Sophos XDR

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

O Intercept X é a única solução XDR da indústria que sincroniza a segurança nativa de endpoint, servidor, firewall, e-mail, nuvem e O365. Veja um quadro holístico do ambiente da sua organização com um rico conjunto de dados e uma análise profunda para detecção, investigação e resposta a equipes de SOC dedicadas e administradores de TI.

Responda a operações de TI e questões de caça a ameaças

Obtenha resposta a questões críticas de negócios com rapidez. Administradores de TI e profissionais de segurança cibernética verão o real valor que ele adiciona quando desempenharem tarefas diárias de operações de TI e caça a ameaças.

Comece com a melhor proteção

O Intercept X interrompe violações antes mesmo que comecem. Com isso você tem a melhor proteção e gasta menos tempo investigando incidentes que deveriam ter sido interrompidos automaticamente. Você também terá acesso a inteligência de ameaças detalhada, para ter as informações necessárias para agir de modo rápido e bem-fundamentado.

Saiba no que se concentrar

Concentre-se nas questões mais importantes com uma lista priorizada de detecções suspeitas e configurações vulneráveis que incluem informações-chave para investigações avançadas. Escolha em uma biblioteca de modelos pré-formulados para fazer uma grande variedade de perguntas sobre operações de TI e caça a ameaças, ou crie suas próprias indagações.

Minimize o tempo de investigação e resposta

Investigações guiadas por IA permitem que você compreenda com rapidez o escopo e a causa de um incidente e minimize o tempo de resposta. Acesse dispositivos para conhecer seu estado em tempo real e seu histórico acumulado de até 90 dias de dados ou de 30 dias no Data Lake.

Visibilidade entre produtos

Obtenha o máximo de visibilidade da sua organização com a integração nativa de dados do Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix e Microsoft Office 365.

Suporte multiplataforma para diferentes sistemas operacionais

Inspecione o seu ambiente tanto no local como na nuvem ou em suas implantações virtuais do Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform e Oracle Cloud Infrastructure.

Destaques

- Responda a operações de TI críticas aos negócios e questões de caça a ameaças
- Utilize uma lista priorizada de detecções e investigações guiadas por IA
- Adote medidas corretivas remotamente em dispositivos de interesse
- Obtenha uma visão holística do ambiente de TI da sua organização e faça o detalhamento granular quando precisar
- Integrações nativas de endpoint, servidor, firewall, e-mail, nuvem, dispositivos móveis e O365
- Acesso à biblioteca de casos de uso de modelos pré-formulados e personalizáveis

SOPHOS

Casos de uso

Operações de TI

- Por que minha máquina está lenta?
- Quais dispositivos apresentam vulnerabilidades conhecidas, serviços desconhecidos ou extensões de navegadores não autorizadas?
- Há programas em execução que deveriam ser removidos?
- Identifique dispositivos não gerenciados, convidados e IoT
- Por que a conexão da rede do escritório está lenta? Qual aplicativo está causando o problema?
- Retroceda 30 dias e verifique atividades incomuns em um dispositivo que foi perdido ou destruído
- Localize dispositivos móveis que estão sem patches ou que apresentam softwares desatualizados

Caça a ameaças

- Quais processos estão tentando estabelecer uma conexão em rede nas portas não regulares?
- Exiba processos que tiveram arquivos ou chaves de registro recém-modificados
- Liste IoCs mapeados na estrutura MITRE ATT&CK
- Estenda as investigações para 30 dias sem precisar colocar o dispositivo online
- Use detecções ATP e IPS do firewall para investigar hosts suspeitos
- Compare informações de cabeçalho de e-mail, SHAs e outros IoCs para identificar o tráfego a um domínio mal-intencionado
- Identifique usuários com várias tentativas de autenticação malsucedidas

O que está incluído?

	Extended Detection and Response (XDR)
Fontes de dados entre produtos	✓
Detecção, investigação e resposta entre produtos	✓
Lista priorizada de detecções e investigações guiadas por IA	✓
Sophos Data Lake	✓
Período de retenção do Data Lake	30 dias
Informações em tempo real	✓
Período de retenção de dados em disco	Até 90 dias
Biblioteca de modelos de caça a ameaças e operações de TI	✓
Funcionalidades de proteção do Intercept X	✓

Para obter mais detalhes sobre licenciamento, consulte os guias de licença do Intercept X e do Intercept X for Server.

Experimente agora gratuitamente

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

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

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

22-01-06 DS-PTBR (MP)

SOPHOS