

Sophos Extended Detection and Response



XDR

Defenda-se de adversários ativos com a amplitude do EDR e XDR.

O bloqueio rápido dos ataques é essencial. O Sophos XDR oferece ferramentas poderosas e inteligência de ameaças que capacitam você a detectar, investigar e responder a atividades suspeitas em todo o seu ambiente de segurança de TI.

Desenvolvido com a mais robusta proteção como base

As equipes de TI, já extenuadas, têm menos incidentes para investigar e resolver quando mais ameaças são bloqueadas na triagem inicial. A Sophos combina detecção e resposta estendida com a proteção de endpoint mais robusta do setor, bloqueando ameaças antes que exijam investigação manual – aliviando a sua carga de trabalho.

Endpoint Detection and Response integrado (EDR)

O Sophos XDR inclui ferramentas de EDR abrangentes, funcionalidades poderosas de pesquisa personalizáveis com acesso a 90 dias de dados de endpoint e servidor, e acesso remoto seguro a dispositivos. Investigue problemas, instale e desinstale softwares, encerre processos e mais.

Visibilidade que se estende além dos seus endpoints

Quanto mais você vê, mais rápido pode agir. Eventos registrados por produtos Sophos e também de outros fornecedores são inseridos, filtrados, relacionados e priorizados, estendendo a sua visibilidade a todas as superfícies de ataque mais importantes, permitindo que você detecte e bloqueie os adversários ativos com mais rapidez.

Soluções prontas para Expansive Sophos XDR

As tecnologias da Sophos trabalham juntas na plataforma XDR para oferecer os melhores resultados de segurança possíveis. As integrações de soluções nativas incluem o Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email e Sophos Cloud.

Compatível com suas ferramentas e tecnologias existentes

Trabalhe com dados de telemetria capturados por diferentes ferramentas de terceiros, aumente o retorno do seu investimento prévio em tecnologias e acelere o processamento das suas operações de segurança. As integrações incluem tecnologias de segurança de endpoint, identidade, rede, firewall, e-mail, nuvem e produtividade.

Destaques

- Visibilidade de atividades suspeitas nas principais superfícies de ataque
- Uma plataforma XDR unificada com uma ampla oferta de soluções integradas da Sophos
- Continue a usufruir de suas ferramentas e investimentos existentes com a integração da Sophos para tecnologias de terceiros
- Investigue e responda a ameaças rapidamente com detecções priorizadas por IA e fluxos de trabalho otimizados
- Inclui EDR e a proteção de endpoint que é líder do setor

Acelere a detecção, investigação e resposta

O Sophos XDR inclui ferramentas e funcionalidades projetadas para maximizar a eficiência dos analistas de segurança e administradores de TI. Investigações guiadas por IA permitem que você compreenda com rapidez o escopo e a causa de um incidente e minimize o tempo de resposta.



Detecções priorizadas por IA nas principais superfícies de ataque

Identifique facilmente atividades suspeitas que exigem atenção imediata. O Sophos XDR prioriza as detecções automaticamente com base no risco, fornecendo todo o seu contexto.



Mapeamento da estrutura MITRE ATT&CK

Detecções e casos são automaticamente mapeados para as táticas MITRE ATT&CK, para você poder identificar facilmente as possíveis lacunas nas defesas e priorizar as melhorias.



Investigue e saia no encalço de ameaças a toda velocidade

Ferramentas de pesquisa poderosas, incluindo modelos pré-formulados de consulta, permitem que você encontre os dados de que necessita com rapidez, sem precisar ser um perito em SQL.



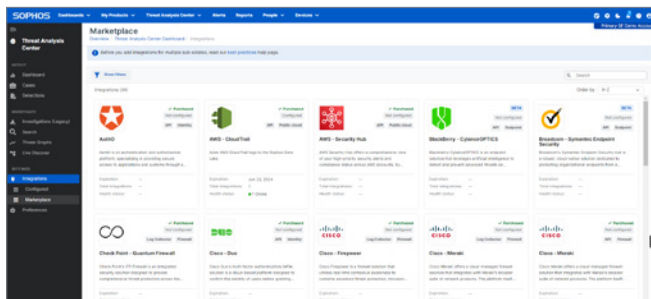
Respostas automatizadas e aceleradas

Ações automatizadas, como encerramento de processo, reversão de ransomware e isolamento de rede, detêm as ameaças rapidamente e economizam um tempo valioso.

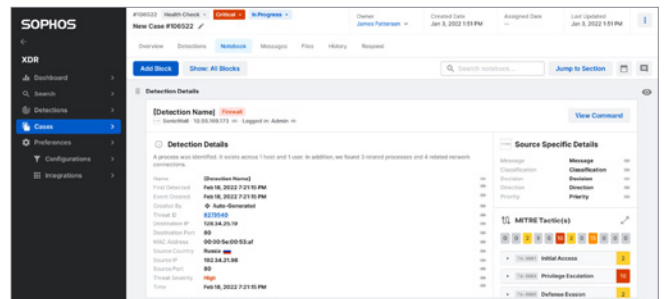


Gerenciamento de caso colaborativo

A criação automática de casos permite fazer uma investigação rápida, com ferramentas de gerenciamento e colaboração que englobam toda a equipe



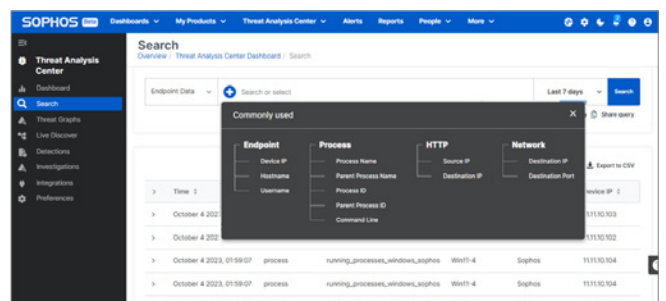
Compatível com soluções da Sophos e de terceiros



Ferramentas poderosas de colaboração e gerenciamento de casos



Detecções priorizadas por IA nas principais superfícies de ataque



Pesquisa simples e poderosa – não precisa ser perito em SQL

Integrações incluídas no Sophos XDR

Dados de segurança das seguintes fontes podem ser integrados com a plataforma Sophos XDR sem custos adicionais. As fontes de telemetria são usadas para expandir a visibilidade em todo o seu ambiente, gerar deteções de novas ameaças e melhorar a fidelidade das deteções de ameaças existentes, conduzir a caça a ameaças e oferecer recursos adicionais de resposta.

Sophos Endpoint

Bloqueie ameaças avançadas e detecte comportamentos mal-intencionados em todos os seus endpoints

Produto incluído no preço do Sophos XDR

Workload Protection

Proteção avançada e deteção de ameaça para contêineres e servidores Linux e Windows

Produto incluído no preço do Sophos XDR

Sophos Mobile

Mantenha seus dispositivos iOS e Android e dados protegidos contra as mais recentes ameaças a dispositivos móveis

Produto vendido separadamente; integração sem custo adicional

Sophos Firewall

Monitore e filtre o tráfego de entrada e saída da rede para bloquear ameaças avançadas antes que possam causar danos

Produto vendido separadamente; integração sem custo adicional

Sophos Email

Proteja a sua caixa de entrada contra malwares com a IA avançada que impede a clonagem direcionada e os ataques de phishing

Produto vendido separadamente; integração sem custo adicional

Sophos Cloud

Interrompa as violações da nuvem e obtenha visibilidade entre todos os seus serviços de nuvem críticos, incluindo AWS, Azure e GCP

Produto vendido separadamente; integração sem custo adicional

Sophos ZTNA

Substitua a VPN de acesso remoto pelo acesso de privilégio mínimo para a conexão segura dos usuários aos seus aplicativos na rede

Produto vendido separadamente; integração sem custo adicional

Endpoint Protection para terceiros

Compatível com:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry [Cylance]
- Broadcom [Symantec]

+ compatível com outras soluções com o agente Sophos "XDR Sensor"

Ferramentas de segurança Microsoft

- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

90 dias de retenção de dados

Retém dados dos produtos Sophos e de terceiros (diferentes fornecedores) no Sophos Data Lake

Prorrogável até 1 ano como complemento opcional

Logs de auditoria da Microsoft

Oferece informações sobre usuário, administração, sistema e ações e eventos da política inserida pelo Office 365 Management Activity API

Google Workspace

Insera telemetria de segurança do Google Workspace Alert Center API

Integrações complementares


Dados de segurança das seguintes fontes podem ser integrados com a plataforma Sophos XDR com a compra dos pacotes de integração. As fontes de telemetria são usadas para expandir a visibilidade em todo o seu ambiente, gerar detecções de novas ameaças e melhorar a fidelidade das detecções de ameaças existentes, conduzir a caça a ameaças e oferecer recursos adicionais de resposta.



NDR Sophos NDR

Monitore continuamente a atividade dentro da sua rede para detectar ações suspeitas ocorrendo entre dispositivos que poderiam passar sem ser percebidas


Compatível com qualquer rede via espelhamento de porta SPAN



Firewall

Compatível com:


- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard



Rede

Compatível com:

- Darktrace
- Secutec
- Thinkst Canary
- Skyhigh Security




Identity

Compatível com:

- Auth0
- Duo
- ManageEngine
- Okta

Integração da Microsoft incluída sem custos adicionais



Email

Compatível com:

- Proofpoint
- Mimecast

Integrações do Microsoft 365 e Google Workspace incluídas sem custos adicionais




Nuvem pública

Compatível com:

- AWS Security Hub
- AWS CloudTrail
- Orca Security


Integre dados adicionais da AWS, Azure e GCP via produtos Sophos Cloud, vendido separadamente



Backup e recuperação

Compatível com:

- Veeam



1 ano de retenção de dados

Retém dados dos produtos Sophos e de terceiros (diferentes fornecedores) no Sophos Data Lake

Desenvolvido com a melhor proteção de endpoint do mundo como base

Foque suas investigações na interrupção de mais violações antes que ocorram. A maioria dos produtos XDR força os analistas a desperdiçarem um tempo valioso investigando incidentes que suas proteções já deveriam ter bloqueado. A Sophos combina XDR com a proteção de endpoint mais robusta do setor, bloqueando ameaças antes que exijam investigação manual – aliviando a sua carga de trabalho.

As assinaturas do Sophos XDR incluem o Sophos Intercept X Endpoint, oferecendo anti-ransomware e anti-exploit avançados, proteção contra malware alimentada por IA e defesas sensíveis ao contexto que se adaptam dinamicamente aos níveis de proteção.

Saiba mais em sophos.com/endpoint

Detecção e resposta como um serviço totalmente gerenciado

Opte por detectar e investigar ameaças com o Sophos XDR ou libere o seu pessoal com o nosso serviço gerenciado 24 horas por dia, sete dias por semana. Com o Sophos Managed Detection and Response (MDR), nossas equipes de caçadores e analistas de ameaças especializados pode oferecer um centro de operações de segurança instantâneo, incluindo a capacidade total de resposta a incidentes.

Saiba mais em sophos.com/mdr

Incluído nas assinaturas do Sophos XDR

	Sophos XDR
Detecções priorizadas por IA e investigações guiadas	✓
Gerenciamento de casos, colaboração e ações de resposta	✓
Ferramentas de pesquisa simples e poderosas para busca e investigação	✓
Soluções Sophos Endpoint e Workload Protection (Intercept X Advanced)	✓
Ferramentas Endpoint Detection and Response (EDR)	✓
Retenção de dados na nuvem	90 dias (prorrogável até 1 ano)
Riqueza de dados de servidores e endpoints no dispositivo EDR	✓
Integrações com soluções da Sophos: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud	✓
Sophos Network Detection and Response (NDR)	Complemento adicional
Integrações com soluções de Endpoint Protection de outros fornecedores	✓
Integrações com soluções da Microsoft	✓
Integração com a solução de produtividade do Google Workspace	✓
Integrações com soluções de firewall, rede, e-mail, nuvem, identidade e backup e recuperação de outros fornecedores	Complementos adicionais

Veja por que os clientes escolhem o Sophos XDR

A Sophos é líder consagrada em detecção e resposta estendida com premiações reconhecidas pelo setor.

Gartner

Líder no 2023 Gartner® Magic Quadrant™ em Plataformas de Proteção de Endpoints em 14 relatórios consecutivos



A Sophos é o único fornecedor reconhecido com o selo Customers' Choice em EPP, MDR, Firewalls e Mobile Threat Defense

G2 Leader

G2 reconhece a Sophos Líder em Endpoint Protection, EDR, XDR, Firewall e MDR em seus relatórios Winter 2024



A Sophos despontou na mais alta posição de liderança sozinha no relatório Omdia Universe for Comprehensive XDR em 2023



A Sophos atingiu resultados excepcionais nas avaliações de 2023 da MITRE Engenuity ATT&CK



A Sophos atinge resultados consistentes em testes independentes em proteção que lideram o setor

Experimente agora gratuitamente

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

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

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