proofpoint.

RESUMO DA SOLUÇÃO

Proofpoint Active Exploits Protection

Interrompa explorações no primeiro estágio — antes que elas sejam executadas

Principais vantagens

- Ofereça a melhor proteção de primeiro estágio contra explorações identificando e interrompendo atividades de exploração na porta de entrada do e-mail — antes da execução da carga ou do comprometimento do endpoint
- Priorize vulnerabilidades com base em explorações ativas observadas no mundo real
- Reduza a exposição antes que correções sejam aplicadas, enquanto protege contra malware impulsionado por explorações e atividades de comando e controle
- Acelere as investigações com contextos de ameaças atuais e históricos e com inteligência de detecção continuamente atualizada
- Prepare-se para fluxos de trabalho de segurança impulsionados por IA e agentes

Visão geral

A velocidade e a escala da exploração estão aumentando. Novas vulnerabilidades estão sendo divulgadas em volume recorde, enquanto os atacantes as transformam em armas com maior rapidez. Soluções tradicionais de gerenciamento de vulnerabilidades e gerenciamento de exposição frequentemente priorizam sua resposta com base em pontuações de gravidade e risco teórico — mas carecem de visibilidade sobre o que os adversários estão tentando explorar ativamente.

O Proofpoint Active Exploits Protection muda esse modelo.

Ao aproveitar a visibilidade do primeiro estágio na entrega de explorações através do tráfego de rede e de e-mail, a Proofpoint ajuda as organizações a identificar atividades maliciosas antes da execução da carga. A solução combina inteligência sobre explorações do mundo real, priorização com base no perfil do adversário e capacidades de proteção imediata para ajudar as equipes de segurança a se concentrarem no que é mais importante e reduzirem a exposição de forma mais rápida. O resultado é uma abordagem mais proativa para a defesa contra explorações — construída em torno da prevenção de ataques nas fases iniciais da cadeia de ataque.

A solução: inteligência sobre explorações de primeiro estágio mais proteção imediata

O Proofpoint Active Exploits Protection transforma a inteligência sobre explorações do mundo real em proteção decisiva e resposta priorizada. A solução combina inteligência sobre explorações baseada no perfil do adversário, detecção de ameaças baseada em e-mail e rede, e integrações operacionais para ajudar as organizações a identificar e interromper atividades de exploração antes de sua execução.

Com visibilidade sobre explorações no primeiro estágio derivada do e-mail — onde muitos ataques modernos começam — a Proofpoint pode identificar tentativas de entrega de explorações e o comportamento real dos atacantes na fase mais inicial da cadeia de ataque, antes da execução da carga, do comprometimento do endpoint ou da movimentação lateral.

Ao aproveitar essa exclusiva inteligência sobre vulnerabilidades e ampla cobertura contra ameaças impulsionadas por rede e por explorações, o Proofpoint Active Exploits Protection ajuda as organizações a priorizar vulnerabilidades com base em explorações ativas, reduzir a exposição durante janelas de aplicação de correções e acelerar investigações com inteligência sobre ameaças decisiva.

Priorize explorações ativas em vez de risco teórico

Concentre os esforços de remediação nas vulnerabilidades associadas a explorações ativas — e não apenas em altas pontuações CVSS.

O Proofpoint Active Exploits Protection correlaciona a inteligência sobre explorações com o comportamento observado dos atacantes em fontes globais de telemetria para ajudar as organizações a identificar rapidamente quais vulnerabilidades apresentam risco operacional imediato.

Essa abordagem orientada pelos adversários ajuda as equipes de segurança a reduzir o ruído, melhorar a priorização e concentrar recursos nas vulnerabilidades com maior probabilidade de serem exploradas.

As principais capacidades incluem:

- Priorização da correção de ativos com base em CVEs exploradas ativamente
- Distinção entre ameaças urgentes e riscos de menor prioridade
- Priorização de correções orientada com um contexto de ameaça claro e decisivo, incluindo feeds de reputação de IP e de domínio em tempo real
- Melhora do foco operacional ao alinhar a priorização com a atividade dos adversários no mundo real

Obtenha proteção imediata ao aplicar correções

A aplicação de correções leva tempo. O Proofpoint Active Exploits Protection ajuda as organizações a reduzir a exposição durante esse período, oferecendo inteligência sobre explorações continuamente atualizada e permitindo proteção imediata no tráfego de rede e no e-mail.

Ele oferece uma lógica de detecção de alta fidelidade em tempo hábil para ameaças avançadas, inclusive:

- Entrega de malware
- Comunicações de comando e controle
- Kits de exploração
- Phishing de credenciais
- Espalhamento de ataques
- Ransomware e redes de bots
- Anomalias de protocolo e aplicativo
- Mineração de criptomoedas
- Ataques de negação de serviço distribuídos (DDoS)
- Ataques a sistemas de controle e aquisição de dados (SCADA)

As principais capacidades incluem:

- Inteligência sobre explorações continuamente atualizada, projetada para melhorar a proteção nas fases iniciais da cadeia de ataque
- Regras de detecção baseadas em rede para IDS, IPS, NGFW e controles de segurança relacionados
- Assinaturas de alta fidelidade para telefonemas de retorno de malware, droppers, comando e controle, ocultação, ameaças relacionadas a kits de exploração e vazamento
- Atualizações diárias de regras para acompanhar o cenário de ameaças em mudança
- Cobertura das principais famílias de malware, campanhas de ataque e vetores de ameaça baseados em rede
- Suporte para formatos de IDS e IPS amplamente utilizados, inclusive implantações compatíveis com Suricata e Snort

Enriqueça as ferramentas de segurança com inteligência global sobre ameaças

O Proofpoint Active Exploits Protection oferece uma inteligência decisiva que se integra a uma ampla gama de ferramentas de segurança, inclusive firewalls, IDS, IPS, NGFW, UTM, SIEM, sistemas de autenticação, plataformas de caça a ameaças, fluxos de trabalho de resposta a incidentes e ferramentas de segurança personalizadas.

A solução oferece inteligência sobre reputação e ameaças em campanhas, assinaturas, malware, domínios e endereços IP suspeitos e maliciosos, bem como atividades de ataque relacionadas.

As principais capacidades incluem:

- Inteligência sobre ameaças atual e histórica para IPs, domínios, hashes de malware, assinaturas e texto de mensagens
- Feeds de reputação de IP e domínio organizados por categoria de ameaça e pontuação de confiança
- Atualizações frequentes de feeds com envelhecimento agressivo para refletir a atividade atual
- Banco de dados global de ameaças pesquisável para pivoting, detalhamento e investigação
- Múltiplos formatos de feed para integração operacional, inclusive TXT, CSV, JSON, IDS e formatos compactados
- Enriquecimento baseado em API para SIEM, TIP, resposta a incidentes e ferramentas internas

Melhore a fidelidade de detecção e reduza o ruído

O Proofpoint Active Exploits Protection é construído a partir de observações de ameaças do mundo real, análise de malware, feedback de sensores globais e pesquisa dedicada de ameaças. Isso possibilita uma detecção de alta fidelidade, além de ajudar a reduzir falsos positivos nas ferramentas de segurança de rede existentes.

As principais capacidades incluem:

- Conteúdo de detecção orientado por pesquisa com base nas ameaças observadas
- Análise de malware em área restrita (sandbox) que captura o comportamento de rede após a execução
- Feedback de sensores globais para aprimorar a precisão da detecção
- Descrições de assinaturas, referências e documentação para apoiar os fluxos de trabalho dos analistas
- Aplicação de políticas baseada em categorias alinhadas às prioridades organizacionais

Expanda com fluxos de trabalho impulsionados por IA

O Proofpoint Active Exploits Protection é projetado para apoiar operações de segurança modernas e orientadas por inteligência. Capacidades futuras devem oferecer acesso a inteligência sobre ameaças por meio de MCP e fluxos de trabalho baseados em agentes, viabilizando casos de uso impulsionados por API e IA.

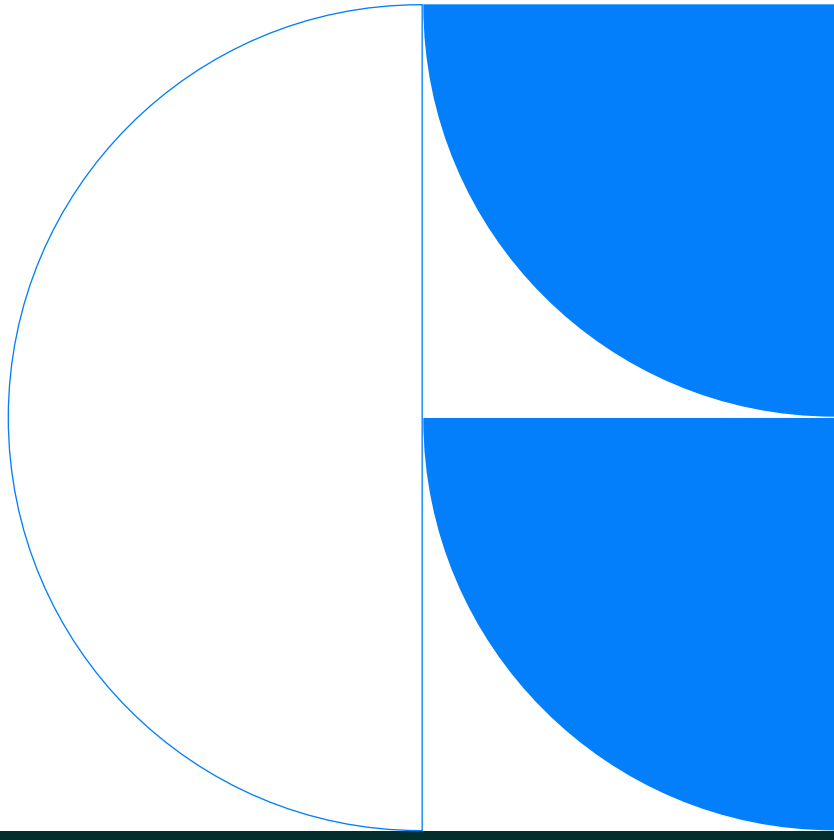
Esses fluxos de trabalho têm como objetivo ajudar as equipes a incorporar inteligência sobre ameaças priorizada diretamente em operações de segurança automatizadas, acelerar decisões e reduzir a triagem manual.

Resumo

O Proofpoint Active Exploits Protection ajuda as organizações a prevenir ataques impulsionados por explorações antes que ocorra um comprometimento, combinando visibilidade sobre explorações de primeiro estágio derivada de e-mails, inteligência sobre explorações orientada por adversários e capacidades de proteção imediata.

Em vez de depender apenas de pontuações de gravidade das vulnerabilidades ou de modelos teóricos de exposição, o Proofpoint Active Exploits Protection permite que as equipes de segurança priorizem com base no que os atacantes estão visando ativamente no mundo real.

Ao unificar priorização, proteção e investigação, o Proofpoint Active Exploits Protection ajuda as equipes de segurança a manter o foco no que realmente importa, proteger imediatamente e investigar com maior rapidez.



proofpoint.