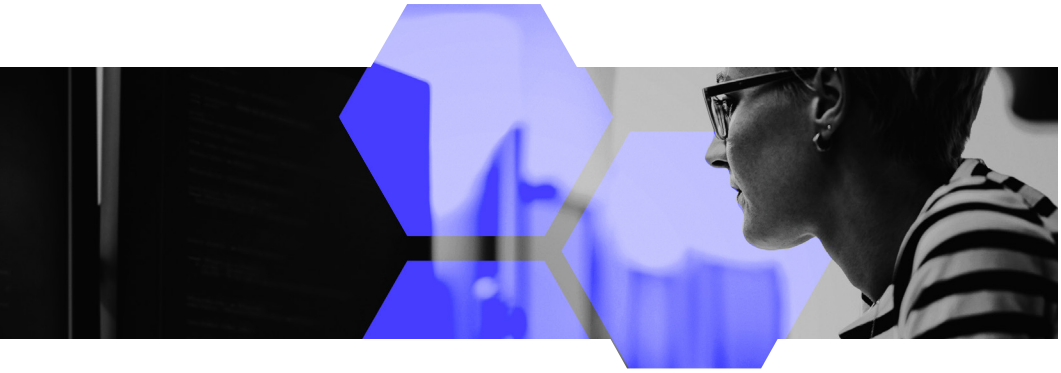
Secureworks®

Secureworks MDR for Microsoft® From Microsoft E5 to Full-service SOC

Extending Microsoft E5 Licenses to a Managed, Full-service Security Operations Center

Microsoft customers with E5 want the full security value of their licenses with the highest possible return on investment and the best security outcomes. Secureworks®, a strategic security partner of Microsoft®, complements and extends any combination of Microsoft technologies to a full-service, managed Security Operations Center (SOC) with up to 24/7/365 availability.



The Secureworks Taegis™ Platform

Secureworks Taegis is an Extended Detection and Response (XDR) platform that powers Managed Detection and Response (MDR) solutions. Taegis integrates seamlessly with Microsoft, gathering telemetry from Microsoft and other sources—including cloud environments, email systems, identity systems, and other business apps—to provide threat prevention, detection, risk mitigation, and response. In addition to its XDR technology and proven Microsoft integrations, Secureworks has more than 20 years of experience running SOCs for virtually any threat environment.

Secureworks has the broadest set of Microsoft integrations, the deepest set of services, and enhances and drives ongoing security efficiencies. Today, over 1,000 customers are using Secureworks integrations for Azure, Office 365, Active Directory, and other Microsoft connectors, and over 1.3 million Microsoft Defender endpoints rely on Secureworks every day for maximum security.

SECUREWORKS TAEGIS XDR BENEFITS

- Telemetry from E5 Azure, Defender Suite, O365, Active Directory, Microsoft Sentinel, and others
- Every customer receives one year of log retention for all telemetry
- Out-of-the box integration with Microsoft- and Azure-based tools
- Integration with mixed and multi-vendor EDR deployments
- Hundreds of vendor telemetry integrations for visibility, detection context, and accuracy
- Ongoing Customer Success operational support
- Monthly threat management advisory services from an experienced Threat Manager
- Access to Secureworks SOC experts through the Taegis interface in 90 seconds or less
- Microsoft for Defender endpoint telemetry within the Taegis platform and Incident Response teams
- Applies Patch Tuesday intelligence
- Delivers Microsoft-specific ransomware and Active Directory assessments
- Allows over one trillion guesses per second against the Windows NT hash format

The Best Security Outcomes

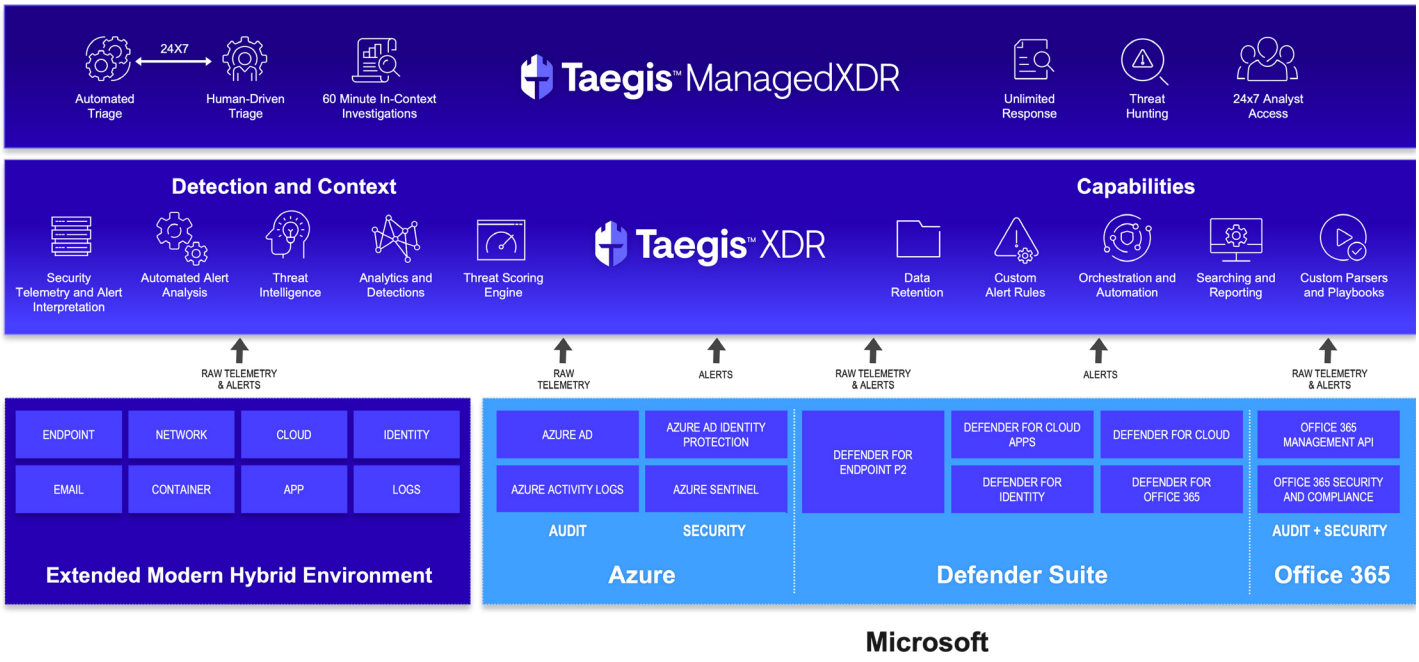
Secureworks Taegis offers fast time-to-benefit through rapid onboarding, predictable operational costs, threat detection automation, and up-to-the-minute threat intelligence, plus these additional solutions:

- Optimized security with fully integrated threat detection and response management
- SIEM-type telemetry and log functionality
- Management portal log access, with telemetry data management and export
- 365 days (continuously rolling) of unlimited telemetry data retention as standard
- Extended log retention for up to five rolling years at fixed additional costs

No matter how complex the IT environment or how many different environments are interconnected with Microsoft, Taegis provides superior security benefits and coverage from E5 licenses.

How Secureworks Taegis Works with Microsoft

Secureworks Taegis is a SaaS platform purpose-built for extended detection and response (XDR) that leverages the SOC expertise and global threat intelligence of Secureworks to deliver MDR for Microsoft and a full-service SOC. To do this, Taegis extracts the maximum security value from Microsoft Azure, Defender Suite, O365 licenses, and other Microsoft technologies, delivering maximum ROI from E5 license investments.



Secureworks Taegis ingests telemetry, event, and alert data into the Taegis XDR platform from Microsoft and many other sources.

Secureworks Taegis gathers enriched threat intelligence and crucial detection information, such as watchlists, and processes it through its advanced analytics and detection engines. It accurately classifies threats into five levels, from informational to critical, and automatically creates categorized detection alerts and responses using the thousands of countermeasures and playbooks available—with minimal false positives. Customers can tailor rules and playbooks to their environments or rely on Secureworks SOC analysts. Taegis generates full reporting and logging and provides a detailed understanding of threats and attacks across all IT and OT environments.

The goal is simple: Recognize, respond to, and mitigate threats before they become attacks that can destroy productivity and brand reputations. Using Microsoft Security data from endpoints, the cloud, and O365 applications—plus data from other systems like identity systems and other business applications—customers can do just that.

In a Secureworks analysis of telemetry from third-party cybersecurity point solutions, it was found that only 1.3% of High & Critical alerts generated by the point solutions were considered High & Critical by Taegis due to its superior detection intelligence.

This means that cybersecurity analysts using Taegis would immediately focus on the 1.3% of alerts that are truly critical instead of the 98.7% of alerts that are low-fidelity noise.

BENEFITS OF SECUREWORKS TAEGIS FOR MICROSOFT

Extend Security Defenses Across IT and OT Stacks

Threat actors exploit gaps in defenses. With Secureworks Taegis, Microsoft customers will detect and respond to anomalous behaviors wherever they occur—including Linux and macOS deployments—and use Taegis' hundreds of security integrations with other security tools and IT applications.

Optimized for Microsoft

Secureworks has a strategic security relationship with Microsoft (see Professional Services supported by Microsoft 365 Defender | Microsoft Learn), and is constantly updating its Microsoft integrations for maximum detection and response value. 60% of Taegis customers using Microsoft also use at least one other EDR (including the Taegis agent included with Taegis MDR). Secureworks also maintains integrations with other major EDR vendors so that EDR coverage is complete.

Rapid 30-Day Deployment

With thousands of customers around the globe, Secureworks offers Governance and Service Lifecycle support from our Customer Success Team and Threat Engagement Managers. Together, they ensure operational security management goals are met, and provide regular reviews, key security findings, and detailed recommendations to heighten security postures.

Track Threat Actors Tactics Over Time

Secureworks has a dedicated threat intelligence research team that monitors over 175+ threat groups. This information is captured within a proprietary threat graph that contains 40 billion unique pieces of threat intelligence. This intelligence enables Taegis to detect threats quickly, catching what cybersecurity point solutions often miss.

Integrate Azure, Defender Suite and Office 365

Taegis ingests and analyzes alerts and telemetry, including those from endpoints, cloud, identity, and Office365. Customers retain the full value of Microsoft E5 licensing.

Predictable All-Inclusive Pricing

Secureworks Taegis solutions offer all-inclusive pricing per endpoint with no hidden extras. Getting an accurate quote from a Secureworks Partner is as simple as providing the number of Microsoft E5 licenses, other EDR solutions, and the number of additional endpoint licenses needed. Unlike other solutions, Taegis does not charge extra by data volume and includes 365 days of unlimited telemetry data retention, compared to 90 days or less from Microsoft Sentinel and other MDR/XDR providers.

Reduce the Strains and Burdens on SecOps Staff

A critical advantage of Taegis is how quickly and easily it enables SecOps team to get vigilant and stay vigilant. Taegis delivers thousands of high-relevance out-of-the-box detections, plus advanced TTP and MITRE ATT&CK detections that require no additional configuration and dramatically reduce false positives, so teams do not waste time with fruitless investigations.

Transparency, Integrity and Collaboration

Taegis was designed and built for collaboration with security analysts, for security analysts. Our customers and in-house analysts engage with the same platform and the same data, leading to superior transparency. Taegis, more than any other security operations management solution available, partners its customers with leading-edge technology and global security experts who, together, will create the best security outcomes.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 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.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com