Sophos Extended Detection and Response

Defend against active adversaries with comprehensive EDR and XDR

Stopping attacks quickly is critical. Sophos XDR 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 built-in (EDR)

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

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.

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.

Compatible with your existing tools and technologies

Leverage telemetry from a wide range of non-Sophos security tools and get more ROI from your existing technology investments while speeding up security operations. Integrations include identity, network, firewall, email, cloud, productivity, and endpoint security technologies.

Highlights

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

Accelerate detection, investigation and response

Sophos XDR includes tools and capabilities designed to maximize the efficiency of security analysts and IT admins. AI-guided investigations enable you to 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.
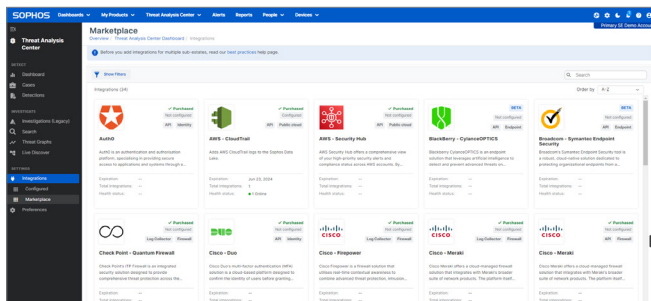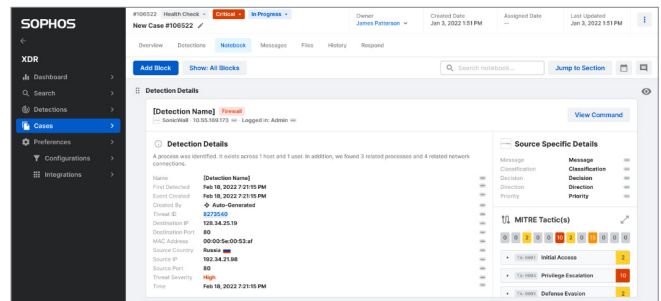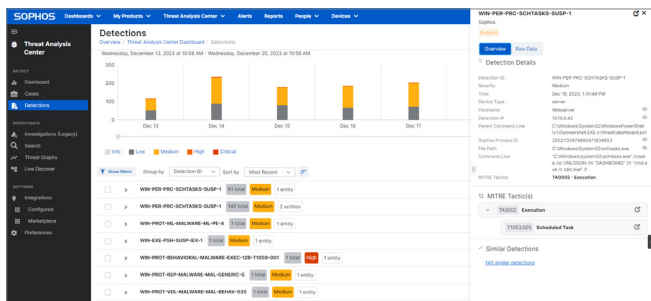
Collaborative case management

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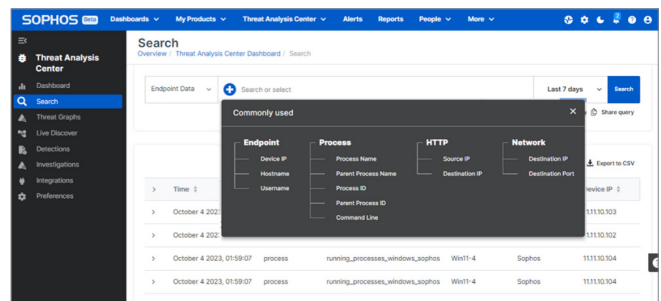

Compatible with Sophos and third-party solutions

Powerful case management and collaboration tools

AI-prioritized detections across all key attack surfaces

Simple and powerful search – no SQL expertise needed

Sophos 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.

Ep Sophos Endpoint

Block advanced threats and detect malicious behaviors across your endpoints

Product included in Sophos XDR pricing

WP Workload Protection

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

Product included in Sophos XDR pricing

Mob Sophos Mobile

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

Product sold separately; integrated at no additional charge

Fw 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

Em 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

Cld Sophos Cloud

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

Product sold separately; integrated at no additional charge

ZT 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

Compatible with:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

+ compatible with other 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 data from Sophos products and third-party (non-Sophos) solutions in the Sophos Data Lake

Extendable to 1 year as an optional add-on

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.

NDR 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

Compatible with:

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

Network

Compatible with:

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

Identity

Compatible with:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft integration included at no additional charge

Email

Compatible with:

- Mimecast
- Proofpoint

Microsoft 365 and Google Workspace integrations included at no additional charge

Cloud

Compatible with:

- Orca Security

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

Backup and Recovery

Compatible with:

- Acronis
- Veeam

1-Year Data Retention

Retains data from Sophos products and third-party (non-Sophos) solutions in the Sophos Data Lake

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 Intercept X Endpoint, providing advanced anti-ransomware and anti-exploitation, AI-powered malware protection and context sensitive defenses that dynamically adapt protection levels.

Find out more at 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

Included with Sophos XDR subscriptions

	Sophos XDR
AI-prioritized detections and guided investigations	✓
Case management, collaboration, and response actions	✓
Simple and powerful search tools for hunting and investigation	✓
Sophos Endpoint and Workload Protection solutions (Intercept X Advanced)	✓
Endpoint Detection and Response (EDR) tools	✓
Cloud data retention	90 days (Extendable to 1 year)
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	✓
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.

Gartner.

Sophos named a Leader in 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for 14 consecutive reports

Gartner Peer Insights Customers' Choice 2024

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

G2 Leader

Sophos named a Leader for Endpoint Protection, EDR, XDR, Firewall, and MDR, in the Summer 2024 G2 Grid® Reports

OMDIA

Sophos was the top-ranked and sole leader in the Omdia Universe for Comprehensive XDR in 2023

MITRE ENGENUITY | ATT&CK® Evaluations

A strong performer in MITRE Engenuity ATT&CK Evaluations for Managed Services

SE Labs

Sophos consistently achieves industry-leading protection results in independent tests

Try it now for free

Register for a free 30-day evaluation at sophos.com/xdr

SOPHOS