

DATA SHEET

Taegis MDR

Scale Your Security Operations with a 24x7 Threat Detection and Response Unit

Secureworks Taegis MDR is our 24x7 managed detection and response service, which works for you to detect advanced threats and take the right action. Our threat hunting, incident response and security operations expertise, combined with our focus on building a trusted relationship with you and your team, help strengthen your organization's security posture.

Up-Level Security Skills and Resources and Reduce Costs

With limited resources at your disposal, protecting your organization from advanced threats can seem overwhelming. [Taegis MDR](#) is designed to alleviate this burden and help you uncover threats 24x7. We achieve this through a combination of:

- Award-winning Taegis XDR extended detection and response software that applies advanced analytics to detect threats
- Optional: Sophos Endpoint is automatically included, delivering industry-best endpoint protection
- Market-leading services that are informed by over 20 years of experience in security operations

This is in addition to a diversity of attacker data gained from thousands of incident response and adversarial testing engagements annually, and in-depth threat research performed by Secureworks Counter Threat Unit™.

[Taegis XDR](#) uses AI, machine learning, automations, threat intelligence, and user behavioral analytics for rapid threat detection. Our team will expose adversaries by prioritizing endpoint, network, and cloud

threat activity and identify which events require action. Receive unlimited response for in-scope assets. While we fully manage* this technology on your behalf, you will have full access to it so that we can collaborate on investigations via live chat.

Threat hunting is an included component of Taegis MDR to proactively isolate any malware that managed to evade your existing controls.

Taegis MDR Plus provides a more tailored solution that enables customers to further maximize their security program investment. Taegis MDR Enhanced delivers everything available in MDR, along with higher-touch threat investigation, governance and advisory, and orchestrated response.

We offer our Elite Threat Hunting add on for customers who want continuous threat hunting and bi-weekly meetings with a designated threat hunter. In addition, for customers who wish to elevate defenses, bolster incident readiness and accelerate cyber resilience, Secureworks Services for MDR can be added to provide easy and flexible access to a broad catalog of cybersecurity services including tabletop exercises, penetration testing and a suite of adversary exercises.

Customer Benefits

- **Achieve a 400% ROI on your Taegis MDR investment** via cost savings, risk reduction, and productivity gains¹
- **Raise the skill level of your team** through collaborative investigations and live chat with our analysts
- **Receive unlimited response for in-scope assets, and monthly threat hunting**, with option of continuous managed threat hunting as part of Elite Threat Hunting
- **Gain threat knowledge** to defend against adversaries
- **Improve your security posture** as our security experts provide regular reviews of your defenses, and easy access to comprehensive Secureworks Services for MDR
- **Combine detection and response capabilities** of Taegis XDR with [Sophos Endpoint](#) for comprehensive prevention, detection and response

Gartner

Sophos named a Leader in the [2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms](#)

Secureworks Taegis MDR

IT/OT

ENDPOINT

NETWORK

CLOUD

BUSINESS SYSTEMS

Prevent



AUTOMATIC PREVENTION

Sophos Endpoint is fully integrated and automatically included with the Taegis platform, providing a prevention-first approach that stops threats fast before they escalate, meaning fewer incidents for your team to investigate and resolve.

Detect



TAEGIS-DRIVEN DETECTION

Taegis XDR analyzes telemetry from your IT and OT environments and uses threat intelligence and advanced analytics (machine and deep learning, UEBA, statistical analyses) to detect threats.

Investigate



INVESTIGATION AND VALIDATION

Secureworks analyst investigates and validates high and critical alerts and makes recommendations within 60-minute SLA.

Respond



IMMEDIATE ACTIONS

Analyst uses Taegis to perform agreed-upon containment actions.

INCIDENT RESPONSE

Secureworks IR team responds if further efforts are required.

Applied Intelligence

Secureworks Network Effect, Incident Response Findings, Secureworks CTU™ Threat Intelligence

Proactive Threat Hunting

- Threat hunting included with MDR
- Continuous managed threat hunting via designated Secureworks expert with Elite Threat Hunting

24/7 Analyst Access

Via in-app Chat, Email, and Phone

Why is Secureworks Different Than Other MDR Providers?

Secureworks’ combination of award-winning XDR software, incident response and threat hunting experience, and more than 20 years of security-service leadership makes us uniquely positioned to help you minimize the risk and business impact of cyberattacks.

Superior Detection & Rapid Response to Fortify Resiliency



90 second access to SOC analysts



Fully transparent user interface



Bring your own EDR technology (Sophos Endpoint included)



Full Incident Response support



Flexibility to shift from MDR to XDR



Included 1 year log retention



Filters out most noise from most sources



Continuously updated detectors, integrations, & TI



Regular security reviews & maturity guidance

About Secureworks

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers’ ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.