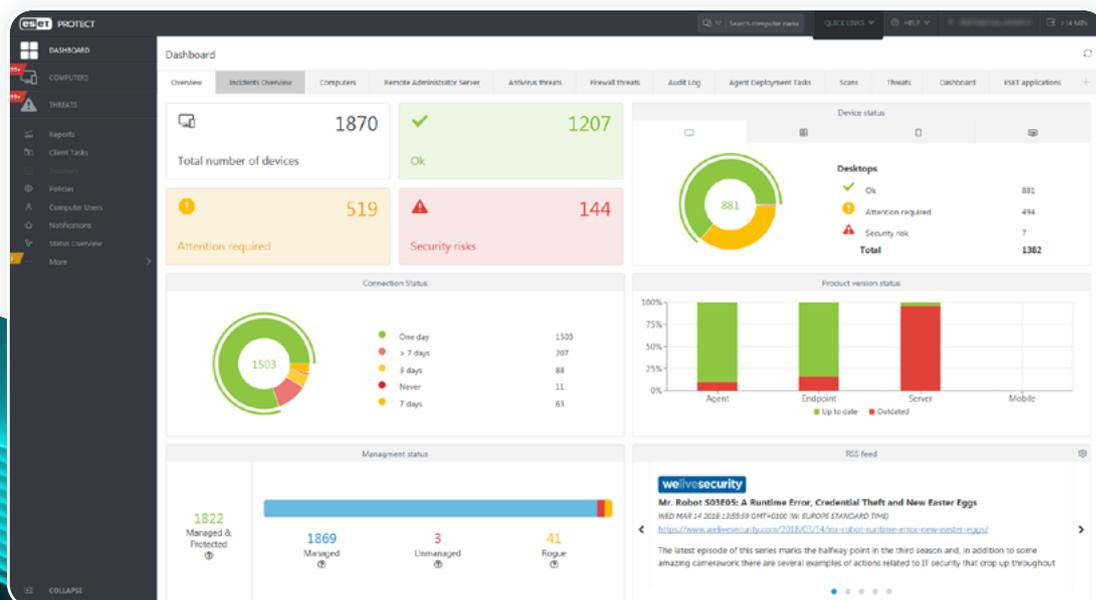
O suporte para defesa avançada contra ameaças melhora significativamente a detecção de ameaças de dia zero, como ransomwares, analisando rapidamente os arquivos suspeitos no poderoso sandbox com base na nuvem da ESET. Além disso, são executadas uma série de varreduras de malware altamente abrangentes, incluindo a execução e análise dos arquivos suspeitos em ambiente controlado na nuvem.

## INVENTÁRIO DE HARDWARE/SOFTWARE

O ESET PROTECT não apenas relata todos os aplicativos de software instalados em uma organização, mas também o hardware instalado.

## MULTILOCAÇÃO

É possível criar diversos usuários e grupos de permissão para permitir o acesso a uma parte limitada do console ESET PROTECT. Esse recurso possibilita a total organização das responsabilidades em grandes equipes corporativas. Também permite que mais ações sejam realizadas em um único local, agrupando dispositivos de forma dinâmica, com base na marca, modelo, sistema operacional, processador, memória RAM, espaço em disco e muitos outros itens.



Painel do ESET PROTECT

## CONTROLE GRANULAR DE POLÍTICAS

As organizações podem configurar diferentes políticas para o mesmo dispositivo ou grupo, podendo englobar políticas para permissões herdadas. Além disso, as organizações podem configurar as definições de política como configuráveis pelo usuário, permitindo bloquear variadas configurações dos usuários finais.

## COMPATÍVEL COM SIEM E SOC

O ESET PROTECT é compatível com as ferramentas de SIEM (gerenciamento de eventos e informações de segurança) e pode gerar todas as informações de log no formato JSON ou LEEF amplamente aceito, permitindo a integração com os centros de operações de segurança (SOC).

## ESET VULNERABILITY & PATCH MANAGEMENT

Rastreia ativamente as vulnerabilidades em sistemas operacionais e aplicativos comuns e permite a aplicação automática de patches em todos os endpoints gerenciados por meio do ESET PROTECT.

# Casos de uso

## Implantações de VDI

### PROBLEMA

Ambientes de hardware não persistentes geralmente requerem interação manual de um departamento de TI e criam grandes problemas de relatórios e visibilidade.

### SOLUÇÃO

- ✓ Após implantar uma imagem mestra nos dispositivos já presentes no ESET PROTECT, os dispositivos permanecerão relatando à instância anterior, mesmo após uma recriação completa da imagem do sistema.
- ✓ As máquinas que retornam ao seu estado inicial no final de um turno de trabalho não causarão duplicação de máquinas e, em vez disso, serão combinadas em um único registro.
- ✓ Ao implantar imagens não persistentes, é possível criar uma imagem que inclua o agente, de modo que, sempre que uma nova máquina for criada com outra impressão de hardware, ela criará automaticamente novos registros no ESET PROTECT.

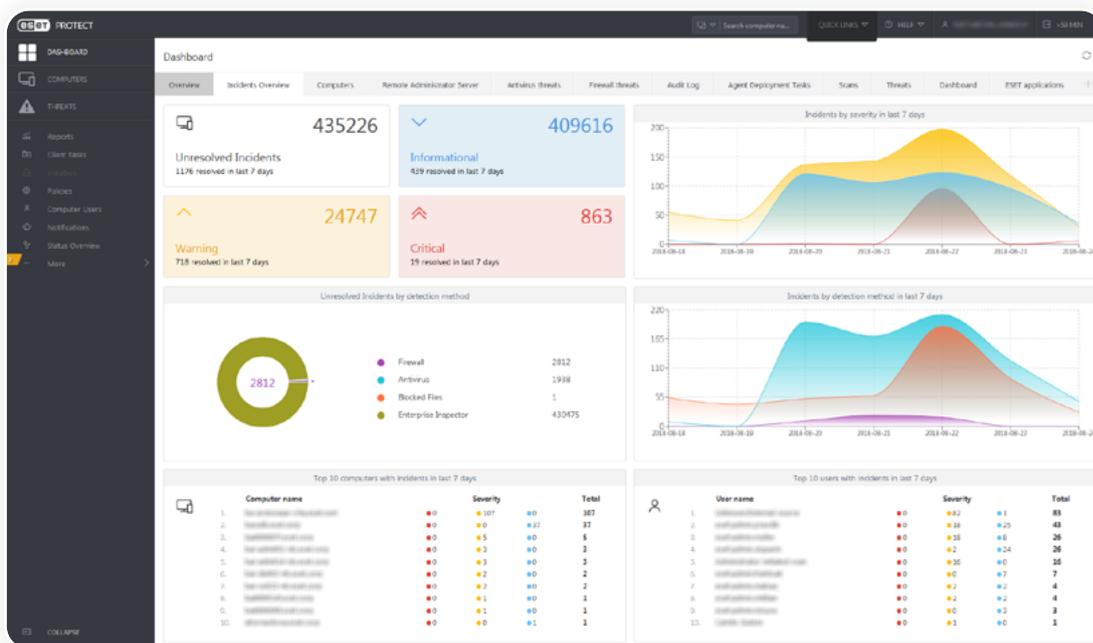
## Correção de software

### PROBLEMA

As organizações precisam saber quando um software não aprovado foi instalado e corrigir o software posteriormente.

### SOLUÇÃO

- ✓ Configure um grupo dinâmico dentro do ESET PROTECT para procurar um software indesejado específico.
- ✓ Crie uma notificação para alertar o departamento de TI quando um dispositivo atender a esse critério.
- ✓ Configure uma tarefa de desinstalação de software no console ESET PROTECT para ser executada automaticamente quando um dispositivo atender aos critérios do grupo dinâmico.
- ✓ Configure uma notificação para o usuário que aparecerá automaticamente na tela, indicando que ele cometeu uma violação de instalação de software ao instalar o software em questão.



Painel do ESET PROTECT - visão geral de incidentes

# Ransomwares

## PROBLEMA

Um usuário abre um e-mail malicioso contendo uma nova modalidade de *ransomwares*.

## SOLUÇÃO

- ✓ O departamento de TI recebe uma notificação por e-mail e seu SIEM sobre a detecção de uma nova ameaça em um determinado dispositivo.
- ✓ Com um único clique, é iniciada uma varredura no dispositivo infectado.
- ✓ Com outro clique, o arquivo é enviado para o ESET LiveGuard Advanced.
- ✓ Após confirmar que a ameaça foi contida, os avisos no console ESET PROTECT são apagados automaticamente.

# Desenvolvedores de código

## PROBLEMA

Programadores que trabalham com código em seus dispositivos de trabalho podem gerar falsos positivos devido à compilação de software.

## SOLUÇÃO

- ✓ O departamento de TI recebe uma notificação por e-mail e em seu SIEM de que uma nova ameaça foi encontrada.
- ✓ A notificação mostra que a ameaça foi originada no dispositivo de um desenvolvedor.
- ✓ Com um clique, o arquivo é enviado ao ESET LiveGuard Advanced para confirmar que não é malicioso.
- ✓ O departamento de TI realiza, com um clique, uma exclusão para evitar que futuros falsos positivos sejam exibidos nessa passa.

# Inventário de hardware e software

## PROBLEMA

As organizações precisam saber qual software está instalado em cada dispositivo, bem como o tempo de vida de cada dispositivo.

## SOLUÇÃO

- ✓ Visualize todos os softwares instalados, incluindo o número da versão, no registro do dispositivo.
- ✓ Visualize os detalhes de hardware de cada dispositivo, como aparelho, fabricante, modelo, número de série, processador, memória RAM, espaço em disco, entre outros.
- ✓ Execute relatórios para obter uma visão abrangente da organização, a fim de tomar decisões orçamentárias sobre futuras atualizações de hardware com base nas marcas e modelos atuais.

### COMO COMPRAR:

Basta adquirir qualquer uma das soluções para empresas diretamente em [nosso site](#)

### INICIE AGORA SEU TESTE DE 30 DIAS

Acesse sua avaliação gratuita de 30 dias para testar a solução completa, incluindo a proteção para *endpoints*.

# Sobre a ESET

**QUANDO A TECNOLOGIA PERMITE O PROGRESSO, A ESET® GARANTE A SUA PROTEÇÃO.**

A ESET traz mais de 30 anos de inovação impulsionada pela tecnologia e oferece as soluções de segurança cibernética mais avançadas do mercado. Nossa proteção moderna de endpoints é alimentada por exclusivas tecnologias de segurança multicamadas do ESET LiveSense®, combinadas com o uso contínuo de machine learning e computação em nuvem. Respaldados pela melhor inteligência e pesquisa de ameaças do mundo, os produtos da ESET oferecem o equilíbrio perfeito entre capacidades de prevenção, detecção e resposta. Com alta usabilidade e velocidade incomparável, estamos empenhados em proteger o progresso de nossos clientes, garantindo uma proteção abrangente.

## A ESET EM NÚMEROS

**MAIS DE 1  
BILHÃO**

usuários da internet  
protegidos

**MAIS DE  
400 MIL**

clientes  
empresariais

**195**

países e  
territórios

**13**

centros globais  
de P&D

## ALGUNS DE NOSSOS CLIENTES



protegida pela ESET desde  
2017 mais de 9 mil endpoints



protegida pela ESET desde  
2016 mais de 4 mil caixas de  
e-mail



protegida pela ESET desde  
2016 mais de 32 mil endpoints



Partner de segurança ISP  
desde 2008 2 milhões de  
clientes

## RECONHECIMENTO



A ESET recebeu o prêmio Business Security APPROVED da AV-Comparatives no Business Security Test, em dezembro de 2022.



A ESET alcança, de forma consistente, as melhores classificações na plataforma global de análise de usuários G2, tendo suas soluções apreciadas por clientes em todo o mundo.



A ESET foi reconhecida como um "Top Player" pelo quarto ano consecutivo no Radicati Advanced Persistent Threat Market Quadrant 2023.