SOLUTION BRIEF

Taegis XDR with Next-Gen SIEM

Enterprise grade threat detection and response

Taegis Extended Detection and Response (XDR) offers superior detection, unmatched response and an open security operations platform that integrates with market-leading technologies to deliver measurable security outcomes.

USE CASES

1 | Open security operations platform

Desired outcome: Gain insights into active and evasive threats across your environment

Solution: The Taegis platform is a highly interoperable security operations platform that provides visibility across your entire attack surface by integrating threat information from your existing and future security investments, enabling greater efficiency and better security outcomes. With hundreds of supported integrations from best-of-breed security vendors and an integration automation layer, the Taegis platform can ingest telemetry and logs, providing visibility and insights across your environment.

2 | Superior detection

Desired outcome: Accelerate your mean-time-to-detect threats

Solution: Taegis XDR uses AI-prioritized detections to improve the signal-to-noise ratio and enriches them with threat intelligence from the Sophos Counter Threat Unit (CTU) to detect advanced and emerging threats. Curated threat detection rules are continuously developed, managed and maintained by Sophos. Security Analysts received the high-fidelity detections augmented with the content and data they need to understand a threat.

3 | Automation and unmatched response

Desired outcome: Accelerate response to stop threats in the shortest timeframe

Solution: Taegis XDR builds a holistic picture of detected threat activity and leverages Automation Actions to swiftly contain threats and Security Automation, Orchestration and Response (SOAR) playbooks to eradicate and remediate effectively and efficiently.

4 | Data retention and Next-Gen SIEM

Desired outcome: Cost effective data retention and compliance

Solution: Next-Gen SIEM capabilities are included with Taegis, providing broad ingestion and generous data storage allocations with predictable pricing. Cost effectively store both threat-relevant and compliance-required telemetry for up to 5 years (1 year as standard), and leverage AI-enabled natural language search across all retained data, prebuilt and custom reports, and dashboards.

RECOGNITION

Gartner

Sophos Endpoint (included with Taegis XDR) is a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the 16th consecutive time

A Leader in the G2 Spring 2025 Overall Grid® Report for Extended Detection and Response

Learn more at sophos.com/taegis

Gartner, Magic Quadrant for Endpoint Protection Platforms, Evgeny Mirolyubov, Deepak Mishra, Franz Hinner, 14 July 2025. Gartner is a registered trademark and service mark and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

2025-11-28 SB-EN (NP)

SOPHOS