SOLUTION BRIEF

Taegis MDR with Next-Gen SIEM

Enterprise grade threat detection and response as a managed service.

Taegis Managed Detection and Response (MDR) is a fully managed service that combines 25 years of service delivery experience with an open platform to deliver measurable security outcomes. Whether fully managed or operated in collaboration with your security analysts, Taegis MDR accelerates your security maturity and delivers superior detection and response with cost-effective retention to support compliance.

USE CASES

1 | 24/7 threat monitoring with human expertise

Desired outcome: Surround yourself with experts who can collaborate with or extend your IT and Security team to respond to threats

Solution: The Taegis MDR team monitors your environment 24/7 with experts who help you achieve your desired outcomes. Customize the service with options like the Elite Threat Hunting add-on for tailored threat hunting or a Technical Account Manager to help you get the most from the Taegis platform. Your Customer Success representative ensures efficient delivery and usage of Taegis services.

2 | Open security operations platform

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

Solution: Taegis is a highly interoperable security operations platform that enhances visibility across your attack surface by integrating threat information from current and future security investments. With hundreds of integrations and an automation layer, it can ingest telemetry and logs, leverage AI to improve signal-to-noise ratios, and enrich detections with threat intelligence to improve security outcomes.

3 | 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.

4 | Comprehensive threat response

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

Solution: Taegis MDR security analysts work on security incidents until resolution, leveraging their knowledge and expertise, along with threat intelligence from the Sophos Counter Threat Unit (CTU). They can take response actions with your prior approval to immediately mitigate detected threats.

RECOGNITION

Gartner Peer Insights Customers' Choice 2024

Sophos named a Customer's Choice in the 2024 Gartner Voice of the customer Report for Managed Detection and Response

Gartner

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

The top-rate managed detection and response services rated and reviewed by customers on G2

Learn more at www.sophos.com/taegis

2025-11-28 SB-EN (NP)

SOPHOS