VISÃO GERAL

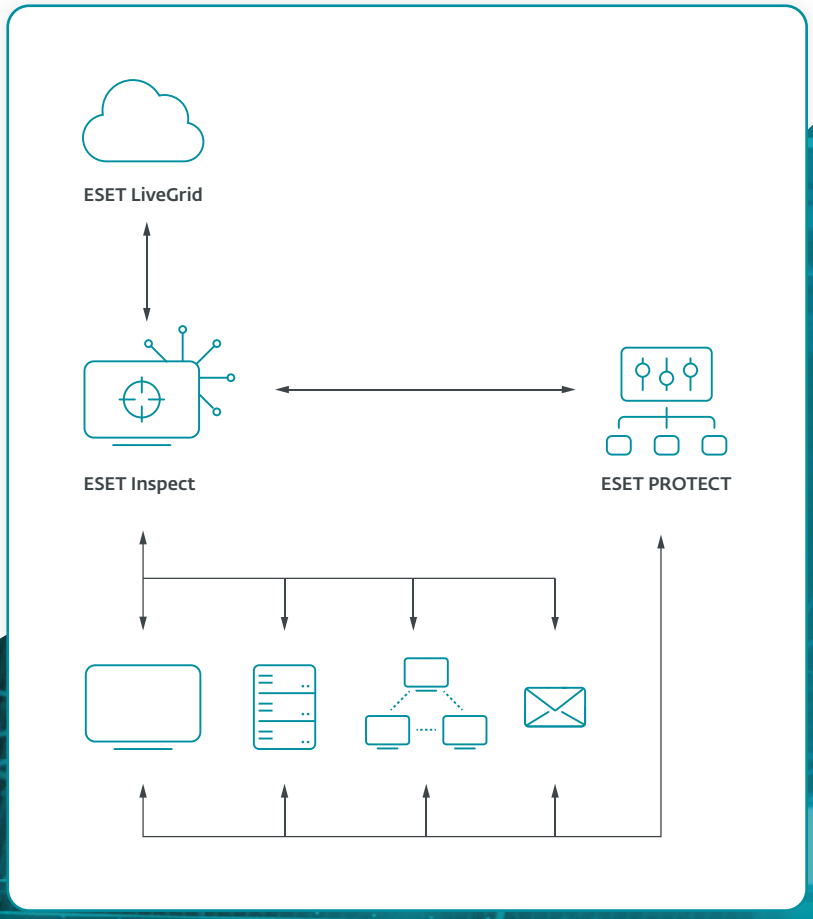
INSPECT

O componente que habilita o XDR na plataforma ESET PROTECT, oferecendo a prevenção de violações, visibilidade aprimorada e remediação

O que é uma solução de detecção e resposta estendida (XDR)?

O ESET Inspect, componente de habilitação de XDR na plataforma ESET PROTECT, é uma ferramenta para identificação de comportamentos anômalos e violações, avaliação de riscos, resposta a incidentes, investigações e remediação.

Ele permite aos respondentes de incidentes monitorarem e avaliarem todas as atividades na rede e nos dispositivos conectados. Além disso, auxilia a automatizar ações imediatas de remediação, caso seja necessário. As mais de 800 regras de detecção da ESET (e contando) possibilitam uma abrangente busca de ameaças.



O diferencial da ESET

PREVENÇÃO, DETECÇÃO E RESPOSTA COMPLETAS

Permite a análise rápida e a remediação de qualquer problema de segurança na sua rede. A segurança multicamadas da ESET, em que cada

camada envia dados para o ESET Inspect, analisa grandes quantidades de dados em tempo real, para que nenhuma ameaça passe despercebida.

SOLUÇÃO DE UM FORNECEDOR QUE PRIORIZA A SEGURANÇA

A ESET tem combatido ameaças cibernéticas há mais de 30 anos. Como uma empresa de base científica, esteve na vanguarda de desenvolvimentos como *machine learning*, tecnologia na nuvem e, agora, o XDR.

É MELHOR PREVENIR DO QUE REMEDIAR

A abordagem da ESET para XDR está estreitamente relacionada aos seus produtos de prevenção multipremiados. Devido ao compromisso com o desenvolvimento de tecnologias de detecção de alta qualidade, a tecnologia de prevenção da ESET é referência mundial.

VISIBILIDADE DETALHADA DA REDE

Com regras de detecção transparentes (a ESET tem, crescentes, mais de 800), IoC (indicadores de comprometimento) avançados e capacidade de pesquisa, uma análise detalhada de executáveis da sua rede permitirá que você identifique qualquer atividade suspeita.

FLEXIBILIDADE DE IMPLEMENTAÇÃO

Deixamos você decidir a forma de implementação da sua solução de segurança: o ESET Inspect pode ser executado por meio de seus próprios servidores no local ou por uma instalação com base nuvem, permitindo que você ajuste sua configuração de acordo com suas metas de TCO e capacidade de hardware.

PRONTA PARA USO

A solução da ESET tem funcionamento imediato, mas é potente o suficiente para permitir modificações granulares por parte de especialistas em detecção de ameaças experientes.

MITRE ATT&CK

O ESET Inspect referência suas detecções com a estrutura MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), que — com apenas um clique — fornece informações abrangentes até mesmo sobre as ameaças mais complexas.

SISTEMA DE REPUTAÇÃO

A filtragem extensiva permite aos engenheiros de segurança identificarem cada aplicativo todos os aplicativos conhecidos, utilizando o robusto sistema de reputação da ESET. O sistema da ESET contém um banco de dados de centenas de milhões de arquivos benignos para garantir que as equipes de segurança dediquem seu tempo aos arquivos desconhecidos e potencialmente maliciosos, em vez de falsos positivos.

AUTOMATIZAÇÃO E PERSONALIZAÇÃO

Ajuste facilmente o ESET Inspect ao nível de detalhe e automatização que você precisa. Escolha o nível de interação desejado — e o tipo e quantidade de dados a serem armazenados — durante a configuração inicial e com a ajuda de perfis de usuário pré-definidos. Em seguida, deixe o modo de aprendizagem mapear o ambiente da sua organização e sugerir exclusões para falsos positivos, quando necessário.

Capacidades da solução

SISTEMA DE GERENCIAMENTO DE INCIDENTES

Agrupe objetos como detecções, dispositivos, executáveis ou processos em unidades lógicas para visualizar eventos potencialmente maliciosos em uma linha do tempo, com ações de usuário relacionadas. O ESET Inspect sugere automaticamente ao respondente de incidente todos os eventos e objetos relacionados que podem ser de grande ajuda nas etapas de triagem, investigação e resolução de um incidente.

OPÇÕES DE RESPOSTA EM TEMPO REAL

O ESET Inspect vem com ações de resposta de fácil acesso em apenas um clique, como reiniciar e desligar um endpoint, isolar os endpoints do restante da rede, executar uma varredura sob demanda, encerrar quaisquer processos em execução e bloquear qualquer aplicativo com base em seu valor de hash. Além disso, devido à opção de resposta em tempo real do ESET Inspect, chamada Terminal, os profissionais de segurança podem se beneficiar do conjunto completo de opções de investigação e remediação no PowerShell.

ANÁLISE DE CAUSA RAIZ

Visualize facilmente a análise de causa raiz e a árvore de processos completa de qualquer cadeia de eventos potencialmente maliciosos, aprofunde-se no nível de detalhe desejado e tome decisões informadas com base no contexto fornecido e nas explicações para as causas benignas e maliciosas, elaboradas por nossos especialistas em malware.

API PÚBLICA

O ESET Inspect dispõe de uma API REST pública, que permite acessar e exportar detecções e sua remediação, permitindo a integração efetiva com ferramentas como SIEM, SOAR, ferramentas de help desk e muitas outras.

MÚLTIPLOS INDICADORES DE COMPROMETIMENTO

Visualize e bloqueie módulos com base em mais de 30 indicadores diferentes, incluindo hash, alterações no registro, alterações de arquivo e conexões de rede.

THREAT HUNTING (CAÇA A AMEAÇAS)

Utilize a poderosa busca baseada em IoC e aplique filtros aos dados brutos para classificação com base na popularidade do arquivo, reputação, assinatura digital, comportamento ou outras informações contextuais. A configuração de diversos filtros permite uma busca fácil e automatizada de ameaças e resposta a incidentes, incluindo a capacidade de detectar e interromper APTs e ataques direcionados.

ACESSO REMOTO SEGURO E TRANQUILO

A resposta a incidentes e os serviços de segurança são tão eficientes quanto fáceis de acessar, tanto em termos da conexão do respondente ao console, quanto da conexão com os *endpoints*. A conexão funciona em velocidade quase em tempo real, com medidas de segurança máximas aplicadas, tudo sem a necessidade de ferramentas de terceiros.

ISOLAMENTO EM UM CLIQUE

Defina políticas de acesso à rede para interromper rapidamente o movimento lateral de malware. Isole um dispositivo comprometido da rede com apenas um clique na interface do ESET Inspect. Além disso, remova dispositivos do estado de contenção facilmente.

DETECÇÃO DE ANOMALIAS E COMPORTAMENTOS

Verifique as ações executadas por um arquivo executável e utilize o sistema de reputação LiveGrid® da ESET para avaliar rapidamente se os processos executados são seguros ou suspeitos. O monitoramento de incidentes anômalos relacionados ao usuário é possível devido a regras específicas escritas para serem acionadas por comportamento, não por malware simples ou detecções baseadas em assinaturas. O agrupamento de dispositivos por usuário ou departamento permite às equipes de segurança identificarem se o usuário tem permissão para executar uma determinada ação.

MARCAÇÕES

Atribua e remova tags para filtragem rápida de objetos, como dispositivos, 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.

DETECÇÃO DE VIOLAÇÃO DE POLÍTICAS DA EMPRESA

Bloqueie a execução de módulos maliciosos em qualquer dispositivo da rede da sua organização. A arquitetura aberta do ESET Inspect oferece flexibilidade para detectar violações de políticas aplicadas ao uso de softwares específicos, como aplicativos de torrent, armazenamento em nuvem, navegação Tor ou outros softwares indesejados.

ARQUITETURA ABERTA E INTEGRAÇÕES

O ESET Inspect oferece detecção única baseada em comportamento e reputação, totalmente transparente para as equipes de segurança. Todas as regras são facilmente editáveis via XML para permitir ajustes refinados ou facilmente criadas para atender às necessidades de ambientes corporativos específicos, incluindo integrações do SIEM.

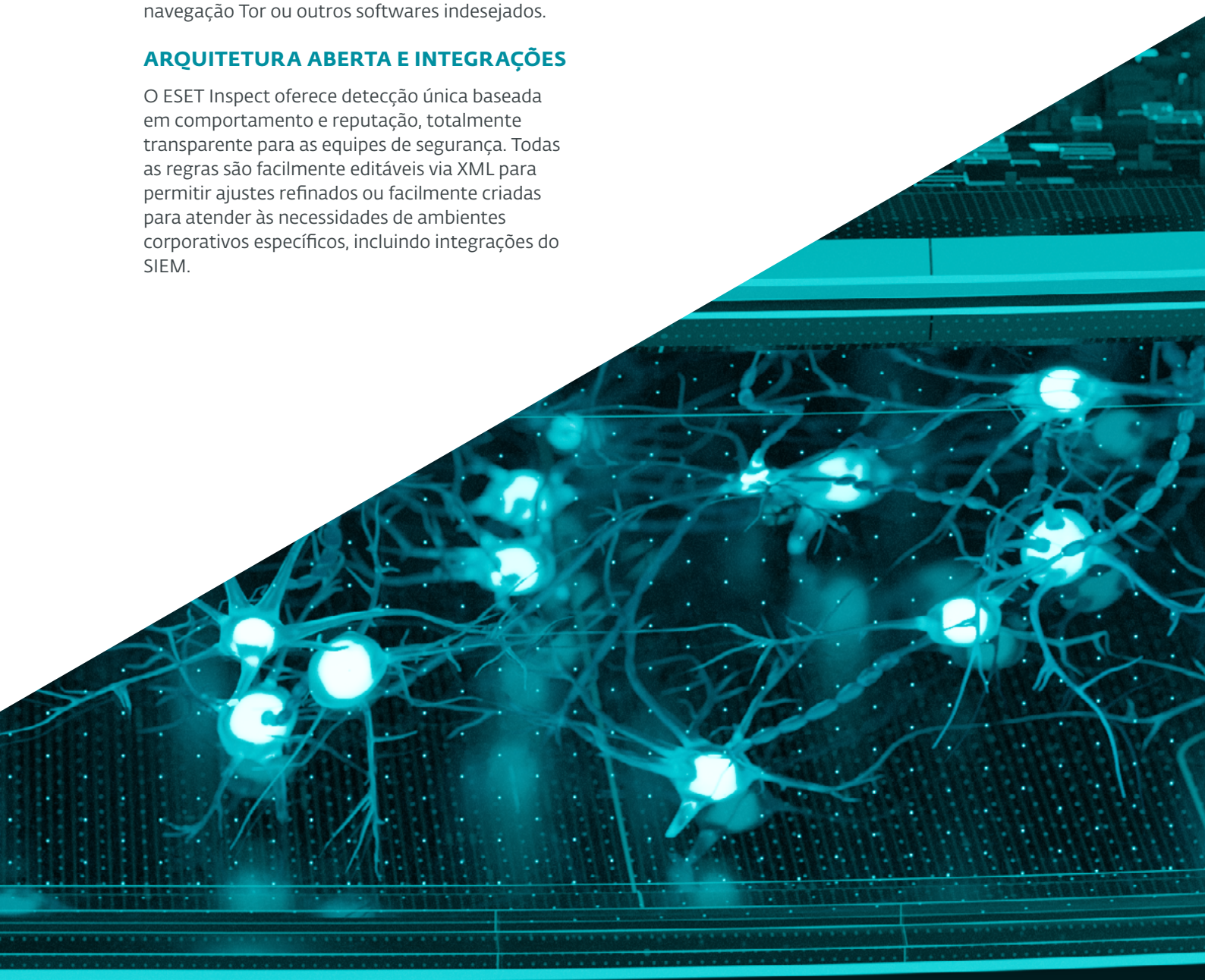
PONTUAÇÃO SOFISTICADA

Priorize a gravidade dos alarmes com uma funcionalidade de pontuação que atribui um valor de gravidade aos incidentes e permite que aos administradores identificarem rapidamente os dispositivos com maior probabilidade de possíveis incidentes.

COLETA DE DADOS LOCAL

Visualize dados abrangentes sobre um módulo recém-executado, incluindo o horário de execução, o usuário que executou, o tempo de permanência e os dispositivos afetados.

Todos os dados são armazenados localmente para evitar vazamento de dados confidenciais.



Casos de uso

Detecção de comportamento e infratores reincidentes

PROBLEMA

Em sua rede, há usuários que são infratores reincidentes em questão de malware. Os mesmos usuários continuam sendo infectados repetidamente. Essa situação ocorre devido a comportamentos arriscados? Ou eles apenas estão sendo alvo com mais frequência do que outros usuários?

SOLUÇÃO

- ✓ Visualize facilmente usuários e dispositivos problemáticos.
- ✓ Conclua rapidamente uma análise de causa raiz para encontrar a origem das infecções.
- ✓ Remedie os vetores de infecção encontrados, como e-mails, web ou dispositivos USB.

Configuração e resposta fáceis — não é necessário uma equipe de segurança

PROBLEMA

Nem todas as empresas têm equipes de segurança dedicadas. Introduzir e implementar regras de detecção avançada pode ser um desafio.

SOLUÇÃO

- ✓ Mais de 300 regras pré-configuradas integradas.
- ✓ Responda facilmente, com apenas um clique, para bloquear, encerrar ou isolar dispositivos.
- ✓ Realize ações de remediação propostas e próximos passos estão integrados aos alertas.
- ✓ As regras podem ser editadas por linguagem XML para permitir ajustes refinados ou a criação de novas regras.

Busca e bloqueio de ameaças

PROBLEMA

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

SOLUÇÃO

- ✓ Utilize o sistema de alerta antecipado para obter dados sobre novas ou futuras ameaças.
- ✓ Procure em todos os computadores a existência da nova ameaça.
- ✓ Procure por indicadores de comprometimento em todos os dispositivos, que indiquem a existência da ameaça antes do alerta.
- ✓ Bloqueie a ameaça para impedir sua infiltração na rede ou execução dentro da organização.

Visibilidade da rede

PROBLEMA

Algumas empresas estão preocupadas com os aplicativos executados pelos usuários em seus sistemas. É necessária uma preocupação não apenas com os aplicativos tradicionalmente instalados, mas também com os aplicativos portáteis que não são, de fato, instalados. Como manter o controle sobre eles?

SOLUÇÃO

- ✓ Visualize e filtre facilmente todos os aplicativos instalados em todos os dispositivos.
- ✓ Visualize e filtre todos os scripts nos dispositivos.
- ✓ Bloqueie facilmente a execução de scripts ou aplicativos não autorizados.
- ✓ Realize a remediação notificando os usuários sobre aplicativos não autorizados e desinstale automaticamente.

Detecção profunda de ameaças — ransomwares

PROBLEMA

Uma empresa deseja ferramentas adicionais para detecção proativa de ransomwares, além de ser notificada prontamente caso seja identificado comportamento semelhante a ransomwares na rede.

SOLUCIÓN

- ✓ Defina regras para detectar aplicativos quando executados a partir de pastas temporárias.
- ✓ Defina regras para detectar arquivos do Office (Word, Excel, PowerPoint) quando executam scripts ou executáveis adicionais.
- ✓ Envie um alerta para caso sejam encontradas alguma das extensões mais comuns de ransomwares em um dispositivo.
- ✓ Visualize alertas do Ransomware Shield das soluções de segurança de endpoints da ESET no mesmo console.

Investigação e remediação conscientes do contexto

PROBLEMA

Os dados são tão bons quanto o contexto. Para tomar decisões adequadas, é necessário saber quais são os alertas, em quais dispositivos eles estão ocorrendo e quais usuários estão os acionando.

SOLUÇÃO

- ✓ Identifique e classifique todos os dispositivos de acordo com o Active Directory, agrupamentos automáticos ou manuais.
- ✓ Permita ou bloqueie aplicativos ou scripts com base no agrupamento de dispositivos.
- ✓ Permita ou bloqueie aplicativos ou scripts com base no usuário.
- ✓ Receba notificações apenas para determinados grupos.

eset® Digital Security
Progress. Protected.

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

MITSUBISHI MOTORS
Drive your Ambition

protegida pela ESET desde 2017 mais de 9 mil endpoints

Allianz Suisse

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

Canon
Canon Marketing Japan Group

protegida pela ESET desde 2016 mais de 32 mil endpoints

Partner de segurança ISP desde 2008 2 milhões de clientes

RECONHECIMENTO

MITRE ATT&CK™

A ESET é um dos fornecedores mais referenciados e envolvidos diretamente no refinamento e preenchimento da base de conhecimento MITRE ATT&CK.

G2 Leader SPRING 2023

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.

The Radicati Group, Inc.
A Technology Market Research Firm

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