SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

Detecção e Resposta Inteligentes de Endpoints

O Sophos Intercept X Advanced with EDR integra a detecção e resposta inteligentes de endpoints (EDR) com a melhor detecção de malwares do mercado, a proteção contra exploração de vulnerabilidades da mais alta qualidade e outros recursos inigualáveis de proteção de endpoints.

Destaques

- EDR combinado com a melhor proteção de endpoints
- Análise de malware com Deep Learning
- Inteligência sob demanda de ameaças selecionadas do SophosLabs
- Detecção por machine learning e priorização de eventos suspeitos*
- Investigações guiadas tornam o EDR acessível, sem abrir mão da eficácia
- Reaja a incidentes com um único clique

A EDR começa com a melhor proteção

Para deter as violações antes que comecem, a prevenção é crucial. O Intercept X reúne uma proteção exclusiva e a detecção e resposta de endpoints em uma única solução. Isso significa que a maioria das ameaças é detida antes que possam causar danos, e o Intercept X Advanced with EDR oferece uma garantia adicional de segurança cibernética com a capacidade de detectar, investigar e reagir a possíveis ameaças de segurança.

A inclusão do EDR em um pacote de proteção de endpoints, considerado consistentemente de alto nível, permite que o Intercept X alivie significativamente a carga de trabalho do EDR. Quanto mais ameaças forem evitadas, menor é a necessidade de investigação pelas equipes de segurança. Isso significa que as equipes podem otimizar os principais recursos, o que permite que se concentrem nos assuntos relacionados ao departamento de TI, ao invés de precisarem investigar os falsos positivos e um grande volume de alertas.

Aumente os conhecimentos, não o número de pessoal

O Intercept X Advanced with EDR replica as tarefas normalmente realizadas por analistas qualificados, para que as organizações possam agregar conhecimentos sem ter que aumentar o número de funcionários. Ao contrário de outras soluções de EDR que contam com analistas humanos altamente qualificados para fazer perguntas e interpretar dados, o Intercept X Advanced with EDR é alimentado por Machine Learning e aprimorado com a inteligência de ameaças selecionadas do SophosLabs.

Especialista em segurança*: O Intercept X Advanced with EDR coloca a especialização em segurança nas mãos do departamento de TI, ao detectar e priorizar ameaças potenciais de forma automática. Com o uso do Machine Learning, os eventos suspeitos são identificados e priorizados como sendo de máxima importância e que necessitam de atenção imediata. Os analistas podem descobrir rapidamente onde concentrar sua atenção e entender quais máquinas podem ser afetadas.

Especialistas em malware: A maioria das organizações conta com especialistas em malware especializados em engenharia reversa para realizar a análise de arquivos suspeitos. Essa abordagem não apenas é demorada e difícil de ser realizada, como também pressupõe um nível de sofisticação de segurança cibernética que a maioria das organizações não possui. O Intercept X Advanced with EDR oferece uma melhor abordagem, ao aproveitar a Análise de Malware com Deep Learning, a qual analisa automaticamente o malware de forma extremamente detalhada ao dividir atributos de arquivo e código e compará-los com milhões de outros arquivos. Os analistas podem facilmente ver quais atributos e segmentos de código são semelhantes aos arquivos "sabidamente bons" e "sabidamente ruins", para que possam determinar se um arquivo deve ser bloqueado ou permitido.

Especialistas em inteligência de ameaças: Quando o Intercept X Advanced with EDR traz à tona um arquivo potencialmente suspeito, os administradores do departamento de TI podem coletar mais informações ao acessar a inteligência sob demanda de ameaças selecionadas pelo SophosLabs, o qual recebe e processa aproximadamente 400.000 amostras de malwares previamente não identificados todos os dias. Essas e outras informações sobre ameaças são coletadas, agregadas e resumidas para facilitar a análise. Isso significa que as equipes que não possuem analistas dedicados à inteligência de ameaças ou acesso aos feeds de ameaças, que são caros e difíceis de compreender, podem se beneficiar de uma das melhores equipes de pesquisa e ciência do mundo em dados sobre segurança cibernética.

Resposta Guiada a Incidentes

O Intercept X Advanced with EDR permite que os administradores respondam a perguntas difíceis sobre incidentes de segurança, ao fornecer visibilidade da abrangência de um ataque, como ele começou, o que foi afetado e de que forma reagir a ele. Equipes de segurança de todos os níveis de habilidade podem entender rapidamente sua postura de segurança graças às investigações guiadas, as quais oferecem sugestões dos próximos passos, representações visuais claras dos ataques e conhecimentos integrados.

Ao concluir uma investigação, os analistas podem responder com apenas um clique. Dentre as opções de resposta rápida estão a capacidade de isolar os endpoints para correção imediata, realizar a limpeza e o bloqueio de arquivos e criar instantâneos forenses.

Casos de utilização da EDR Inteligente

Com a detecção e resposta inteligentes de endpoints, as equipes de segurança têm a visibilidade e o conhecimento de que necessitam para responder às difíceis perguntas feitas como parte de um esforço de resposta a incidentes.

Responda às perguntas difíceis sobre um um incidente:

- Entenda a abrangência e o impacto dos incidentes de segurança
- Detecte ataques que podem ter passado despercebidos
- Busque por indicadores de comprometimento em toda a rede
- Priorize eventos para investigações adicionais
- Analise arquivos para determinar se são uma ameaça ou potencialmente indesejados
- Comunique com confiança a postura de segurança de sua organização a qualquer momento

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Técnicas básicas	✓	✓		✓
Deep learning	✓	✓	✓	
Proteção contra exploração de vulnerabilidades	✓	✓	✓	
Proteção contra ransomware CryptoGuard	✓	✓	✓	
Detecção e resposta de endpoints (EDR)	✓			

Experimente agora gratuitamente

Registre-se para uma avaliação gratuita de 30 dias em sophos.com/intercept-x.

* Disponível no início de 2019

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas na Brasil
E-mail: Brasil@sophos.com

18-10-02 DS-PTBR (3098-DD)

SOPHOS