Solution Brief

Sophos XDR

Defend against adversaries with AI-powered EDR and XDR

Active adversaries constantly evolve their techniques to exploit vulnerabilities and accelerate their attack timelines. Reducing the time to detect and respond has never been more critical. Sophos' open, AI-native extended detection and response (XDR) platform enables you to rapidly identify, investigate, and neutralize multi-stage threats across your entire security ecosystem.

Use cases

1 | START WITH A STRONG 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. Protect endpoints and servers using sophisticated technologies, including deep learning AI models that secure against known and novel attacks, behavioral analysis, anti-ransomware, and anti-exploitation.

2 | ACCELERATE THREAT RESPONSE

Desired outcome: Detect, investigate, and respond to threats quickly.

Solution: AI-prioritized detections — leveraging threat intelligence from Sophos X-Ops — make it quick and easy to identify suspicious events that need immediate attention. Conduct threat hunts and rapidly respond with optimized investigation workflows, powerful search capabilities, collaborative case management tools, and automated responses.

3 | VISIBILITY ACROSS ATTACK SURFACES

Desired outcome: Gain full visibility and insight into evasive threats across your environment.

Solution: Use Sophos' fully integrated and XDR-ready solutions to provide visibility beyond endpoints — or leverage your existing technology investments. Integrate an extensive ecosystem of third-party endpoint, firewall, network, email, identity, backup, and cloud security solutions to detect and respond to threats with a unified XDR platform.

4 | POWERFUL FOR ALL USERS

Desired outcome: IT generalists and security analysts can investigate and respond with ease.

Solution: Designed for both dedicated in-house SOC teams and IT administrators, Sophos XDR helps maximize user efficiency and provides full visibility and guidance to help you respond to threats. Extensive GenAI-powered capabilities empower you to neutralize adversaries faster, increasing both analyst and business confidence.

Gartner

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

MITRE ATT&CK™

Sophos XDR delivered exceptional results in the 2024 MITRE ATT&CK® Evaluations: Enterprise

G2 Leader

Sophos rated a Leader in the Winter 2025 G2 Grid® report for XDR Platforms

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

2025-02-03 DS-EN (MP)

SOPHOS