block

CrowdStrike vs Microsoft Defender

Qualidade e capacidade de detecção

Microsoft

A solução da Microsoft tem como foco e adota uma abordagem de antivírus tradicional baseado em assinaturas, demandando atualizações diárias para garantir proteção constante. Além disso, também há confusões sobre o que está incluído nos diferentes pacotes de produtos, o que pode colocar dados e informações em risco.

CrowdStrike

A CrowdStrike é cloud-based, oferecendo atualizações contínuas e automáticas, sem necessidade de reiniciar sistemas. Além disso, utiliza inteligência artificial (IA) avançada para identificar ameaças, focando em comportamentos atípicos e suspeitos, conhecidos como indicadores comportamentais de ataque (IOA). Esta técnica é eficaz, principalmente, na identificação de malwares desconhecidos e ameaças de dia zero ou zero day, oferecendo uma camada robusta de segurança contra ameaças sofisticadas e complexas.

Implantação e instalação

Microsoft

O Microsoft Defender for Endpoint faz parte do sistema operacional Windows. Por isso, costuma apresentar alguns desafios relacionados às diferentes edições e versões do Windows. Para funcionar com eficiência, é essencial que o sistema operacional esteja sempre atualizado, o que pode ser uma barreira.

CrowdStrike

A implantação da CrowdStrike se destaca pela simplicidade. Seu agente leve pode ser rapidamente aplicado a diversos endpoints. Isso vale para qualquer sistema operacional, seja Windows, macOS ou Linux. Não há necessidade de configurações complexas. Na prática, milhares de endpoints podem ser protegidos em apenas minutos.

Manutenção

Microsoft

A manutenção do Microsoft Defender, integrada à gestão do Windows, requer reinicializações e atualizações contínuas. Essa necessidade pode causar interrupções nos negócios, afetando a produtividade da organização. Além disso, o gerenciamento dessas atualizações frequentes pode aumentar a complexidade operacional e os custos para a empresa.

CrowdStrike

O agente da CrowdStrike é atualizado automaticamente, assegurando proteção contínua sem a necessidade de reinicializar os dispositivos. Essa eficiência reduz o tempo de inatividade e simplifica a manutenção. Com essa abordagem, o time de TI da organização pode se concentrar mais na prevenção de violações e menos na gestão de atualizações, aumentando a eficácia da segurança cibernética.

Facilidade de uso (usabilidade)

Microsoft

A complexidade do Defender costuma gerar confusão, já que as configurações de segurança e os relatórios estão distribuídos por diversos lugares. Esta separação dificulta a visão unificada das ameaças e das medidas de segurança aplicadas, aumentando a complexidade operacional. Além disso, essa dispersão de recursos pode atrasar a detecção de ameaças e a resposta a incidentes, o que é crucial em um ambiente de segurança dinâmico.

CrowdStrike

A solução da CrowdStrike proporciona uma experiência de usuário simples e integrada por meio de um console unificado. Esta abordagem centralizada torna o gerenciamento de endpoints, nuvem e identidades mais ágil e eficiente. A plataforma não só oferece uma visão completa dos ataques, mas também fornece contexto de ameaças em tempo real, acelerando a investigação e a resposta. Além disso, conta com automações de fluxo de trabalho personalizáveis e uma vasta gama de integrações com parceiros, enriquecendo ainda mais a operação de segurança.

Custos e investimentos

Microsoft

A solução Microsoft Defender pode envolver custos imprevisíveis devido a sua complexidade de licenciamento e operações. Além disso, há a questão das interrupções contínuas nos negócios e a necessidade de pessoal adicional para gerenciar as atualizações.

CrowdStrike

O modelo de custo da CrowdStrike é previsível, com licenciamento transparente e gerenciamento de segurança simplificado para reduzir interrupções e minimizar despesas com treinamento e mão de obra.

Suporte

Microsoft

Na abordagem da Microsoft para segurança de endpoint, existe uma dependência das versões do sistema operacional e seus respectivos ciclos de suporte. O ponto-chave é que este ciclo de vida de suporte varia, com muitas versões sendo suportadas por apenas 18 meses.

CrowdStrike

Com a CrowdStrike, não faz diferença a versão ou o sistema operacional utilizado. O suporte é oferecido mesmo para versões descontinuadas do Windows, garantindo proteção consistente e abrangente.

MDR (serviço gerenciado)

Microsoft

O ‘Defender Experts’, serviço gerenciado de resposta e detecção estendida, fundamenta-se principalmente em inteligência artificial treinada, ao invés de utilizar equipes reais. Além disso, o ‘Defender Experts for Hunting’, serviço específico de caça a ameaças, requer pagamento adicional e não se concentra primariamente em estratégias proativas de busca e caça a ameaças.

CrowdStrike

Nas avaliações MITRE ATT&CK® para provedores de serviços, o MDR da CrowdStrike alcançou o topo em termos de cobertura de detecção. Com o Falcon Complete MDR, a segurança é garantida ininterruptamente, todos os dias da semana, incluindo análises forenses detalhadas e uma abordagem precisa na resolução de incidentes e combate a ameaças.

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