SOPHOS

SOPHOS XDR + NEXT-GEN SIEM

Superior detection. Unmatched response. Open by design.

Security operations and compliance for the agentic era.

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.

500+
technology integrations with the ability to add more

130+
turnkey automation playbooks with built-in extensibility

10yrs
data retention for security and compliance telemetry

Attackers are using AI to move faster, target more systems, and evade traditional defenses. At the same time, compliance requirements are tightening, retention timelines are extending, and security teams are stretched thinner than ever.

Sophos XDR and Next-Gen SIEM meets these challenges within Sophos Fusion, the most complete AI-native Cybersecurity Defense System, unifying protection, detection, investigation, response, and long-term data retention so your team can stop modern attacks faster and meet regulatory requirements without adding tools or complexity.

SOPHOS XDR
Powered by Secureworks

As part of Sophos Fusion, **Sophos XDR Powered by Secureworks** brings together Secureworks' Taegis detection and response capabilities, X-Ops intelligence, and deep security operations expertise within Sophos XDR. Following Sophos' acquisition of Secureworks in 2025, this combination unites Sophos' AI-driven security and industry-leading threat intelligence with advanced XDR to deliver an open, unified architecture with broad integrations and adaptive protection, detection, and response.

OUTCOMES THAT MATTER

- **Faster, more confident threat detection and response.** AI-driven triage, insights, plain-language summaries, and automatic response empowers every analyst to operate at scale.
- **Reduced analyst burnout and alert fatigue.** Best-in-class endpoint protection is built in to stop more threats upfront.
- **Compliance support without a separate SIEM,** combining long-term retention and compliance-focused data in the same system your security analysts already use.
- **Predictable, scalable costs** with user-and-server count pricing instead of data-volume billing, eliminating cost surprises as data requirements grow.
- **Unified visibility across your full environment,** including turnkey integrations with 500+ third-party tools, cloud environments, identity systems, business applications, and AI-assisted custom integrations to meet your specific needs.
- **Long-term data retention options** of 13 months, 3, 5, 7, and 10 years, giving compliance and security teams their required data without managing a separate platform.
- **Seamlessly upgrade to Sophos MDR** when your organization needs a fully managed 24/7 detection and response service.

THE CHALLENGE

The adversary got an AI upgrade

Attackers now operate with speed, scale, and automation that manual workflows can't match. At the same time, AI is embedded across email, identity, cloud, and SaaS applications, expanding the attack surface.

Your challenges

- Faster attacks
- Expanded attack surface
- Fragmented tools
- Under-resourced teams
- Alert overload
- Compliance pressure

Attackers don't break in. They log in. They move laterally, blend into systems, and use legitimate credentials and familiar tools to evade detection at every layer. 67% of attacks last year succeeded by simply logging into trusted tools with compromised credentials.[1]

Most environments are built on disconnected tools, each with separate data, separate alerts, and separate AI. This fragmentation is where agentic, multi-vector attacks thrive, hopping from email to identity to endpoint to cloud at AI speed while tools fire in isolation and manual analysis can't correlate.

At the same time, the pressure on security teams continues to compound:

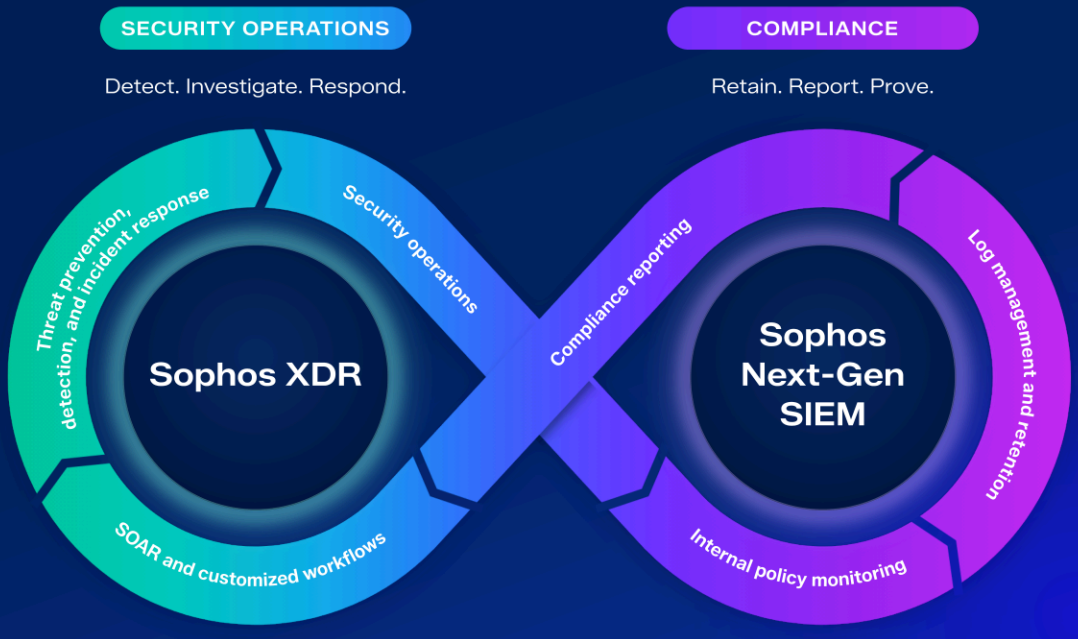
- **Fragmented tech stacks are growing while team headcounts remain the same.** 67% of organizations hit by ransomware cite lack of resources as a contributing factor.[1]
- **76% of security teams report burnout** from low-fidelity alerts.[2]
- **80% of CISOs report duplicate effort** between security and compliance efforts.[3]

Effective defense now requires more than standalone tools. It requires an AI-native architecture, always-on visibility, adversary threat intelligence, and a compliance-ready data layer, all operating as one system.

THE SOLUTION

Sophos XDR with Next-Gen SIEM

Sophos XDR with Next-Gen SIEM is part of **Sophos Fusion, the most complete cyber defense system** that continuously unifies threat protection, detection, investigation, response, and long-term data retention in a single solution. It is purpose-built to help security teams stop modern attacks faster, meet compliance requirements without duplication, and operate with confidence as the threat landscape evolves.



What Sophos XDR with Next-Gen SIEM delivers

Designed for the agentic era

AI is native to the architecture, not bolted on, empowering every analyst to operate at scale across detection, triage, investigation, and response.

Intelligence that compounds

Real-world intelligence from 625,000+ Sophos-protected organizations and insights from 380,000+ annual MDR investigations compounds automatically, strengthening security across all customers in real time.

Protect, detect, investigate, respond, retain

One unified system serves both security operations and compliance needs, extending Sophos XDR with long-term retention and audit-ready data.

Vendor-agnostic, open by design

Use the tools you already have. With 500+ pre-built integrations and AI-assisted custom data parsers, connect your existing solutions across endpoint, identity, email, cloud, network, and business applications. No rip-and-replace required.

Respond at machine speed

Automate actions including threat response, ticket creation, and notifications with extensive out-of-the-box SOAR connectors and 130+ playbooks, with the flexibility to create more.

Adversary intelligence, built in

Access top-tier threat intelligence from Sophos X-Ops directly within your investigation workflows, including threat intelligence actor insights, malware intelligence, and real-world attack context.

Better protection, fewer alerts

Sophos Endpoint is included and natively integrated with Sophos XDR to block more attacks upfront and reduce alert fatigue.

Expose hidden email threats

The Sophos Email Monitoring System (EMS) is also included to detect advanced email threats missed by existing tools — without impacting mail flow — so your team can monitor and clawback malicious messages.

AI-augmented security analyst workflow

AI bends the learning curve. Every analyst operates with confidence, faster.

Detect and correlate: AI connects signals across your environment, turning raw events into prioritized, understandable threats.

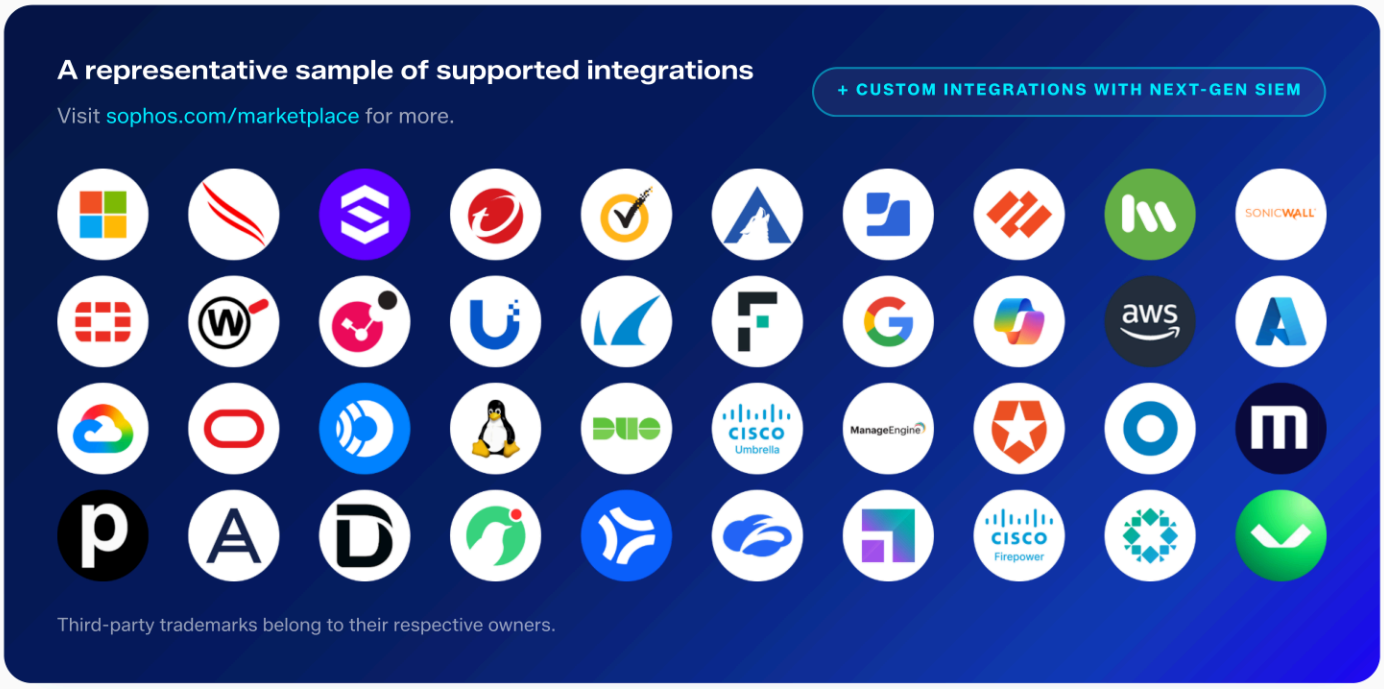
Triage and prioritize: AI eliminates manual triage, grouping related activity into clear, context-rich cases so analysts can focus on what matters most.

Investigate: AI assistants designed in partnership with Sophos MDR frontline analysts turn complex security data into clear, explainable insights.

Respond and resolve: AI accelerates response with guided actions, context-aware automation, and integrated SOAR to deliver faster resolution without sacrificing control.

INTEGRATION ECOSYSTEM

Vendor-agnostic. Bring your stack or use ours.



Defend against attacks that move across systems without replacing your existing tools. Sophos XDR with Next-Gen SIEM enables your security teams to defend against multi-stage, multi-vector attacks, regardless of the technologies in place, including the most comprehensive Microsoft security integration on the market.

With 500+ integrations included, and AI-assisted custom integrations, you can bring together telemetry from endpoint, identity, email, cloud, network, and business applications into a single workflow. Two-way integrations and built-in automation allow your team to take action directly within your existing tools, reducing friction and accelerating response.

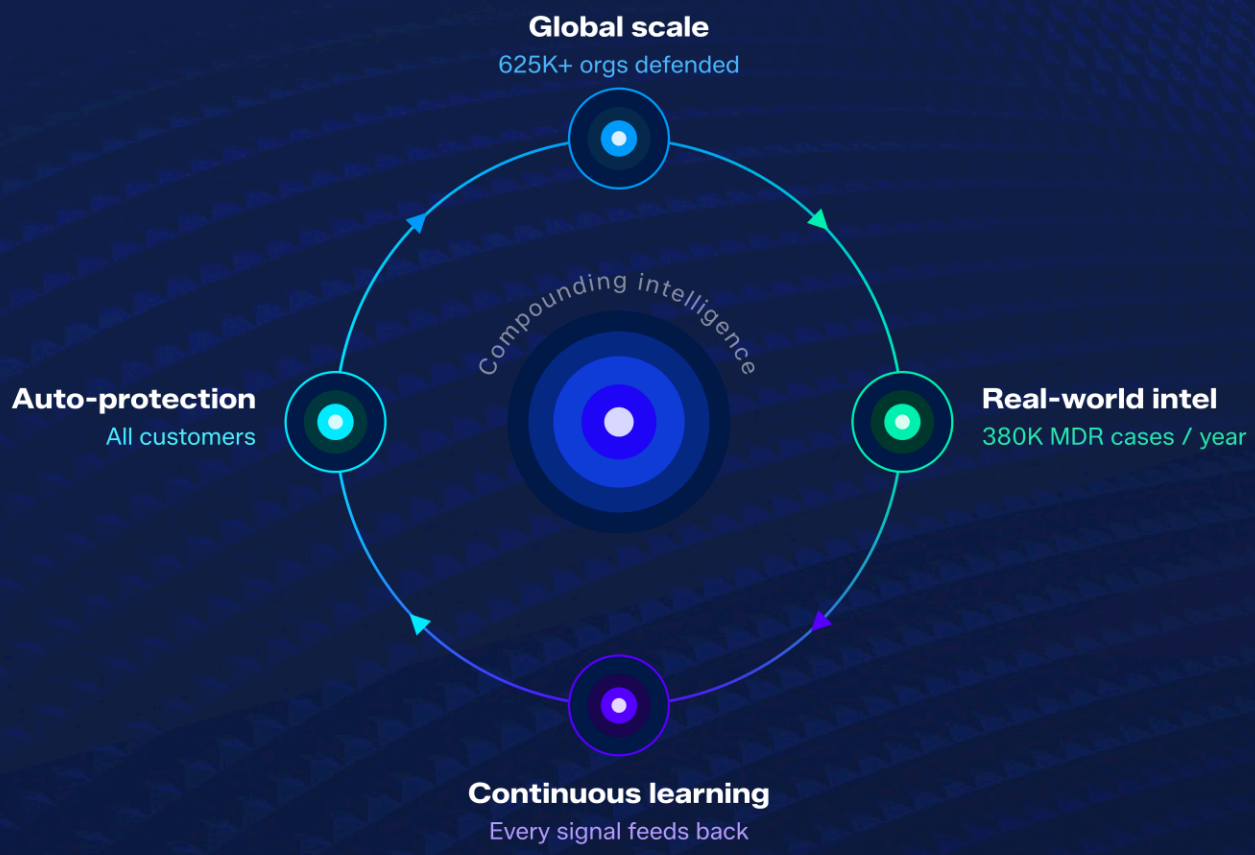
The same system supports real-time security operations and long-term data needs. Seamlessly ingest data from any source and retain it over time, ensuring full context for investigations, audits, and compliance reporting.

SECURITY OPERATIONS AND COMPLIANCE. ONE SYSTEM.

- **Sophos XDR Powered by Secureworks** provides the speed and precision to detect and respond to threats in real time. **Sophos Next-Gen SIEM** extends XDR with the historical depth compliance teams require. Both run on the same unified system, so security and compliance-focused telemetry coexist without duplication, and analysts have access to the full picture, whether they are investigating an active threat or building an audit trail.
- **Sophos XDR Powered by Secureworks** comes with 90 days of data retention by default, with Sophos Next-Gen SIEM add-ons extending retention to your choice of 13 months, 3, 5, 7, or 10 years. This supports organizations with the most demanding regulatory and audit requirements with predictable user-and-server count pricing, rather than data-volume billing.

AI-NATIVE CYBERSECURITY

Intelligence that compounds



Built to learn and improve security over time.

Sophos XDR with Next-Gen SIEM is part of Sophos Fusion, the most complete cyber defense system that unifies and continuously learns from real-world activity across 625,000+ customer environments. Insights from 380,000+ Sophos MDR investigations each year refine Sophos XDR detections, AI models, and response logic, automatically applied in real time to strengthen protection across all Sophos customers. Every threat encountered makes the next defense stronger.

PREVENTION-FIRST

Better prevention. Fewer alerts.

Attacks frequently enter through email and execute or spread at the endpoint. Sophos XDR Powered by Secureworks takes a prevention-first approach, stopping more threats upfront so analysts can focus on the sophisticated attacks that evade automated tools.

Sophos Endpoint is included with Sophos XDR, providing AI-driven threat prevention and behavioral detection. High-fidelity endpoint telemetry gives analysts deeper context for faster, more confident investigation and response.

Sophos Email Monitoring System (EMS) is also included, bringing email signals into the same XDR detection and investigation workflow without replacing or interrupting existing email security tools. Vendor-agnostic and compatible with third-party email security solutions, EMS identifies advanced phishing, BEC, and malicious emails that other solutions miss, with clawback capability for Microsoft 365 and Google Workspace.

UPGRADE TO SOPHOS MDR

Run a world-class SOC without building one

Sophos XDR with Next-Gen SIEM can be seamlessly upgraded to Sophos MDR for fully managed, 24/7 expert-led detection, investigation, and response. Sophos MDR is the world's largest Agentic SOC. AI speed. Human judgment.

52%

of MDR cases are resolved end-to-end by AI

89 sec

on average to resolve a case end-to-end by AI

Why organizations choose Sophos XDR with Next-Gen SIEM

AI-native architecture, not bolted-on

AI is the connective tissue of the system, not a module layered on top. It correlates signals, reduces noise, drives triage, and guides response across your full environment.

One system for security and compliance

Sophos XDR and Next-Gen SIEM operate within the same Cybersecurity Defense System. Security and compliance-focused telemetry coexist without duplicate ingestion. Analysts use a single workflow for investigations, audits, and reporting, and accelerating response and compliance efforts.

Compounding intelligence

Every threat encountered, every investigation completed, and every environment defended feeds back into the system's AI models and detection logic. Customers don't just benefit from their own data, they benefit from the collective intelligence of 625,000+ defended organizations and 380,000+ annual MDR investigations.

Vendor-agnostic by design

Bring your stack, or use ours. With hundreds of pre-built and AI-assisted custom integrations, connect your existing tools into a unified detection and response system, with no rip-and-replace and no forced consolidation.

Predictable, scalable pricing with Next-Gen SIEM

Simple user-and-server count pricing means costs scale with your organization, not your data volume. As compliance requirements tighten and retention timelines extend, your pricing remains predictable.

LICENSING

Security operations... without compliance complexity

Sophos XDR
Powered by Secureworks

SecOps / threat detection and response

- **Sophos AI tools** — Empower your team with AI natural language search, case summaries, and command-line analysis.
- **Sophos AI assistants** — Accelerate threat discovery and remediation with security analyst and threat hunting AI agents.
- **Vast, pre-built integrations** for full visibility of your environment. Two-way integrations enable direct response actions.
- **Thousands of advanced detectors** from Secureworks, developed and continuously enhanced by our detection engineers as the threat landscape evolves.
- **Powerful rule builder** to create custom detections unique to your environment.
- **Automatic case generation** and comprehensive case management tools.
- **Extensive SOAR connectors and playbooks** to automate manual tasks.
- **Embedded top-tier threat intelligence** and threat actor information from Sophos X-Ops.
- **Sophos Endpoint, Sophos EDR, and Sophos Email Monitoring System (EMS)** included.
- **90-day data retention** included as standard.

+ ADD-ON

Sophos Next-Gen SIEM

Extends XDR for compliance

+ **Extend data retention** up to 13 months, 3, 5, 7, or 10 years.
+ **Ingest additional compliance-focused telemetry** in addition to threat-related signals.
+ **Custom integrations** with AI-assisted data parsers.
+ **Built-in compliance dashboards.**
+ **Predictable user/server based pricing** aligned to your Sophos XDR subscription.

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

SPEAK WITH AN EXPERT

Sophos XDR with Next-Gen SIEM: One system for security operations and compliance.

Request a quote or start a free trial.

sophos.com/XDR →

[1] Sophos Active Adversary Report 2026.
[2] Sophos — Addressing Cybersecurity Burnout in 2025.
[3] The CISO Society — 2025 State of Continuous Controls Monitoring Report.

2026-07-07 BR-EN (MC)

SOPHOS