Secureworks®

Secureworks® Taegis™ NDR

Monitor Traffic Across Your Network to Rapidly Prevent, Detect and Respond to Threats

Secureworks Taegis NDR monitors network traffic entering, leaving, and within your network to reduce the risk of a breach by blocking 99%* of malicious activity identified on the network. Through up-to-date countermeasures, AI-based detectors and automated response actions, the security burden on downstream systems and staff is greatly reduced. Seamless integration with the Taegis XDR platform provides central management and more holistic visibility and protection across the complete attack surface.

Reduce Risk with Integrated Threat Prevention and Response

With the continued evolution of cloud applications and pervasiveness of remote work, threat actors can easily mask their behavior in increased network traffic. Organizations need a layered cybersecurity defense, especially those without the resources, central governance and strong policies to ensure 100% up-to-date coverage at the endpoint.

"Taegis NDR empowers us to proactively mitigate cyber risks to our business. It adds an extra layer of intelligence that fortifies our cyber defenses. When Taegis NDR sends us an alert, I know there's an issue so I can quickly assign my resources to tackle it and protect our business."

Steve Hey Senior Vice President of Information Technology, Infrastructure, and Operations, National 9/11 Memorial & Museum

CUSTOMER BENEFITS

Taegis NDR blocks 99%* of malicious activity identified on the network across both north-south (external) and east-west (internal) traffic.

Protection from the latest attack vectors with over tens-of-thousands of curated and maintained countermeasures, derived from real-world threat intelligence, block 1 million network threats each month.

Seamless integration with the Taegis XDR platform available to correlate telemetry across different threat vectors (endpoint, network telemetry, etc.) that would have not necessarily been elevated when analyzed individually.

AI engine analyzes network traffic for anomalous application and port usage, identifying potential threats before they can cause harm, such as data exfiltration or ransomware attacks.

Available automated response actions eliminate manual effort to improve response rates to emerging threats.

Eliminates the burden of device management, saving your team time and resources that can be deployed elsewhere.

Deep packet inspection (DPI) provides for more comprehensive detection of network threats.

Central visibility in the Taegis platform for reporting and unlimited chat support.

* as measured across Secureworks entire customer base

Taegis NDR performs in-line deep packet inspection of inbound and outbound network traffic using multiple integrated defense technologies to identify and block real security events requiring attention, without impacting network performance.

Secureworks rich history of tracking and preventing threat actor behavior, combined with unique insights based on the trillions of events we process, deep security research, and our adversarial testing and IR engagements, have resulted in over tens-of-thousands of curated and maintained countermeasures. Those block 1 million network threats each month for our customers, while built-in AI analyzes network traffic for anomalous application and port usage in order to identify potential threats before they can cause harm.

Taegis NDR can deploy both physically and virtually for full attack-surface coverage without impacting network flow. Countermeasures are updated daily by the Secureworks Counter Threat Unit™ to automatically protect against the latest threats, and Taegis NDR eliminates the burden of device management, including the management of rules and signatures, which saves your team time and resources that can be deployed elsewhere.

Central visibility within the Taegis platform provides reporting and unlimited direct access to our SOC through chat, and optional seamless integration with Taegis XDR correlates network activity with endpoint and cloud threats for enhanced lateral movement detection.

WHY IS SECUREWORKS TAEGIS NDR DIFFERENT?

AI-powered detections uncover advanced threats and malicious behavior

Countermeasures updated daily by the Secureworks Counter Threat Unit to automatically protect against the latest threats.

Full integration into Secureworks SOAR capabilities for remediation actions including:

- Block/Shun IP address: Block unwanted traffic from specific IP addresses or a range
- UnBlock/Trust IP address: Allow traffic from trusted IP addresses or a range
- Validate Rules: Ensure rules applied to the device are formatted properly
- Get Job Status/Health: Check the status of Taegis NDR to ensure operating as expected
- Get Devices: Fetches lists of all NDR devices to ensure compliance

Pre-built reports already available for Executive Summary and Change Management Reporting

Available integration with the Taegis XDR Platform provides more holistic visibility and enhances lateral movement detection and enables richer investigations for improved protection.

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

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.