Solution Brief

Sophos XDR

Defend Against Active Adversaries with EDR and XDR

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' unified extended detection and response (XDR) platform enables you to rapidly detect, investigate, and respond to multi-stage threats and active adversaries across your 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 AI, 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 all of your key attack surfaces.

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, 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 internal SOC teams and administrators who cover security and other IT responsibilities, Sophos XDR helps maximize user efficiency and provides full visibility and guidance to help you respond to threats.

Gartner

Recognized in the 2023 Gartner Market Guide for XDR

MITRE ATT&CK

Exceptional results in the 2023 MITRE Engenuity ATT&CK Evaluations

Leader

Rated the #1 XDR solution by G2 users (Spring 2023)

Learn more and trial Sophos XDR:
sophos.com/xdr

2023-11-08 DS-EN (MP)

SOPHOS