SOLUTION BRIEF

Sophos XDR

Protect against sophisticated multi-stage, multi-vector attacks

Active adversaries are highly skilled cybercriminals that execute attacks at scale and employ sophisticated tactics designed to avoid triggering preventive security solutions. Sophos Extended Detection and Response (XDR) provides powerful tools and threat intelligence that enable you to detect, investigate, and neutralize threats across your entire IT ecosystem, delivered through Sophos' adaptive AI-native, open platform.

Use cases

1 | START WITH THE STRONGEST DEFENSE

Desired outcome: Stop more threats upfront to reduce your workload.

Solution: Focus investigations by stopping more breaches before they start. Sophos XDR includes unparalleled protection to stop advanced threats quickly before they escalate. Elevate your defenses with best-in-class endpoint security — including deep learning AI models that secure against known and novel attacks, behavioral analysis, anti-ransomware, and anti-exploitation.

2 | TOTAL ATTACK SURFACE VISIBILITY

Desired outcome: Gain insights into evasive threats across your environment.

Solution: Our open, extensible architecture provides visibility across the entire attack surface by integrating threat information from your existing and future security investments. Sophos XDR includes turnkey integrations with an extensive ecosystem of endpoint, firewall, network, email, identity, backup, cloud security, and productivity solutions.

3 | ACCELERATE SECURITY OPERATIONS WITH AI

Desired outcome: Empower your security analysts to neutralize adversaries faster.

Solution: AI tools included with Sophos XDR help streamline investigations by providing real-time insights, contextualizing threat data, and offering natural language-driven recommendations. Designed in partnership with our frontline security analysts, the Sophos AI Assistant enables your in-house team to benefit from real-world workflows and the experience of Sophos experts. Use AI tools to conduct an extensive range of SecOps tasks using everyday language or pre-defined prompts. Analyze suspicious commands, identify impacted entities, enrich data with threat intelligence, create detailed reports, and more.

4 | AN OPEN PLATFORM DESIGNED TO OPTIMIZE AND UNIFY

Desired outcome: Respond to threats across multiple attack vectors.

Solution: Benefit from a single view across your entire IT ecosystem in a unified detection and response platform, 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.

Gartner

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

MITRE | ATT&CK® Evaluations

Sophos XDR consistently delivers strong results in MITRE ATT&CK Evaluations for Enterprise products

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

Learn more and start your free trial:
sophos.com/xdr

2025-09-12 SB-EN (NP)