



CrowdStrike *vs* Palo Alto

Segurança de endpoint e os desafios de arquitetura

⊗ Palo Alto

A arquitetura de segurança da Palo Alto Networks costuma ser um ponto de preocupação para muitas empresas devido a três fatores: grande consumo de recursos do sistema por causa do agente Cortex, necessidade de reinicializações após instalações e um processo de atualização automática que frequentemente apresenta falhas. Esses aspectos acabam afetando a eficiência operacional dos endpoints.

✓ CrowdStrike

Em contrapartida, a CrowdStrike tem recebido elogios por sua abordagem inovadora em segurança de endpoints. A plataforma utiliza o Falcon, um agente extremamente leve, e suas atualizações automáticas garantem que a proteção seja contínua e eficiente. Tudo isso sem afetar o desempenho dos sistemas, consolidando sua posição como líder em visão abrangente e execução no mercado segundo o Quadrante Mágico da Gartner para Plataformas de Proteção de Endpoint.

Proteção de Identidade

⊗ Palo Alto

O módulo de Proteção de Identidade da Palo Alto é criticado por suas limitações, funcionando apenas como detecção sem oferecer medidas de bloqueio ou prevenção de ameaças em progresso, o que afeta diretamente o fator segurança. A instalação também é tida como complexa e mais demorada, já que depende de múltiplos componentes para funcionar.

✓ CrowdStrike

A CrowdStrike oferece uma proteção de identidade avançada, com detecção de ataques usando Inteligência Artificial, que já se mostrou 85% mais rápida e eficiente do que a detecção baseada somente em comportamento e política. A plataforma da CrowdStrike também permite uma série de respostas proativas, como a aplicação de MFA e redefinição de senhas, para prevenir ameaças em tempo real. Tudo entregue em um agente unificado, simplificando o gerenciamento e a implementação.

Segurança na Nuvem

⊗ Palo Alto

O Prisma Cloud da Palo Alto é baseado em critérios comportamentais estáticos para identificação e detecção de ameaças, o que pode deixar os clientes expostos a violações por 24 horas após a implementação de novas cargas de trabalho. Além disso, esse critérios precisam ser ajustados manualmente, um processo trabalhoso e sujeito a erros, que pode resultar em muitos falsos positivos e negativos.

✓ CrowdStrike:

A estratégia da CrowdStrike com o Falcon Cloud Security se sobressai devido à sua ampla cobertura e capacidade de segurança. A plataforma oferece um arsenal completo de detecções pré-definidas, proteção baseada em inteligência artificial e uma sofisticada infraestrutura de análise de ameaças. Integrados de forma coesa, esses recursos proporcionam às empresas capacidades avançadas de detecção e uma resposta ágil a incidentes, tudo acessível através de um console unificado.

Gerenciamento de Logs e SIEM

⊗ Palo Alto

A plataforma XSIAM da Palo Alto tem dificuldades para cumprir com os requisitos e casos de uso tradicionais de SIEM, sofrendo com velocidade de busca reduzida, opções restritas para visualização de dados e um processo complicado de integração de dados. Além disso, o processo de integração de dados é muitas vezes visto como oneroso e ineficiente, envolvendo muito mais trabalho manual do que parece.

✓ CrowdStrike

Projetado para atender às exigências de velocidade e escalabilidade de um SOC moderno, o SIEM de última geração da CrowdStrike facilita o bloqueio de violações com alertas em tempo real, fornece buscas rápidas e tem um sistema de inteligência de ameaças abrangente e de alto nível. A solução da CrowdStrike processa petabytes de dados com uma latência menor que um segundo, oferecendo tudo isso a um custo mais acessível em comparação com outras soluções SIEM do mercado.

Serviços Gerenciados (MDR)

⊗ Palo Alto

O MDR da Palo Alto Networks é muitas vezes considerado incompleto, pois se limita a ações de remediação básica e delega responsabilidades significativas ao cliente para a mitigação completa de ataques, a menos que se opte por opções mais caras. Além disso, o MDR da Palo Alto não inclui suporte para manutenção da plataforma/agente e é incapaz de responder a ameaças baseadas em identidade.

✓ CrowdStrike

Por sua vez, a CrowdStrike lidera o mercado de MDR, segundo a Gartner, oferecendo uma gestão completa que abrange de ponta a ponta desde a resposta a incidentes até a manutenção regular de identidade, nuvem e plataforma/agente. Isso elimina a necessidade de intervenção do cliente, fortalece a segurança e maximiza a eficiência na resolução de questões relacionadas a ameaças.

Inteligência de Ameaças

⊗ Palo Alto

A inteligência de ameaças da Palo Alto Networks é frequentemente considerada insuficiente para os analistas de SOC, porque costuma falhar ao fornecer as informações contextuais e os perfis detalhados dos adversários. Embora o recurso Autofocus proporcione algum nível de atribuição de adversários, ele não entrega informações detalhadas ou perfis completos que possam enriquecer as investigações.

✓ CrowdStrike

Referência mundial quando o assunto é inteligência de ameaças, a CrowdStrike oferece uma plataforma integrada de inteligência de ameaças que otimiza o trabalho dos especialistas em segurança. A CrowdStrike disponibiliza uma lista atualizada de Indicadores de Comprometimento (IOCs), atribuição de adversários e uma sandbox para análise de malware. São mais de 230 grupos de ameaças monitorados e a publicação de 200 mil novos IOCs todos os dias.

Proteção de dados

⊗ Palo Alto

A tecnologia de Data Loss Prevention da Palo Alto Networks, que se baseia exclusivamente em rede, costuma ter problemas para identificar e bloquear de forma eficaz a transferência de dados confidenciais e sensíveis de endpoints, especialmente aqueles que não estão conectados a redes corporativas. O resultado disso é uma maior vulnerabilidade na proteção de dados.

✓ CrowdStrike


O CrowdStrike Falcon Data Protection adota uma estratégia moderna para prevenir o roubo de dados. Ao fazer uso do agente unificado da CrowdStrike e de diversos métodos de detecção, a plataforma realiza a identificação e prevenção da transferência de dados de modo confiável. Ela integra análises de conteúdo e contexto em várias camadas, como endpoints, identidades, e dados.



oblock.com.br

AGENDE UM FREE TRIAL

Veja na prática por que a
CrowdStrike é líder de mercado
em proteção de endpoints.

 +55 (11) 2626-3401

 contato@oblock.com.br

 Curitiba, Brasil

