CROWDSTRIKE

DETECÇÃO E RESPOSTA DE ENDPOINT (EDR) FALCON

Processando o ciclo de vida da detecção e resposta de ameaças com velocidade, automação e visibilidade incomparável

FALCON INSIGHT - TORNANDO EDR FÁCIL

As ferramentas tradicionais de segurança de endpoints têm pontos cegos, o que as torna incapazes de ver e interromper ameaças avançadas. CrowdStrike® Falcon Insight™ resolve isso, oferecendo visibilidade completa de endpoint para toda a sua organização.

O Insight monitora continuamente todas as atividades dos endpoints e analisa os dados em tempo real para identificar automaticamente as atividades de ameaças, permitindo detectar e impedir ameaças avançadas à medida que ocorrem. Todas as atividades de endpoint também são transmitidas para a plataforma CrowdStrike Falcon®, para que as equipes de segurança possam investigar incidentes rapidamente, responder a alertas e procurar proativamente novas ameaças.

A CROWDSTRIKE É CONSISTENTEMENTE RECONHECIDA COMO UMA SOLUÇÃO PARA PROTEÇÃO DE ENDPOINT LÍDER

A CrowdStrike está posicionada como líder no Quadrante Mágico do Gartner de 2019 para Plataformas de Proteção de Endpoint

A plataforma CrowdStrike é validada conforme o framework MITRE ATT&CK™ para rastrear e detectar ataques avançados nos Testes de Emulação de Estado de Nação do MITRE, 2018

A CrowdStrike é o único fornecedor posicionado como líder tanto no Forrester Wave™: Detecção e Resposta de Endpoint (EDR), Q3 2018, quanto no Forrester Wave: Suíte de Segurança de Endpoint, Q3 2019

A CrowdStrike obteve a melhor pontuação em outubro de 2019 no Recursos Críticos para Plataformas de Proteção de Endpoint do Gartner entre organizações "Tipo A"

PRINCIPAIS BENEFÍCIOS

Detecte e priorize de forma inteligente as ameaças avançadas automaticamente

Acelere as investigações com análises forenses detalhadas em tempo real e visualizações sofisticadas

Responda e corrija com confiança

Obtenha uma visão integral com CrowdScore™, sua pontuação de ameaças corporativas

Reduza a fadiga de alerta em 90% ou mais

Compreenda rapidamente ataques complexos com o framework de detecção baseado em MITRE e o CrowdScore Incident Workbench

DETECÇÃO E RESPOSTA DE ENDPOINT (EDR) FALCON

PRINCIPAIS RECURSOS DO PRODUTO

DETECÇÃO E RESOLUÇÃO SIMPLIFICADAS

- **Detecte automaticamente as atividades do invasor:** O Insight usa IOAs (Indicadores de Ataque) para identificar automaticamente o comportamento do invasor e envia alertas prioritários à interface de usuário da plataforma Falcon, eliminando pesquisas demoradas e buscas manuais. O banco de dados CrowdStrike Threat Graph® armazena dados de eventos e responde a consultas em cinco segundos ou menos, mesmo considerando bilhões de eventos.
- **Desvende ataques inteiros em apenas uma tela:** O CrowdScore Incident Workbench fornece uma visão abrangente de um ataque do início ao fim, com um contexto aprofundado para permitir investigações mais rápidas e fáceis.
- **Acelere o fluxo de trabalho da investigação com o MITRE ATT&CK™:** O mapeamento de alertas conforme o framework MITRE ATT&CK™ (Adversarial Tactics, Techniques and Common Knowledge) permite entender imediatamente até mesmo as detecções mais complexas, reduzindo o tempo necessário para a triagem de alertas e acelerando a priorização e correção. Além disso, a interface de usuário intuitiva permite alternar rapidamente e pesquisar por toda a organização em segundos.
- **Ganhe contexto e inteligência:** A inteligência integrada contra ameaças fornece o contexto completo de um ataque, incluindo a atribuição.
- **Responda de forma decisiva:** Aja contra os adversários em tempo real para interromper os ataques antes que eles se tornem violações. As poderosas ações de resposta permitem que você contenha e investigue sistemas comprometidos, e o recurso de resposta em tempo real do Falcon Insight fornece acesso direto aos endpoints sob investigação. Isso permite que os responsáveis pela segurança executem ações no sistema e erradiquem as ameaças com precisão cirúrgica.

GANHE VISIBILIDADE TOTAL DO ESPECTRO EM TEMPO REAL

- **Veja o panorama em tempo real:** O CrowdScore fornece uma métrica simples que ajuda a organização a entender seu nível de ameaça em tempo real. Isso torna mais fácil para os líderes de segurança entenderem rapidamente se estão sob ataque e avaliarem a gravidade da ameaça, para que possam coordenar a resposta apropriada.
- **Capture detalhes críticos para investigação de ameaças e investigações forenses:** O driver em modo kernel do Falcon Insight captura mais de 400 eventos brutos e as informações relacionadas necessárias para rastrear incidentes.
- **Obtenha respostas em segundos:** O banco de dados CrowdStrike Threat Graph armazena dados de eventos e responde a consultas em cinco segundos ou menos, mesmo considerando bilhões de eventos.
- **Registre até 90 dias:** O Falcon Insight fornece um registro completo das atividades do endpoint ao longo do tempo, quer seu ambiente consista em menos de 100 endpoints ou mais de 500 mil.

VALOR IMEDIATO

- **Economize tempo, esforço e dinheiro:** O Falcon Insight habilitado para nuvem é fornecido pela plataforma CrowdStrike Falcon e não requer nenhuma infraestrutura de gerenciamento local.
- **Implemente em minutos:** Os clientes CrowdStrike podem implementar o agente Falcon entregue por serviços em nuvem para até 70.000 endpoints em menos de um dia.
- **Operacional imediatamente:** Com detecção e visibilidade incomparáveis desde o primeiro dia, o Falcon Insight sai na frente, monitorando e gravando na instalação sem exigir reinicializações, ajustes finos, linhas de base ou configurações complexas.
- **Nenhum impacto no endpoint:** Com apenas um agente leve no endpoint, as pesquisas são realizadas no banco de dados Threat Graph sem nenhum impacto no desempenho dos endpoints ou da rede.

Saiba mais em www.crowdstrike.com.br

SOBRE A CROWDSTRIKE

A CrowdStrike® Inc. (Nasdaq: CRWD), líder global em cibersegurança, está redefinindo a segurança para a era da nuvem com uma plataforma de proteção de endpoint criada do zero para impedir ataques. A arquitetura de um único agente leve da plataforma CrowdStrike Falcon® utiliza inteligência artificial (IA) em escala de nuvem, e oferece visibilidade e proteção instantâneas para toda a empresa, evitando ataques a endpoints dentro ou fora da rede. Alimentada pelo patenteado CrowdStrike Threat Graph™, a plataforma CrowdStrike Falcon correlaciona em tempo real mais de 3 trilhões de eventos relacionados a endpoints de todo o mundo por semana, abastecendo uma das plataformas de dados para segurança mais avançadas do mundo.

AVISO LEGAL:

O Gartner não endossa nenhum fornecedor, produto ou serviço descrito em suas publicações de pesquisa e não aconselha os usuários de tecnologia a selecionar apenas os fornecedores com as classificações mais altas. As publicações de pesquisa do Gartner consistem nas opiniões da organização de pesquisa do Gartner e não devem ser interpretadas como declarações de fato. O Gartner se isenta de todas as garantias, expressas ou implícitas, com relação a esta pesquisa, incluindo quaisquer garantias de comercialização ou adequação a uma finalidade específica.