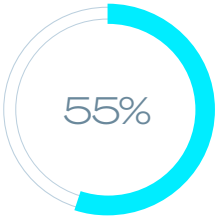
SOLUTION BROCHURE

Sophos Extended Detection and Response (XDR)

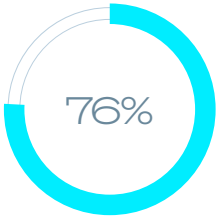
Protect against sophisticated multi-stage, multi-vector attacks

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



Legitimate credentials and unknown vulnerabilities are used to penetrate organizations in 55% of ransomware attacks.[1]

The overall median attacker dwell time in cases investigated by the Sophos Incident Response team is 7 days.[2]



Disparate tools create data silos and manual effort. 76% of organizations experienced cybersecurity burnout over the past year.[3]

Highlights

- Get visibility of suspicious activity and evasive threats across all key attack surfaces.
- An open XDR platform with an expansive range of integrations included.
- Get more ROI from your existing technology investments.
- Investigate and respond to threats quickly with prioritized detections and AI-powered tools.
- Includes industry-leading endpoint protection and EDR.

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.

Gain total attack surface visibility

The more you see, the faster you can act. Our open, extensible architecture provides visibility across your entire IT environment by integrating threat information from your existing investments into a single detection and response platform. Sophos XDR includes integrations with an extensive range of tools and technologies.

Accelerate security operations with GenAI

Maximize analyst efficiency and accelerate investigation and response. AI-powered tools included with Sophos XDR streamline investigations by providing real-time insights, contextualizing threat data, and offering clear recommendations.

An open platform designed to optimize and unify

Benefit from a single view across your IT ecosystem and focus investigation efforts on high-priority items instead of noisy, unactionable alerts. Identify the most serious threats with AI-powered prioritization and analytics, and collaborate with team members with robust investigation workflows and case management tools.

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

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

Natural language AI search and pre-canned query templates enable you to find the information you need for investigations, without needing to be an SQL expert.

Automated responses

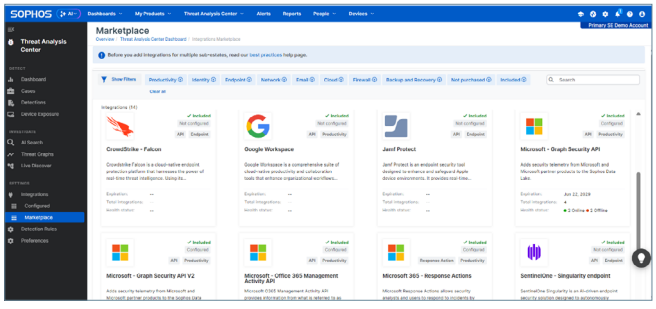
Automated actions like process termination, ransomware rollback, network isolation, and adaptive attack protection, contain threats rapidly and save your team valuable time.

Collaborative case management

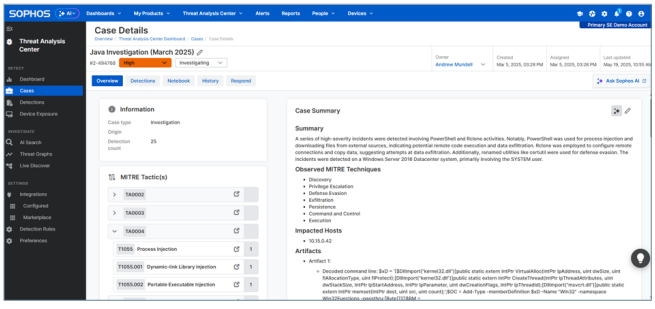
Automatic case creation enables rapid investigation, with comprehensive case management tools for collaboration with other team members.

Analyst response actions

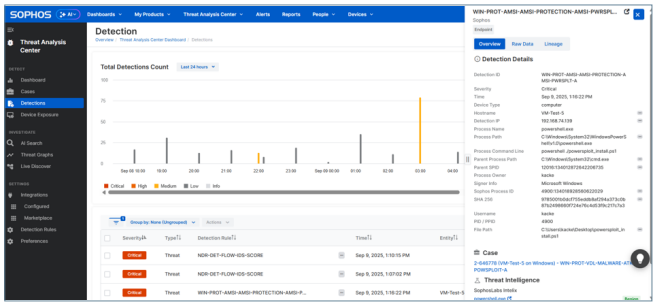
Execute an extensive range of response actions to contain and neutralize threats fast, including in Microsoft 365 environments.



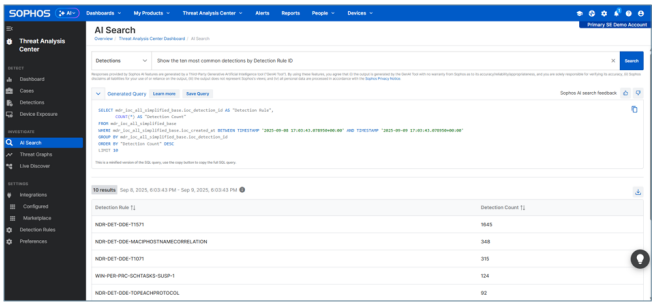
Includes integrations with Sophos and non-Sophos solutions.



Powerful case management and collaboration tools.



AI-prioritized detections across all key attack surfaces.



Natural language AI search– no SQL expertise needed.

Accelerate security operations with GenAI

Extensive Generative AI capabilities in Sophos XDR empower your team to make smart decisions and neutralize adversaries faster, increasing both analyst and business confidence. GenAI features are included automatically with Sophos XDR.

AI Assistant

Guides users of all skill levels through each stage of a case investigation, maximizing efficiency to stop threats fast.

AI Search

Uses natural language to accelerate day-to-day tasks and lower the technology barrier to security operations.

AI Case Summary

Provides an easy-to-understand overview of detections and recommended next steps, helping analysts make smart decisions fast.

AI Command Analysis

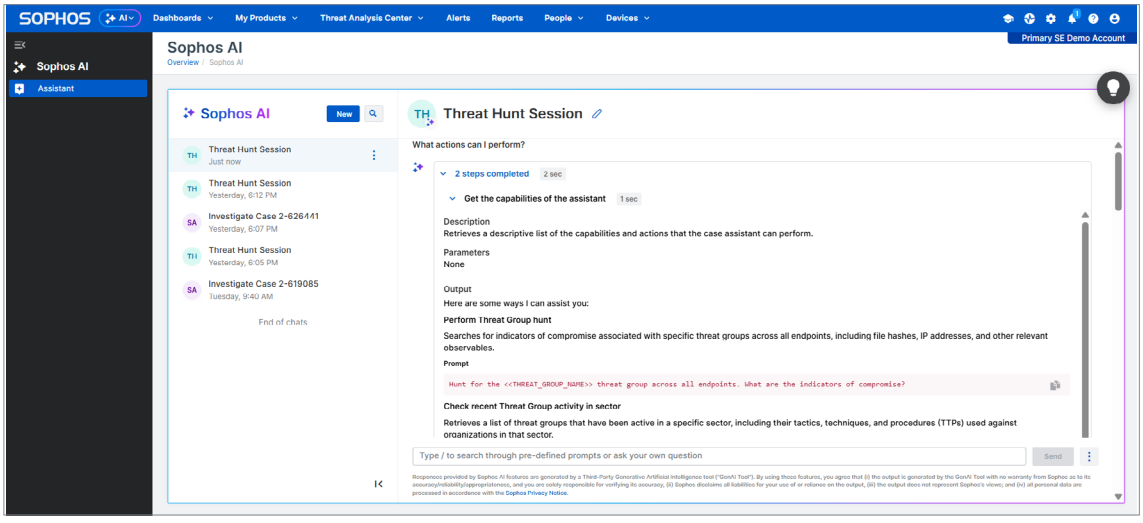
Analyzes complex command line arguments to uncover their intent and impact, with explanations in plain language.

Sophos AI Assistant

The Sophos AI Assistant makes it easy for all users — from IT generalists to Tier 3 SOC analysts — to get the information they need to progress threat investigations and neutralize adversaries fast.

- **Conduct an extensive range of SecOps tasks:** Analyze suspicious commands, list IOCs, enrich data with threat intelligence, create detailed reports, and more.
- **Ask questions using everyday language** or use pre-defined prompts provided by Sophos' threat experts. Benefit from clear summaries and recommended next steps.
- **Designed in partnership with Sophos' frontline security analysts:** Benefit from real-world workflows and the experience of Sophos MDR experts.
- **Continually updated based on the threat landscape:** Ensures access to the latest investigation techniques and threat intelligence from Sophos X-Ops.

This isn't just another AI tool — it's expertise from the team behind the world's leading Managed Detection and Response service, distilled into an intelligent agent.



Sophos "XDR-ready" product integrations

Sophos solutions work together seamlessly to deliver the best-possible security outcomes. Our broad range of award-winning products, including Endpoint, Firewall, NDR, ZTNA, Email, and Mobile, are fully integrated into the XDR platform — and the best-in-class protection of Sophos Endpoint is automatically included.

SOPHOS ENDPOINT

Block advanced threats across your endpoints and servers, including sophisticated ransomware attacks.

Included with Sophos XDR

SOPHOS EDR

Detect, investigate, and respond to suspicious activity and evasive threats targeting your endpoints.

Included with Sophos XDR

SOPHOS ITDR

Monitor your environment for identity risks, and gain dark web intelligence on compromised credentials.

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 NDR

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

Product sold separately; integrated at no additional charge. Compatible with any network via SPAN port mirroring.

SOPHOS ZTNA

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

Product sold separately as part of Sophos Workspace Protection bundle; integrated at no additional charge.

SOPHOS MOBILE

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

Product sold separately; integrated at no additional charge

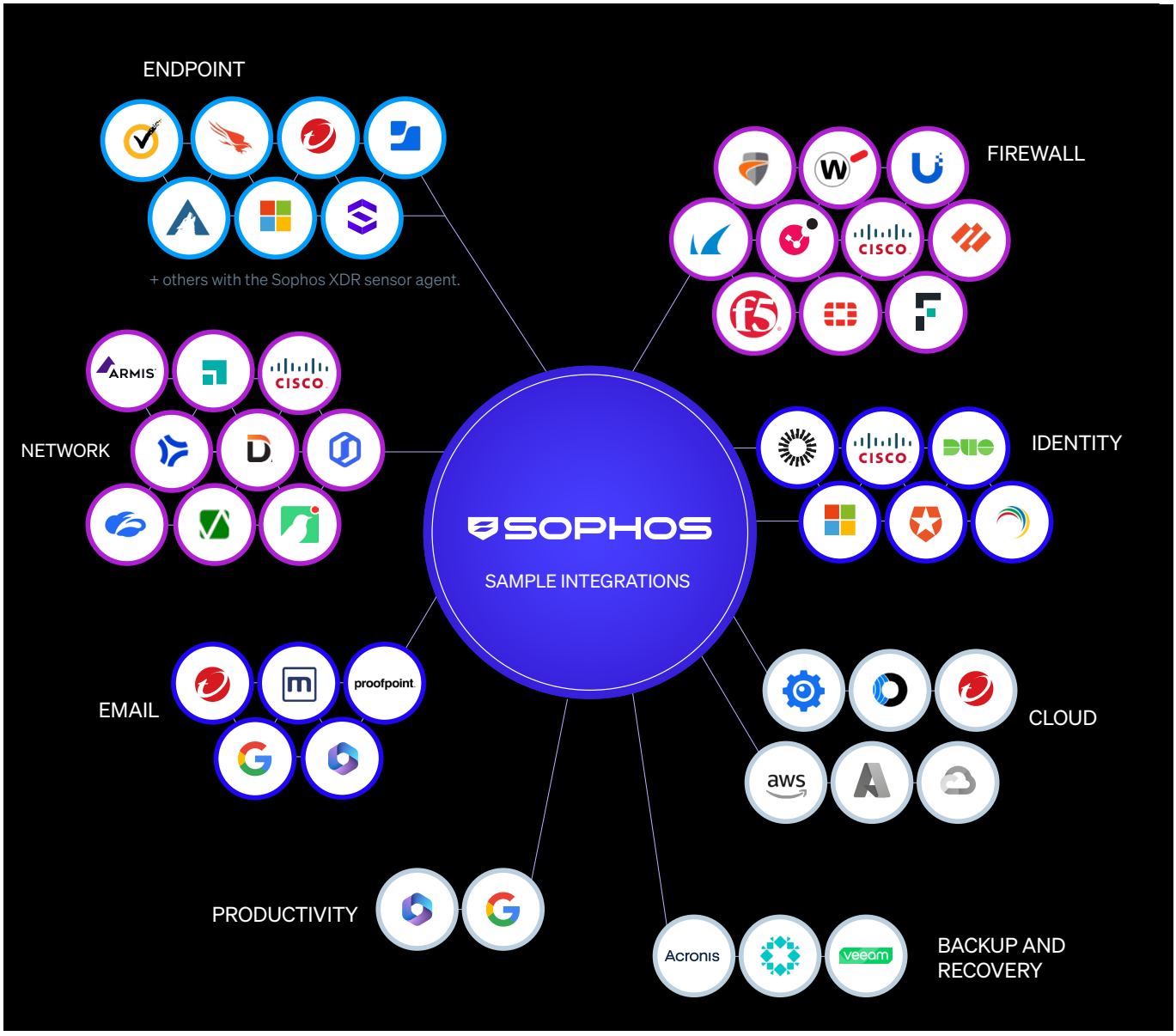
SOPHOS EMAIL

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

Product sold separately; integrated at no additional charge

Leverage your non-Sophos technology investments

Get more ROI from the security tools you use today by integrating them into our open platform. Sophos XDR includes turnkey integrations with an extensive ecosystem of third-party endpoint, firewall, network, email, identity, backup, cloud security, and productivity tools, including Microsoft 365.



The above is a representative sample of non-Sophos technology integrations.

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

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 experienced team of 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-generated threat scores and prioritized detections	✓
Case management, collaboration, and response actions	✓
Powerful natural language search tools for hunting and investigation	✓
GenAI-powered XDR features: AI Assistant, AI Case Summary, AI Command Analysis, AI Search	✓
Sophos Endpoint included (or use your existing non-Sophos endpoint solution)	✓
Detection data retained in the Sophos data lake (90 days as standard)	✓
1-year data retention available	Optional Add-on
Native integrations with Sophos solutions: Sophos Endpoint, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email	✓
Integrations with non-Sophos endpoint, firewall, network, email, cloud, identity, backup, Microsoft 365, and Google Workspace solutions	✓
Sophos Network Detection and Response (NDR)	Optional Add-on
Sophos Identity Threat Detection and Response (ITDR)	Optional Add-on

See why customers choose Sophos XDR

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

Gartner

A Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the 16th consecutive time.

Gartner Peer Insights Customers' Choice 2025

A "Customers' Choice" in the 2025 Gartner® Voice of the Customer report for Extended Detection and Response.

Leader

A Leader in the G2 Spring 2025 Overall Grid® Report for Extended Detection and Response.

MITRE | ATT&CK® Evaluations

Sophos XDR is a strong performer in MITRE ATT&CK Evaluations for Enterprise products.

SE Labs

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

1 Sophos State of Ransomware Report 2025
2 Sophos Active Adversary Report 2025
3 Sophos Report - Addressing Cybersecurity Burnout in 2025

Try it now for free

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

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

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2026-02-04 DS-EN (NP)

SOPHOS