Sophos Extended Detection and Response (XDR)

Stopping attacks quickly is critical. Sophos XDR enables organizations to detect, investigate, and respond to multi-stage threats, across all key attack vectors, in the shortest time.

Why XDR

- XDR unifies data from multiple security products to automate and accelerate threat detection, investigation, and response in ways that isolated point solutions cannot.
- XDR capabilities reduce the complexity of threat detection and response, enabling organizations to prevent successful attacks from advanced adversaries.

Sophos XDR Overview

- Sophos XDR provides comprehensive detection and response capabilities across all key attack surfaces.
- Includes Sophos' industry-leading endpoint protection and EDR capabilities.
- Data from multiple Sophos solutions and third-party tools is correlated with advanced threat analytics to identify suspicious activity.
- Intuitive tools and workflows are provided in a dedicated Threat Analysis Center in Sophos Central.

Simple Licensing Approach

- Start by selling XDR licenses for to "endpoints and servers, then add other Sophos XDR-ready solutions.
- Add third-party Integration Packs to increase visibility — and your deal size!
- Volume discounting built-in.
- MSP Flex billing available.

Why Choose Sophos XDR

- Complete and integrated portfolio of XDR-ready solutions (Endpoint, Workload, Mobile, Firewall, Network, ZTNA, Email, and Cloud).
- Leverage existing technology investments by integrating third-party tools with Sophos XDR.
- A single console provides visibility and control across all key attack surfaces.
- Prevention-first approach reduces breaches, adapts defenses, and reduces your investigation workload.
- Optimized workflows designed for both IT generalists and experienced analysts.

Sophos XDR: Delivering Superior Cybersecurity Outcomes

Sophos delivers superior cybersecurity outcomes by giving customers the advantages they urgently need. See how competitor solutions stack up at sophos.com/compare.

"I love my SentinelOne"

Response: Sophos allows you to consolidate your cybersecurity spending and significantly reduce your management burden. SentinelOne is primarily an endpoint company and offers little opportunity for consolidation. You need more than just SentinelOne's endpoint protection to optimize your security posture and defend against active adversaries.

"I love my CrowdStrike"

Response: CrowdStrike certainly has a popular detection and response product. However, customers are often looking for the strongest prevention capabilities to minimize their investigation workload. Sophos provides on-device protection and automated response that eliminates threats in real time. CrowdStrike gathers and analyzes data in the cloud, slowing response time.

"I love my <Any other XDR>"

Response: We replace many of these products because customers often struggle with them. Customers want simple, optimized workflows and the ability to leverage their existing technology investments by integrating them into a unified XDR platform and toolset.

Discovery Questions

- Are you overwhelmed with alerts from multiple tools?
- Can you easily identify the most important events to investigate across your attack surfaces?
- Are you using multiple consoles to see and investigate suspicious activity?
- Do your tools provide optimized workflows for quick investigation, like SQL-free search?
- Does your current solution stop most threats upfront to minimize your investigation workload?
- Does your vendor regularly participate in third-party tests? Have you checked their latest results and reviews on Gartner Peer Insights, G2, Gartner MQs, and MITRE ATT&CK?

23-11-08 -DA-[MP]

SOPHOS