

VISÃO GERAL DAS
SOLUÇÕES



FILE SECURITY

Proteja os servidores recorrendo a uma solução
multicamada fiável e sem compromissos

ESPECIALISTAS EM
CIBERSEGURANÇA DO SEU LADO



O que é uma solução de segurança de ficheiros?

Um produto de segurança de ficheiros é concebido para proteger os servidores centrais de uma organização contra ameaças. Este produto deve ser instalado em qualquer servidor não especializado para assegurar que os recursos organizacionais não sejam infetados. Hoje em dia, as empresas põem a sua organização em risco, permitindo que os utilizadores guardem ficheiros na partilha de rede da empresa, sem proteger adequadamente esses dados. Um único utilizador que salve um ficheiro malicioso para uma unidade de rede pode causar instantaneamente um efeito em cascata que faz com que os ficheiros da sua organização fiquem inacessíveis.

O **ESET File Security** fornece proteção avançada a todos os servidores gerais, de armazenamento de ficheiros na rede e servidores para diferentes utilizações. Esta solução presta especial atenção em assegurar que os servidores sejam estáveis e livres de conflitos, para manter janelas de manutenção e reinícios de sistema a um nível mínimo, a fim de não perturbar a continuidade do negócio.

Porquê soluções de segurança de ficheiros?

RANSOMWARE

O Ransomware tem sido uma preocupação constante para as indústrias em todo o mundo desde o Cryptolocker em 2013. Apesar desta ameaça existir há muito mais tempo, nunca foi uma grande preocupação das empresas. No entanto, agora uma única incidência de ransomware pode facilmente tornar um negócio inoperante através da encriptação de ficheiros importantes ou necessários. Quando uma empresa sofre um ataque de ransomware, rapidamente se apercebem de que as cópias de segurança que têm não são suficientemente recentes, pelo que a empresa sente necessidade de pagar o resgate. Com servidores, o ransomware pode ser um problema ainda maior devido à capacidade de um utilizador de guardar o ransomware para uma unidade de rede. As soluções ESET File Security fornecem camadas de defesa não só para prevenir ransomware, mas também para o detetar se ele alguma vez existir dentro de uma organização. É importante tentar prevenir e detetar o ransomware, pois cada vez que alguém paga um resgate, confere legitimidade económica para que criminosos continuem a recorrer a esta tática.

ATAQUES DIRECCIONADOS E VIOLAÇÕES DE DADOS

O atual panorama de cibersegurança está em constante evolução com novos métodos de ataque e ameaças nunca antes vistas. Quando acontece um ataque ou violação de dados, organizações ficam surpreendidas com a forma como as defesas são comprometidas, ou desconhecem completamente que o ataque até aconteceu. Depois de descobrirem finalmente o ataque, as organizações implementam reactivamente mitigações para impedir que ele se repita.

No entanto, esta medida não protege do próximo ataque que pode utilizar outro vetor de ameaça novinho em folha. O ESET File Security utiliza Threat Intelligence Information com base na sua presença global para priorizar e bloquear eficazmente as mais recentes ameaças antes que elas sejam disseminadas. Os servidores são tipicamente um alvo muito procurado devido ao fato de conterem dados sensíveis ou informações confidenciais. Para melhor proteger contra este aumento de ameaças, o ESET File Security conta com atualizações na cloud para responder rapidamente no caso de uma deteção falhada, pelo que não é preciso esperar por uma atualização através do processo normal.

ATAQUES SEM FICHEIROS

As novas ameaças de fileless malware - ou malware sem ficheiros - existem exclusivamente na memória do computador, tornando impossível que as proteções baseadas na digitalização de ficheiros o detetem. Além disso, alguns ataques de fileless malware aproveitam aplicações atualmente instaladas que estão incorporadas no sistema operativo para tornar ainda mais difícil a deteção de conteúdo malicioso. Por exemplo, a utilização do PowerShell nestes ataques é muito comum. As soluções de File Security apresentam mitigações para detetar aplicações mal formadas ou desviadas, de forma a proteger contra fileless malware. Outras empresas criaram scanners dedicados para verificar constantemente a memória de tudo o que é suspeito. Seja como for, as soluções de File Security têm sido sempre desafiadas a tentar ficar um passo à frente do mais recente malware.

As soluções da ESET fornecem camadas de defesa não só para prevenir malware, mas também para o detetar se ele alguma vez existir dentro da organização.

Quando ocorre um ataque ou violação de dados, as organizações ficam surpreendidas com o facto de as suas defesas terem sido comprometidas ou desconhecem completamente que o ataque tenha sequer acontecido.

Uma nova ameaça, chamada fileless malware, existe exclusivamente na memória do computador, tornando impossível que as proteções baseadas no scan de ficheiros a detetem.

“A ESET tem sido a nossa solução de segurança, garantindo fiabilidade ao longo de vários anos. Faz o que tem a fazer e não temos que ficar preocupados. ESET significa: fiabilidade, qualidade e serviço”.

—Jos Savelkoul, Team Leader ICT-Department; Hospital Zuyderland, Holanda;
10.000+ postos



OneDrive



Office 365



Azure

vmware®

Soluções de segurança ESET File Server

ESET File Security para Microsoft Windows Server

ESET File Security para Linux / FreeBSD

ESET File Security para Microsoft Azure

A diferença ESET

PROTEÇÃO MULTICAMADA

A ESET combina tecnologia multicamada, machine learning e conhecimentos humanos para fornecer aos clientes o melhor nível de proteção possível. A nossa tecnologia está constantemente a ajustar-se e a mudar para proporcionar o melhor equilíbrio de deteção, falsos positivos e desempenho.

SUPORTE INTER- PLATAFORMAS

As soluções de File Security da ESET suportam múltiplos sistemas operativos e plataformas, incluindo Windows Server, Office365 OneDrive, Linux/FreeBSD e Microsoft Azure. É possível gerir todas as soluções ESET a partir de um único painel.

DESEMPENHO INIGUALÁVEL

A maior preocupação de uma organização é muitas vezes o impacto no desempenho de uma proteção do endpoint. Os produtos ESET continuam a destacar-se na arena de desempenho e ganhar testes de terceiros que provam quão leves são as nossas soluções endpoint.

PRESENÇA MUNDIAL

A ESET tem escritórios em 22 países em todo o mundo, laboratórios de I&D em 13 e presença em mais de 200 países e territórios. Este argumento ajuda-nos a recolher dados para parar o malware antes que ele se espalhe por todo o mundo, bem como a estabelecer prioridades no que respeita a novas tecnologias baseadas nas ameaças mais recentes ou possíveis novos vetores de ataque.



Fonte: Network Performance Test, Business Security Software

"...o melhor testemunho? As estatísticas do nosso helpdesk: depois de implementarmos soluções ESET, os nossos técnicos de helpdesk não recebem chamadas - não têm de lidar com qualquer antivírus ou questões relacionadas com a guerra ao malware!"

— Adam Hoffman, IT Infrastructure Manager; Mercury Engineering, Irlanda; 1.300 postos

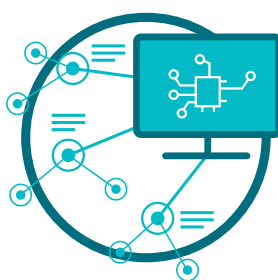
A tecnologia

Os nossos produtos e tecnologias baseiam-se em 3 pilares



ESET LIVEGRID®

Sempre que é verificada uma ameaça de dia zero, como seja ransomware, o ficheiro é enviado para o nosso sistema de proteção contra malware baseado na cloud - LiveGrid®, onde a ameaça é acionada e o comportamento é monitorizado. Os resultados deste sistema são fornecidos a todos os endpoints a nível mundial em apenas minutos, sem necessidade de quaisquer atualizações.



MACHINE LEARNING

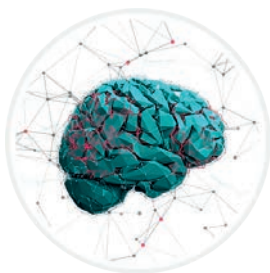
Utiliza o poder combinado das redes neurais e algoritmos escolhidos manualmente para rotular corretamente as amostras recebidas como limpas, potencialmente indesejadas ou maliciosas.



ESPECIALIZAÇÃO HUMANA

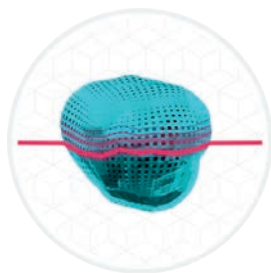
Investigadores de segurança de classe mundial que partilham conhecimentos aprofundados para assegurar a melhor informação sobre ameaças, 24 horas por dia.

Uma única camada de defesa não é suficiente para o cenário de ameaças em constante evolução. Todos os produtos de segurança ESET têm a capacidade de detetar malware antes de este ser executado, durante a sua ativação e pós-execução. A concentração em mais do que uma parte específica do ciclo de vida do malware permite-nos fornecer o mais alto nível de proteção possível.



MACHINE LEARNING

Todos os produtos finais ESET utilizam machine learning, para além de todas as outras camadas de defesa, desde 1997. A ESET recorre atualmente a esta tecnologia máquinas em conjunto com todas as nossas outras camadas de defesa. O Machine Learning é utilizado especialmente sob a forma de output consolidado e redes neurais.



ADVANCED MEMORY SCANNER

O Advanced Memory Scanner monitoriza o comportamento de um processo malicioso e avalia-o assim que ele se revela na memória. O Fileless malware opera sem necessitar de componentes persistentes no sistema de ficheiros que possam ser detetados convencionalmente. Só o Advanced Memory Scanner pode descobrir e parar com sucesso estes ataques maliciosos.



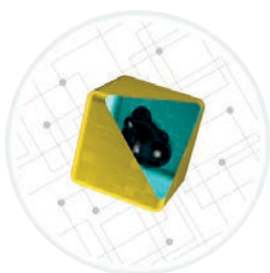
RANSOMWARE SHIELD

O ESET Ransomware Shield é uma camada adicional que protege os utilizadores de ransomware. Esta tecnologia monitoriza e avalia todas as aplicações executadas com base no seu comportamento e reputação. Foi concebido para detetar e bloquear processos que se assemelham ao comportamento de ransomware.



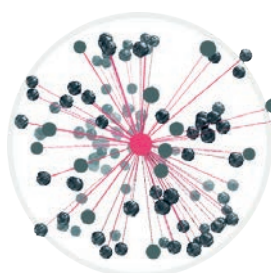
EXPLOIT BLOCKER

O ESET Exploit Blocker monitoriza aplicações tipicamente exploráveis (browsers, leitores de documentos, clientes de correio eletrónico, Flash, Java e outros), e em vez de visar apenas identificadores CVE específicos, centra-se em técnicas de exploração. Quando ativada, a ameaça é imediatamente bloqueada na máquina.



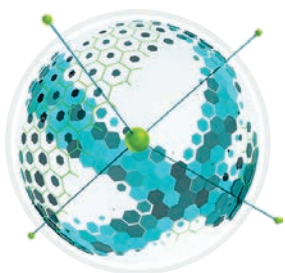
SANDBOX DENTRO DO PRODUTO

O malware de hoje em dia está muito bem escondido e tenta escapar à deteção tanto quanto possível. Para identificar o comportamento real escondido por baixo da superfície, utilizamos o sandboxing. Com a ajuda desta tecnologia, as soluções ESET emulam diferentes componentes de hardware e software de um computador para processar uma amostra suspeita num ambiente virtualizado isolado.



PROTEÇÃO CONTRA BOTNET

O ESET Botnet Protection deteta a comunicação maliciosa utilizada por botnets, e ao mesmo tempo identifica os processos nocivos. Qualquer comunicação maliciosa detetada é bloqueada e comunicada ao utilizador.



PROTEÇÃO CONTRA ATAQUES NA REDE

Esta tecnologia melhora a detecção de vulnerabilidades conhecidas ao nível da rede. Constitui outra camada importante de proteção contra a propagação de malware, ataques conduzidos pela rede e exploração de vulnerabilidades para as quais ainda não foi lançada ou implementada qualquer correção.



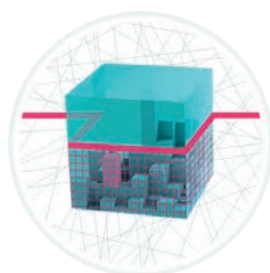
DETEÇÕES POR DNA

Os tipos de detecção variam de hashes muito específicos a ESET ADN Detections, que são definições complexas de comportamento malicioso e de características de malware. Muito embora o código malicioso possa ser facilmente modificado por atacantes, o comportamento dos objetos não pode ser alterado tão facilmente e as ESET ADN Detections foram concebidas para tirar partido deste princípio.



DETEÇÃO POR COMPORTAMENTO - HIPS

O Sistema de prevenção de intrusão baseado no host monitoriza a atividade do sistema e utiliza um conjunto pré-definido de regras para reconhecer comportamentos suspeitos no sistema. Além disso, o mecanismo de autodefesa HIPS impede o processo de levar a cabo a atividade nociva.



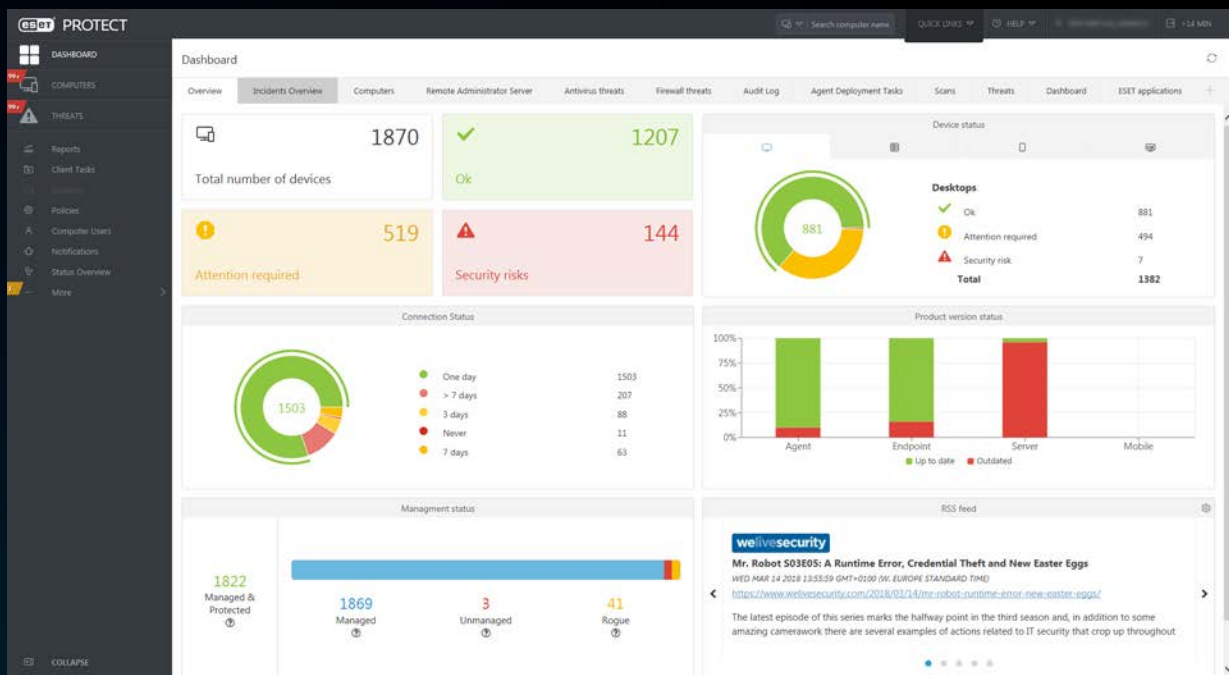
SCANNING AMSI/SCRIPT

As soluções ESET aproveitam a Antimalware Scan Interface (AMSI) para fornecer proteção melhorada contra malware para utilizadores, dados, aplicações, e carga de trabalho. Além disso, utilizam a interface protegida, que é um novo módulo de segurança integrado no Windows e que apenas permite carregar código assinado e de confiança para melhor proteger melhor contra ataques de injeção de código.

“O que mais se destaca é a sua forte vantagem técnica sobre outros produtos no mercado. A ESET oferece-nos segurança fiável, o que significa que posso trabalhar em qualquer projeto em qualquer altura sabendo que os nossos computadores estão 100% protegidos.”

— Fiona Garland, Business Analyst Group IT; Mercury Engineering, Irlanda;

1.300 postos



ESET PROTECT

Todas as soluções ESET endpoint são geridas a partir de um único painel na consola na cloud - a ESET PROTECT - assegurando a visão geral completa da sua rede.

“Quando encontramos a ESET, sabíamos que era a escolha certa: tecnologia fiável, deteção robusta, presença local e excelente apoio técnico: tudo o que precisávamos.”

— Ernesto Bonhoure, IT Infrastructure Manager; Hospital Alemán, Argentina,
1.500+ postos



Casos de utilização

Fileless malware

Caso de utilização: O malware sem ficheiros é uma ameaça relativamente nova e devido ao facto de apenas existir na memória, requer uma abordagem diferente da utilizada no tradicional malware baseado em ficheiros.

SOLUÇÃO

- ✓ Uma tecnologia ESET única, o Advanced Memory Scanner, protege contra este tipo de ameaça através da monitorização do comportamento de processos maliciosos e da sua monitorização uma vez que se ativam na memória.

- ✓ Se o ESET File Security não tiver a certeza de uma potencial ameaça, tem a capacidade de carregar a amostra para o Cloud Sandbox, o Dynamic Threat Defense, para tomar a melhor decisão sobre a questão.

- ✓ Se uma ameaça for confirmada, é possível reduzir a recolha de dados e tempo de investigação através do carregamento da ameaça na solução ESET Threat Intelligence para fornecer informações sobre como opera a ameaça.

Ameaças zero day

Caso de utilização: As ameaças de zero day são uma grande preocupação para as empresas, devido ao facto de estas não saberem como se protegerem contra algo que nunca viram antes.

SOLUÇÃO

- ✓ O ESET Threat Intelligence fornece dados sobre as mais recentes ameaças e tendências, bem como ataques direcionados para ajudar as empresas a prever e prevenir as mais recentes ameaças.

- ✓ Os produtos ESET endpoint baseiam-se na heurística e no machine learning como parte da abordagem multicamadas para prevenir e proteger contra malware nunca antes visto.

- ✓ O sistema de proteção contra malware na cloud da ESET protege automaticamente contra novas ameaças sem necessidade de esperar pela próxima atualização de deteção.

Ransomware

Caso de utilização: Algumas empresas querem a garantia adicional de que serão protegidas contra ataques de Ransomware. Além disso, visam assegurar-se de que as suas unidades de rede estão a salvo de encriptação.

SOLUÇÃO

- ✓ O Network Attack Protection tem a capacidade de prevenir ataques de ransomware parando as infeções ao nível da rede.

- ✓ A nossa defesa multicamada apresenta um modelo de sandbox no produto que tem a capacidade de detetar malware que tenta evadir à deteção.

- ✓ Beneficia do sistema de proteção contra malware na cloud da ESET para proteger automaticamente contra novas ameaças sem a necessidade de esperar pela próxima atualização de deteção.

- ✓ Todos os produtos contêm proteção pós-execução na forma de Ransomware Shield para assegurar que as empresas estão protegidas contra a encriptação de ficheiros maliciosos.

- ✓ Se o ESET File Security não estiver seguro quanto a uma potencial ameaça, ele tem a capacidade de carregar a amostra para a Cloud Sandbox - Dynamic Threat Defense - para fazer a melhor decisão quanto à potencial ameaça.

Sobre a ESET

Ao longo de mais de 30 anos, a ESET® tem vindo a desenvolver software e serviços de segurança de TI líderes da indústria, garantindo uma proteção imediata e abrangente contra as ameaças de cibersegurança em constante evolução enfrentadas por empresas e consumidores de todo o mundo.

A ESET é uma empresa privada. Sem dívidas nem empréstimos, temos liberdade para fazer aquilo que é preciso para garantir a melhor proteção de todos os nossos clientes.

A ESET EM NÚMEROS

110m+ de utilizadores em todo o mundo	400k+ clientes empresariais	200+ países e territórios	13 centros globais de investigação e desenvolvimento
---	--	--	--

ALGUNS DOS NOSSOS CLIENTES



**MITSUBISHI
MOTORS**

Drive your Ambition

protegida pela ESET desde 2017
mais de 14.000 endpoints

Canon

Canon Marketing Japan Group

protegido pelo ESET desde 2016
mais de 9.000 endpoints

Allianz 
Suisse

protegido pelo ESET desde 2016
mais de 4.000 caixas de correio



Parceiro de segurança de ISP desde 2008
base de 2 milhões de clientes

Porquê escolher a ESET



A ESET cumpre a norma [ISO/IEC 27001:2013](#), uma norma de segurança reconhecida e aplicável internacionalmente na implementação e gestão da segurança da informação. A certificação é assegurada pela entidade de certificação credenciada independente [SGS](#), e comprova a total conformidade da ESET com as melhores práticas da indústria.

PRÉMIOS DA ESET



RECONHECIMENTO DE ANALISTAS

Gartner

A ESET foi nomeada como única Desafiadora no 2019 Gartner Magic Quadrant para Plataformas de Proteção de Endpoint pelo segundo ano consecutivo.

FORRESTER®

A ESET foi classificada como Strong Performer no Forrester Wave(™): Endpoint Security Suites, 3.º trimestre de 2019.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

A ESET foi classificada como "Top Player" no relatório Radicati Endpoint Security de 2019 de acordo com dois critérios principais: funcionalidade e visão estratégica.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 de agosto de 2019. Gartner não endossa nenhum fornecedor, produto ou serviço descrito nas suas publicações de pesquisa. Os estudos da Gartner consistem nas opiniões da organização de estudos da Gartner e não devem ser interpretadas como declarações de facto. A Gartner isenta-se de todas as garantias, expressas ou implícitas, com relação a este estudo, incluindo quaisquer garantias de comercialização ou adequação a uma finalidade específica.

A Gartner Peer Insights é uma plataforma gratuita de análise e classificação por pares concebida para os decisores de software e serviços empresariais. As análises passam por um processo rígido de validação e moderação para garantir a autenticidade das informações. As análises Gartner Peer Insights são opiniões subjetivas de utilizadores finais individuais com base nas suas próprias experiências e não representam as opiniões da Gartner nem das suas afiliadas.



eset

ENJOY SAFER
TECHNOLOGY™