VISÃO GERAL DO PRODUTO

ENTERPRISE INSPECTOR

Desvende o desconhecido em sua rede com esta solução EDR de nossos especialistas em cibersegurança

CYBERSECURITY EXPERTS ON YOUR SIDE

O que é uma **solução de detecção e resposta para endpoint?**

O ESET Enterprise Inspector é uma ferramenta EDR sofisticada para a identificação de comportamentos anômalos e brechas, avaliação de risco, resposta a incidentes, investigações e reparos.

Ela monitora e avalia todas as atividades que acontecem na rede (por exemplo, usuário, arquivo, processo, registro, memória e eventos de rede) em tempo real e permite que você tome ações imediatas caso seja necessário.

Por que uma **detecção & resposta para endpoint?**

BRECHAS DE DADOS

Não apenas as empresas precisam identificar que uma brecha de dados ocorreu, como elas também precisam contê-la e repará-la. A maioria das empresas não está preparada para fazer esse tipo de investigação de forma plena e, ao invés, contratam pessoal externo para auxiliá-las. Hoje, as empresas precisam aumentar a visibilidade dentro de seus computadores para assegurar que ameaças emergentes, comportamento de risco de funcionários e aplicativos indesejados não coloquem seus lucros e sua reputação em risco.

As industrias com maior risco de brecha de dados são aquelas que tradicionalmente têm dados valiosos como o setor financeiro, de varejo, saúde e o setor público. Contudo, isso não significa que outras indústrias estejam salvas - somente que os hackers geralmente pesam o esforço versus o lucro.

AMEAÇAS AVANÇADAS PERSISTENTES (APT) E ATAQUES DIRECIONADOS

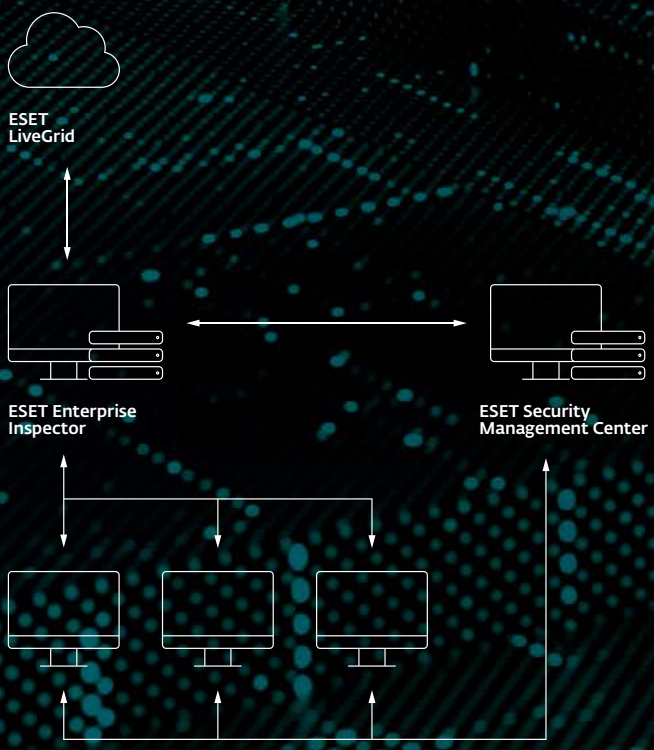
Os sistemas EDR são comumente utilizados para identificar APTs ou ameaças direcionadas via Threat Hunting; reduzem o tempo de resposta a incidentes; e proativamente previnem ataques futuros. Descobrir APTs em particular é importante para as grandes empresas já que a maioria das empresas hoje em dia não se sente preparada para os ataques mais novos que podem não ser detectados na rede por dias ou mesmo meses.

Fornece um **comportamento exclusivo e de detecção baseado em reputação , totalmente transparente para as equipes de segurança**, além de feedback em tempo real, coletado em mais de 100 milhões de endpoints em nosso LiveGrid..

VISIBILIDADE DA EMPRESA AUMENTADA

Ameaças internar e ataques de phishing são os maiores problemas para as grandes empresas. Os ataques de phishing são comumente usados contra grandes empresas por causa do grande número de funcionários como alvo. Existe a probabilidade de que um único funcionário morda a isca e acabe por comprometer todo o negócio. Ataques internos são outra ameaça para as grandes empresas, novamente porque o grande número de trabalhadores aumenta a probabilidade de que um deles possa trabalhar contra os melhores interesses da empresa.

Os sistemas EDR fornecem visibilidade aumentada, que é necessária para que as empresas vejam, compreendam, bloqueiem e reparem quaisquer problemas em todos os seus dispositivos. Isso inclui bloqueio de anexos de e-mail que contenham ameaças e assegurar que os funcionários estejam apenas acessando e utilizando os recursos empresarias apropriados.



Plataforma de Proteção para Endpoint da ESET
Segurança multicamada para endpoint onde cada uma das camadas envia dados para o ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Ferramenta EDR sofisticada que analisa uma vasta quantidade de dados em tempo real de modo que nenhuma ameaça deixará de ser detectada.

=

Prevenção completa, solução de detecção e resposta que permite analise rápida e reparo de quaisquer problemas de segurança na rede.

Hoje, as empresa precisam aumentar a visibilidade dentro dos computadores para assegurar que os **ataques emergentes, o comportamento de risco dos funcionários** e **os aplicativos indesejados** não coloquem os lucros e a reputação da empresa em risco.

A diferença da ESET

RESPOSTA SINCRONIZADA

Construído com base nas ofertas de segurança para endpoint ESET existentes, criando um ecossitema consistente que permite uma ligação cruzada de todos os objetos relevantes e reparação sincronizada dos incidentes. As equipes de segurança podem eliminar alguns processos, fazer o download de arquivos que disparam alertas ou simplesmente iniciar um desligamento ou reinicialização do computador diretamente
do console.

ARQUITETURA ABERTA

Fornece um comportamento único e detecção beseada em reputação que é completamente transparente para a segurança das equipes. Todas as regras são facilmente editáveis em XML para permitir refinamento ou fácil criação para combinar as necessidades específicas dos ambientes da empresa, incluindo as integrações SIEM.

ACESSO REMOTO

O ESET Enterprise Inspector possui recursos remotos do PowerShell que permitem aos engenheiros de segurança inspecionar e configurar remotamente os computadores da empresa para que uma resposta sofisticada possa ser alcançada sem interromper o fluxo de trabalho do usuário.

MULTIPLATAFORMAS

O ESET Enterprise Inspector suporta Windows e MacOS, o que o torna uma escolha perfeita para ambientes multiplataformas.

API PÚBLICA

O ESET Enterprise Inspector possui uma API que permite acessar e exportar detecções , cujas correções permitem uma integração efetiva com ferramentas, como SIEM, SOAR, ferramentas de emissão de bilhetes e muitas outras.

SENSIBILIDADE AJUSTADA

Suprima facilmente falsos alarmes ajustando a sensibilidade das regras de detecção para grupos de computadores e usuários diferentes. Combine critérios como nome de arquivo / path / hash / linha de comando / signatário para ajustar as condições de disparo.

MITRE ATT&CK™

O ESET Enterprise Inspector faz referência a suas detecções na estrutura MITRE Adversarial Tactics, Techniques e Common Knowledge (ATT&CK™), que fornece informações abrangentes com apenas um clique, mesmo para as ameaças mais complexas.

SISTEMA DE REPUTAÇÃO

A filtragem extensiva da ESET permite que os engenheiros de segurança filtrem cada aplicativo bem conhecido usando o sistema de reputação potente da ESET. Nosso sistema de reputação contém um banco de dados de centenas de milhões de bons arquivos para assegurar que as equipes de segurança gastem seu tempo no que for desconhecido e não em falsos positivos.

Casos de uso

Detecção de ameaças em profundidade - Ransomware

Hoje em dia, o ransomware tenta não ser notado na rede, silenciosamente se espalhando por quantos endpoints de rede for possível. Ele penetra dentro dos backups da máquina para assegurar que mesmo a volta para as imagens anteriores não prevenirão a execução imediata do ransomware.

O agente do ESET Enterprise Inspector estende a funcionalidade das soluções de segurança para endpoint da ESET e permite que você detecte proativamente o ransomware que talvez já exista na sua rede. Em um cenário típico de ransomware, um usuário recebe um e-mail com um documento anexado. O usuário então abre o documento em Word e a ele é pedido que rode o macros. Uma vez que o usuário roda o macros, um executável é jogado no sistema e começa a criptografar tudo o que ele pode, incluindo o mapeamento dos drives.

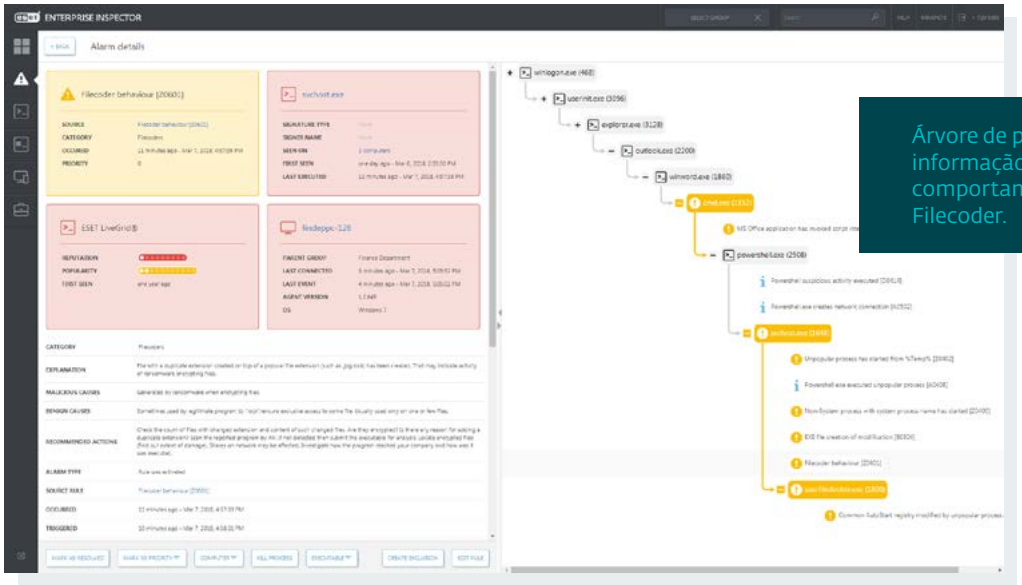
O ESET Enterprise Inspector permite que sua equipe de segurança veja os alertas deste tipo de comportamento e, com apenas alguns cliques, você pode ver o que foi afetado, onde e quando um executável específico, script ou ação foi feita e analisar a causa disso "desde a raiz".

CASO DE USO

Uma empresa quer ferramentas adicionais para detectar proativamente o ransomware em adição a ser notificado prontamente se um comportamento como o do ransomware tenha sido visto na rede.

SOLUÇÃO

- ✓ Insira regras para detectar aplicativos quando os estiver executando a partir de pastas temporárias.
- ✓ Insira regras para detectar arquivos Office (Word, Excell, PowerPoint) quando eles executarem scripts ou executáveis adicionais.
- ✓ Avisa se qualquer extensão de ransomware mais comum for vista em um dispositivo.
- ✓ Veja os alertas do Escudo Ransomware a partir do ESET Endpoint Security Solutions no mesmo console.



Árvore de processo e informação detalhada do comportamento de um Filecoder.

Detecção de comportamento e ofensores frequentes

O ponto mais fraco na segurança é frequentemente uma pessoa sentada em frente ao teclado, mesmo sem qualquer má intenção.

O ESET Enterprise Inspector facilmente identifica estes elementos fracos classificando os computadores pelo número de alarmes únicos disparados, Se um usuário dispara múltiplos alarmes, é um sinal claro de que a atividade deve ser validada.

CASO DE USO

Em sua rede, você tem usuários que são ofensores repetitivos no que diz respeito a malware, Os mesmos usuários continuam a ser infectados de tempos em tempos. Isso é por causa de comportamento de risco? Ou eles estão sendo alvos mais vezes do que outros usuários?

SOLUÇÃO

- ✓ Visualize facilmente usuários e dispositivos problemáticos.
- ✓ Complete rapidamente análise de causa raiz para achar a fonte das infecções.
- ✓ Faça reparos nos vetores infectados encontrados como e-mail, web e dispositivos USB.

Busca e bloqueio de ameaças

A força distintiva do ESET Enterprise Inspector está na busca de ameaças com abordagem que "procura uma agulha no palheiro".

Aplicando filtros aos dados classificados baseado na popularidade ou reputação do arquivo, assinatura digital, comportamento e informações contextuais, qualquer atividade maliciosa pode ser facilmente identificada e investigada. Configurar filtros múltiplos permite tarefas de busca de ameaças automatizada e pode ajustar o patamar de detecção para um ambiente específico da empresa.

Qualquer atividade maliciosa pode ser facilmente identificada e investigada.

CASO DE USO

Seu sistema de aviso antecipado ou centro de operações de segurança (SOC) entrega um novo alerta de ameaça. Quais são seus próximos passos?

SOLUÇÃO

- ✓ Aproveite o sistema de avisos antecipados para recuperar dados frente a ameaças iminentes ou novas.
- ✓ Busque em todos os computadores a existência de novas ameaças.
- ✓ Busque em todos os computadores por indicadores que comprovem que a ameaça existiu antes do aviso.
- ✓ Bloqueie a ameaça para que ela não possa se infiltrar na rede ou se executar dentro de uma empresa.

Visibilidade de rede

O ESET Enterprise Inspector é uma solução de arquitetura aberta, o que significa que sua equipe de segurança pode ajustar as regras de detecção descrevendo técnicas de ataque para ambientes específicos das empresas.

A arquitetura aberta também dá flexibilidade para configurar o ESET Enterprise Inspector para detectar violações das políticas da empresa sobre o uso de software específico como aplicativos torrent, armazenamentos de rede, navegadores Tor, iniciação de servidores próprios e outros softwares indesejados.

CASO DE USO

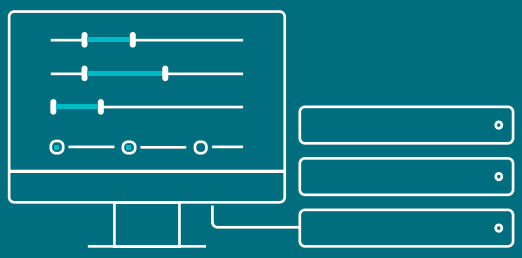
Algumas empresas estão preocupadas com os aplicativos que os usuários estão rodando nos sistemas. Você não somente precisa se preocupar com os aplicativos tradicionalmente instalados como também com os aplicativos portáteis que na verdade não se instalam. Como você pode manter o controle deles?

SOLUÇÃO

- ✓ Visualize facilmente e filtre todos os aplicativos instalados nos dispositivos.
- ✓ Visualize e filtre todos os scripts nos dispositivos.
- ✓ Bloqueie facilmente scripts ou aplicativos não autorizados para que não rodem.
- ✓ Faça reparos notificando os usuários sobre aplicativos não autorizados e os desinstale automaticamente.

Você não somente precisa se preocupar com os aplicativos tradicionalmente instalados como também com os aplicativos portáteis que na verdade não se instalam. Como você pode manter o controle deles?

A equipe de segurança pode **ajustar as regras de detecção** descrevendo técnicas de ataque para ambientes específicos da empresa.



Investigação e reparo de alerta de contexto

A "maliciosidade" de uma atividade depende de seu contexto.

Atividades feitas em computadores de administradores de rede são muito diferentes das feitas no departamento de finanças. Com o agrupamento apropriado dos computadores, as equipe de segurança podem facilmente identificar se este usuário pode executar uma atividade específica nesta máquina. A sincronização dos grupos de endpoint do ESET Security Management Center e as regras do ESET Enterprise Inspector fornecem resultados excelentes de informações contextuais.

CASO DE USO

Os dados são tão bons quanto o contexto por trás deles. Para decisões apropriadas, você precisa saber o que os alertas são, em quais dispositivos eles ocorreram e quais usuários estão disparando-os.

SOLUÇÃO

- ✓ Identificar e classificar todos os computadores de acordo com o Active Directory, agrupamentos automáticos ou agrupamentos manuais.
- ✓ Permitir ou bloquear aplicativos ou scripts baseado em agrupamentos de computadores.
- ✓ Permitir ou bloquear aplicativos ou scripts baseado em usuários.
- ✓ Receber apenas notificações para certos grupos.

Configuração fácil e resposta fácil - não é necessário equipe de segurança

Mesmo que a empresa tenha equipes de segurança dedicadas, frequentemente é difícil priorizar rapidamente e decidir os próximos passos entre os alarmes disparados.

Portanto, para cada alarme disparado, há próximos passos propostos para que os reparos sejam feitos. Quando o ESET Enterprise Inspector identifica a ameaça, ele fornece uma reposta rápida funcionalmente. Arquivos específicos pode ser bloqueados por hash, processos podem ser eliminados e colocados em quarentena e máquinas selecionadas podem ser isoladas ou desligadas remotamente.

CASO DE USO

Nem todas as empresas têm equipes de segurança dedicadas e adicionar e implementar regras de detecção avançada pode ser uma luta.

SOLUÇÃO

- ✓ Mais de 180 regras preconfiguradas integradas.
- ✓ Responda facilmente clicando rapidamente em um único botão pata bloquear, eliminar ou colocar dispositivos em quarentena.
- ✓ Reparos propostos e próximos passos estão integrados nos alarmes.
- ✓ Regras são editáveis via XML e permite facilmente o ajuste ou a criação de novas regras.

A "maliciosidade" de uma atividade depende de seu contexto. A sincronização dos grupos de endpoint do ESET Security Management Center e as regras do ESET Enterprise Inspector fornecem resultados excelentes das informações de contexto.

Para cada alarme disparado, há próximos passos propostos para que os reparos sejam feitos.

As possibilidades

CAÇA ÀS AMEAÇAS

Aplicar filtros aos dados para classificar baseado na popularidade, assinatura digital, comportamento ou informações contextuais. Configurar filtros múltiplos permite uma caça às ameaças automatizada que pode ser customizada para cada ambiente de empresa. Permite uma caça fácil às ameaças, incluindo APTs e ataques direcionados.

DETECÇÃO DE INCIDENTE (ANÁLISE DE CAUSA RAIZ)

Veja rápido e facilmente todos os incidentes de segurança na seção de alarmes, Com apenas alguns cliques, as equipes de segurança podem ver uma análise completa de causa raiz que inclui: o que foi afetado, onde e quando o executável, script ou ação foi realizado.

INVESTIGAÇÃO E REPARAÇÃO

Use um conjunto de regras construído internamente ou crie suas próprias regras para responder a indicentes detectados. Cada alarme disparado apresenta um próximo passo proposto para ser executado na reparação. A funcionalidade de resposta rápida permite que arquivos específicos sejam bloqueados por um hash, que processos sejam eliminados e colocadods em quarentena e que máquinas selecionadas sejam isoladas ou desligadas remotamente. Essa funcionalidade de resposta rápida ajuda a assegurar que cada um dos incidentes não caia em brechas.

ISOLAMENTO COM UM CLIQUE

Defina políticas de acesso à rede para interromper rapidamente os movimentos laterais do malware. Isole um dispositivo comprometido da rede com apenas um clique na interface EEI. Além disso, remova facilmente os dispositivos do estado de contenção.

PONTUAÇÃO

Priorize a gravidade dos alarmes com a funcionalidade de pontuação que atribui um valor de gravidade aos incidentes e permite que o administrador identifique com facilidade computadores com maior probabilidade de um possível incidente.

TAGGING

Atribua e cancele a atribuição de tags para filtragem rápida de objetos EEI, como computadores, alarmes, exclusões, tarefas, executáveis, processos e scripts. As tags são compartilhadas entre os usuários e, uma vez criadas, podem ser atribuídas em questão de segundos.

COLETA DE DADOS

Visualize dados abrangentes sobre um módulo executado recentemente: tempo de execução, usuário que executou, tempo de permanência e dispositivos atacados.

LOGIN SEGURO

Habilite a autenticação de dois fatores - uma camada extra de segurança para sua conta de administrador para impedir que um invasor faça login, mesmo que tenha sua senha.

INDICADORES DE DETECÇÃO COMPROMETIDA

Visualize e bloqueie módulos baseados em mais de 30 indicadores diferentes, incluindo hash, modificações de registro, modificações de arquivo e conexões de rede.

DETECÇÃO DE ANOMALIA E COMPORTAMENTO

Cheque as ações que foram realizadas por um executável e utilize o sistema de reputação do ESET LiveGrid para determinar rapidamente se processos executados são seguros ou suspeitos. Agrupamento de computadores por usuário ou departamento permite que as equipes de segurança identifiquem se o usuário pode realizar ações específicas ou não.

VIOLAÇÃO DA POLÍTICA DA EMPRESA

Bloqueie módulos maliciosos de serem executados em sua rede. Detecte violações de políticas sobre o uso específico de softwares como aplicativos torrent, armazenamento em, navegação em Tor ou outro software indesejado.

Sobre a ESET

Por mais de 30 anos, a ESET tem desenvolvido software e serviços de segurança líderes da indústria, entregando proteção instantânea e abrangente contra as ameaças de cibersegurança em desenvolvimento para empresas e clientes em todo o mundo.

A ESET é uma empresa privada. Sem dívidas ou empréstimos, somos livres para fazer o necessário para garantir a máxima proteção para todos os nossos clientes.

ESET EM NÚMEROS

+ de 110
milhões de usuários no mundo todo

+ de 400
mil clientes corporativos

+ de 200
países e territórios

13
centros globais de pesquisa e desenvolvimento

NOSSOS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

Canon
Canon Marketing Japan Group

Allianz
Suisse

T

A ESET está em conformidade com a ISO/IEC 27001:2013, um padrão de segurança aplicável e reconhecido internacionalmente na implementação e no gerenciamento de segurança da informação. A certificação é concedida pelo organismo terceirizado de certificação acreditado SGS e demonstra a total conformidade da ESET com as melhores práticas líderes do setor.

MITRE | ATT&CK™

A ESET é um colaborador dedicado ao MITRE ATT&CK. Por ser um dos fornecedores e colaboradores ativos mais referenciados, a ESET confirma seu compromisso de fornecer a melhor proteção para a comunidade e nossos clientes.

RECONHECIMENTOS E PRÊMIOS DA INDÚSTRIA

RECONHECIMENTOS DO ANALISTA

Gartner

Pelo segundo ano consecutivo, a ESET foi nomeada Challenger única no Quadrante Mágico do Gartner de 2019 para Proteção de pontos finais.

FORRESTER®

A ESET é reconhecida como "Strong Performer" no Forrester Wave™: soluções de segurança para endpoints, terceiro trimestre de 2019.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

A ESET foi destacada como "Melhor Player" no Relatório de Segurança Radicati 2019 por suas funcionalidades e visão estratégica.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure information is authentic. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

ENJOY SAFER TECHNOLOGY™