SOPHOS

SOPHOS XDR + NEXT-GEN SIEM

Security operations and compliance for the agentic era.

Stop AI-driven attacks and simplify compliance without adding complexity.

As AI expands the threat surface and accelerates attacks, fragmented security tools struggle to keep up. Sophos XDR with Next-Gen SIEM unifies protection, detection, investigation and response, and supports your regulatory requirements in a unified AI-Native Cybersecurity Defense System.

55% of ransomware attacks use legitimate credentials or exploit vulnerabilities[1]

76% of organizations experience cybersecurity burnout due to alerts[2]

80% of CISOs cite redundant compliance efforts due to siloed workflows[3]

1.3B AI agents projected by 2028, expanding your attack surface[4]

WHAT SOPHOS DELIVERS

AI architecture. Smarter, accelerated response.

Empower every analyst to operate at scale.

AI tools and automation flatten the learning curve, eliminate fatigue, and drive more efficient detection, investigation, and response — so analysts can do more, faster, and with confidence.

- AI assistants speed investigations and threat hunting
- Case-centric workflows automatically group, prioritize, and contextualize related activity
- Built-in automation playbooks accelerate response actions and eliminate manual tasks

Intelligence that compounds.

Sophos XDR gets smarter with every threat, using real-world intelligence at a global scale to strengthen detection and response.

- Intelligence from 625,000+ protected organizations feeds AI models and detection logic
- Insights from 380,000+ MDR investigations annually
- Learnings applied automatically, in real time

Detect, investigate, respond, retain.

Eliminate duplicated effort. Sophos XDR with Next-Gen SIEM powers modern security operations and long-term compliance, all unified by design.

- Protection, detection, investigation, response, and audit workflows, all within one system
- Security and compliance-focused telemetry retention for up to 10 years
- Licensed by users and servers, not data volume, keeps costs predictable

Bring your own stack, or use ours.

Vendor-agnostic by design. Ingest everything from security signals to compliance-focused telemetry from the tools you already use.

- Vast, AI-assisted integrations bring in telemetry across security and compliance data sources
- Two-way integrations enable response directly in your existing tools
- Sophos Endpoint and Sophos Email Monitoring System (EMS) included for superior protection

AT A GLANCE

- Unify security operations (threat protection, detection, investigation, and response) and compliance efforts in one cohesive system
- Accelerate investigations and response with AI tools and assistants
- Identify multistage attacks across endpoint, identity, email, cloud, network, and productivity tools
- Automate threat response using built-in SOAR playbooks
- Stay ahead of threats with embedded adversary intelligence from Sophos X-Ops

WHO NEEDS IT

- Security teams overwhelmed by alert noise and manual investigations
- Organizations modernizing security operations for AI-driven threats
- Businesses looking to unify threat response and compliance workflows
- Compliance teams needing to meet audit requirements without the complexity and cost of a traditional SIEM
- MSPs and resellers delivering scalable, premium SecOps solutions

UPGRADE TO SOPHOS MDR

Run a world-class SOC without building one.

24/7 fully managed threat response.

Sophos XDR and Next-Gen SIEM can be seamlessly upgraded to Sophos MDR for expert-led investigation and response.

AI speed. Human judgment.

Sophos MDR is the world's largest Agentic SOC — AI investigates and resolves threats in seconds; analysts own the outcomes.

Expertise at global scale.

Extend your in-house team with Sophos global security experts including analysts, threat hunters, researchers, responders, and AI engineers.

INDUSTRY RECOGNITION

Validated by the analysts and organizations that matter most.

GARTNER 2026

17-time Leader, Endpoint Protection

G2 SUMMER 2026

#1 rated XDR solution

MITRE ATT&CK EVALS

100% detection coverage

GARTNER PEER INSIGHTS

A "Customers' Choice" for XDR

One system. Every control point. Defending as one.

Sophos XDR with Next-Gen SIEM is part of Sophos Fusion, the world's most complete cyber defense system. It protects organizations from AI-enabled threats that move faster than defenders can respond. **sophos.com/XDR →**

[1] Sophos State of Ransomware Report 2026. [2] Sophos, Addressing Cybersecurity Burnout in 2025. [3] The CISO Society 2025 State of Continuous Controls Monitoring Report. [4] IDC Info Snapshot, 2025.

2026-07-07 SB-EN (MC)

SOPHOS