Server Workload Protection

Linux Protection

Intercept X Advanced for Server, Intercept X Advanced for Server with XDR e Intercept X Advanced for Server with MTR

Nuvem ou datacenter, host e contêiner. Proteja sua infraestrutura agora e acompanhe a evolução com a Sophos: proteção de carga de trabalho de alto impacto que resulta em baixo impacto no desempenho.

Minimize o tempo de detecção e resposta

Obtenha visibilidade completa de seus hosts e cargas de trabalho em contêineres, identificando comportamentos anômalos e protegendo-se antes que malwares e exploits se coloquem em posição de ataque. Detecção e resposta estendidas (XDR) oferecem insight detalhado de hosts, contêineres, endpoints, tráfego de rede e serviços de segurança nativos do provedor da nuvem.

Detecções comportamentais nativas na nuvem e em tempo de execução de exploits identificam ameaças, incluindo de escapes de contêiner, exploits de kernel e tentativas de escalonamento de privilégios. Fluxos de trabalho de investigação de ameaças agilizados priorizam as detecções de incidentes de alto risco e consolidam eventos conectados para aumentar a eficiência e economizar tempo.

Melhore as operações de segurança

Combata ameaças com detecções acionáveis de ameaças e visibilidade de host e contêiner em tempo de execução através do nosso painel de gerenciamento central ou integrado às suas ferramentas existentes de resposta a ameaças com opções de implantação a escolher.

Gerenciamento do Sophos Central – Este agente leve Linux dá às equipes de segurança as informações críticas de que precisam para investigar e responder a ameaças comportamentais, exploits e malwares em um mesmo lugar. Monitorando o host do Linux, essa opção de implantação permite que as equipes gerenciem todas as soluções da Sophos a partir de um único painel, sem rupturas na atividade ao mudar entre busca, correção e gerenciamento de uma ameaça.

Integração da API – O Sophos Linux Sensor é uma opção de implantação altamente flexível que é ajustada para oferecer o melhor desempenho. O sensor Linux usa APIs para integrar detecções avançadas de ameaças em tempo de execução, em ambientes de host ou em contêiner, às suas ferramentas existentes de resposta a ameaças. Oferece uma ampla gama de detecções, controle para criar conjuntos de regras personalizadas e opções de configuração para sintonizar a utilização dos recursos do host.

Desempenho sem atrito

A proteção do Intercept X for Server é otimizada para fluxos de trabalho DevSecOps, identificando ataques sofisticados em tempo real, o que ocorre sem a necessidade de um módulo kernel, orquestrações, linhas de base ou varreduras de sistema. A limitação otimizada de recursos, incluindo limites de CPU, memória e coleta de dados, ajuda a evitar desperdícios e períodos de inatividade dispendiosos devidos a questões de instabilidade e hosts sobrecarregados. A sua garantia de otimização do desempenho do aplicativo e tempo de atividade.

Destaques

- Protege cargas de trabalho e contêineres Linux na nuvem, no local e virtuais
- Minimiza o tempo de detecção e resposta a ameaças
- Otimizado para cargas de trabalho de missão crítica quando o desempenho é crucial
- Aproveite os dados de endpoint, rede, e-mail, nuvem, M365 e móveis com a detecção e resposta estendidas (XDR)
- Entenda e proteja todo o seu ambiente de nuvem com o gerenciamento de postura de segurança da nuvem incluído
- Proporciona segurança 24 horas durante o ano todo como um serviço totalmente gerenciado

SOPHOS

Automatize sua lista de tópicos de segurança na nuvem

Projete o seu ambiente de nuvem para atender aos padrões das melhores práticas com a visibilidade e as ferramentas para mantê-las com o gerenciamento de postura de segurança da nuvem, cobrindo todo o seu ambiente de nuvem pública, de ponta a ponta:

- Identifique de modo proativo atividades não autorizadas, vulnerabilidades de imagem de contêiner e host, e configurações incorretas em ambientes como Amazon AWS, Microsoft Azure e Google Cloud Platform (GCP)
- Mantenha a continuidade da descoberta de recursos na nuvem com inventário detalhado e visibilidade da proteção do host da Sophos e das implantações do Sophos Firewall
- Sobreponha automaticamente os padrões das melhores práticas de segurança para detectar lacunas na postura e identificar problemas de solução rápida e outros mais sérios
- Detecte anomalias de alto risco no comportamento da função de IAM do usuário que indicam locais e padrões de acesso incomuns e comportamentos maliciosos rapidamente para evitar violações

A parceria que aumenta a sua equipe

Os analistas especializados do SOC do Sophos Managed Threat Response trabalham em parceria com a sua equipe, monitorando o seu ambiente 24 horas por dia e saindo no encalço de ameaças para remediá-las por você com a expertise em Linux necessária para aumentar sua eficiência. Os analistas da Sophos respondem a ameaças potenciais, buscam indicadores de comprometimento e oferecem análise detalhada sobre eventos, incluindo o que ocorreu e onde, quando, como e por que ocorreu.

Especificações técnicas

Para obter as mais recentes informações, consulte os requisitos do sistema Linux. Para obter detalhes sobre a funcionalidade do Windows, consulte a folha de dados do Windows.

Pontos de destaque	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Agente de proteção Linux (Incluindo varredura de malware, prevenção de exploit, varredura de arquivo e mais)	✓	✓	✓
Linux Sensor (Integre detecções de ameaças em tempo de execução em contêiner e Linux com suas ferramentas existentes de resposta a ameaças via API)		✓	✓
Segurança de infraestrutura da nuvem (Monitore a postura de segurança da nuvem para prevenir riscos de conformidade e segurança)	✓	✓	✓
XDR (Detecção e resposta estendida)		✓	✓
MTR (Managed Threat Response – serviço 24/7/365 de caça a ameaças e resposta)			✓

Experimente agora gratuitamente

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

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

Vendas no Brasil
E-mail: brasil@sophos.com

22-05-24 DS-EN (MP)