SOPHOS NEXT-GEN SIEM

# Compliance without complexity.

## More data. More to retain. One system to handle it.

Regulatory demands are growing, and fragmented tools can't keep pace. Sophos Next-Gen SIEM extends Sophos XDR and MDR with long-term retention and compliance-focused reporting to meet your regulatory needs — no new console, no added complexity.

**80%** of CISOs cite redundant compliance efforts due to siloed workflows[1]

**85%** of organizations report rising compliance complexity[2]

**42%** of SOCs have no plan for the data in their SIEM[3]

WHAT SOPHOS DELIVERS

## Security and compliance. Built in, not bolted on.

### Eliminate duplicated effort.

Sophos Next-Gen SIEM is a natural extension to Sophos XDR or Sophos MDR, not a separate tool. Get compliance-focused data and long-term retention inside the system you already use.

- Unified with Sophos XDR and MDR workflows
- Ingests both threat-relevant and compliance-focused data
- No separate console, no fragmented investigations

### No ingestion fees. No cost creep.

Traditional SIEM solutions charge by volume. The more data you retain, the more you pay. Sophos Next-Gen SIEM is licensed by users and servers, keeping your costs predictable.

- Retain data for up to 10 years
- Predictable costs as data volumes grow
- Helps meet major compliance framework requirements

### Retain what your regulations demand.

Sophos Next-Gen SIEM adds flexible ingestion for the data sources needed to meet your organization's requirements, beyond the 500+ integrations already included with Sophos XDR and MDR.

- Ingest additional compliance-focused telemetry from endpoint, identity, network, cloud, email, and more
- Retain threat-relevant and compliance data for long-term investigation and reporting
- Custom, AI-assisted integrations for data sources unique to your environment

### Your security data, now audit-ready.

Compliance shouldn't mean storing your data in multiple systems. Sophos Next-Gen SIEM keeps your full historical context centralized and accessible for streamlined audits and reporting.

- Unify security and compliance data for faster reporting
- Reduce redundant data collection
- Monitor coverage and posture with built-in compliance dashboards

## AT A GLANCE

- Extend Sophos XDR or Sophos MDR to meet compliance needs
- Retain security and compliance telemetry for up to 10 years
- Ingest data from custom sources unique to your environment
- Unify protection, detection, investigation, response, and audit workflows in one system
- Simple, predictable pricing based

## WHO NEEDS IT

- Organizations facing multi-year retention requirements
- Compliance and risk teams seeking data retention without the cost and complexity
- Organizations in heavily regulated industries — financial services, healthcare, government
- MSPs and resellers delivering scalable, premium SecOps and compliance solutions

SOPHOS NEXT-GEN SIEM + SOPHOS MDR

# More context. Better outcomes.

### Managed threat response with full context

Sophos Next-Gen SIEM brings years of security and compliance telemetry into Sophos MDR investigations, giving analysts the full context needed to validate, contain, and respond.

### AI speed. Human judgment.

Sophos MDR is the world's largest Agentic SOC — AI analyzes volumes of real-time and historical data in seconds; analysts own the security outcomes.

### Smarter with every threat.

Every threat across 625,000+ defended organizations and 380,000+ annual MDR investigations makes the next defense stronger. Expanded historical context surfaces patterns that point to future risk, strengthening protections everywhere.

INDUSTRY RECOGNITION

# Validated by the analysts and organizations that matter most.

**GARTNER 2026**

17-time Leader, Endpoint Protection

**G2 SUMMER 2026**

#1 rated for XDR and MDR

**MITRE ATT&CK EVALS**

100% detection coverage

**GARTNER PEER INSIGHTS**

A "Customers' Choice" for XDR and MDR

**FROST & SULLIVAN**

Leader, Frost Radar™ for MDR

**KUPPINGERCOLE 2026**

Leader, Leadership Compass for MDR

## One system. Every control point. Defending as one.

Sophos 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/NG-SIEM →**

[1] The CISO Society, 2025 State of Continuous Controls Monitoring Report. [2] PwC, Global Compliance Survey 2025. [3] SANS, 2025 SOC Survey.



2026-07-07 SB-EN (MC)

SOPHOS