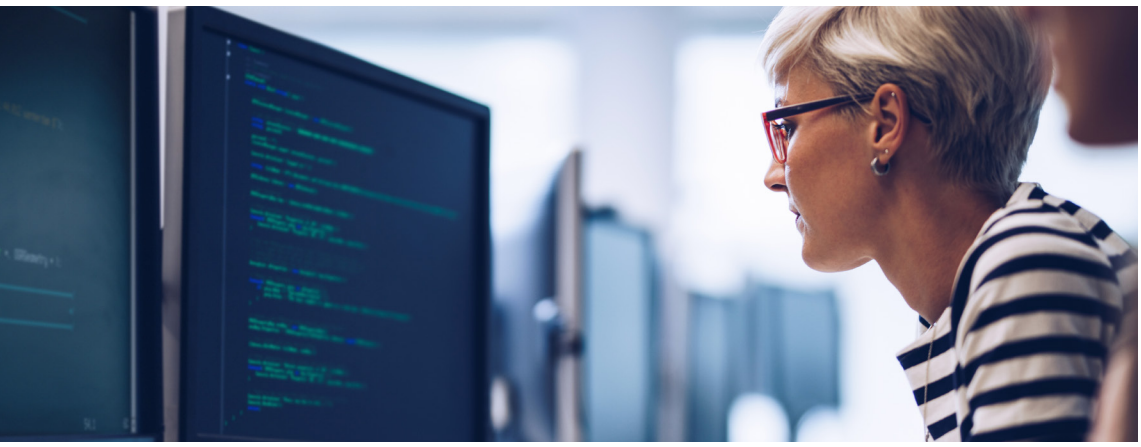
Secureworks

SOLUTION BRIEF

Taegis™ Security Operations and Analytics Platform

Outpace and Outmaneuver Adversaries



The Taegis platform incorporates the knowledge and best practices Secureworks has developed over its 22 years of running a global security-operations center, providing security services, and researching threats.

A Forrester Wave™ Leader in both Managed Security Services and Managed Detection and Response, Secureworks has been protecting businesses, non-profits, and government agencies for 22 years. As customer IT infrastructure and the threat landscape grew increasingly complex, Secureworks consultants found it harder and harder to do their jobs using the tools available on the market. So, we decided to do something about it.

We leveraged our extensive experience running a global security-operations center and first-hand knowledge of the threat landscape to create Secureworks Taegis™, the cloud-native security operations and analytics platform that our experts now use to defend customers. Taegis has been battle-tested during global cyberattacks—featuring, among others, the Sunburst backdoor, Supernova malware, Microsoft Exchange zero-day and REvil and Ryuk ransomware—and continues to help Secureworks keep 5,200 global organizations secure day in and day out.

Our original vision for Taegis spanned beyond Secureworks internal teams. We wanted customers and partners to take advantage of our

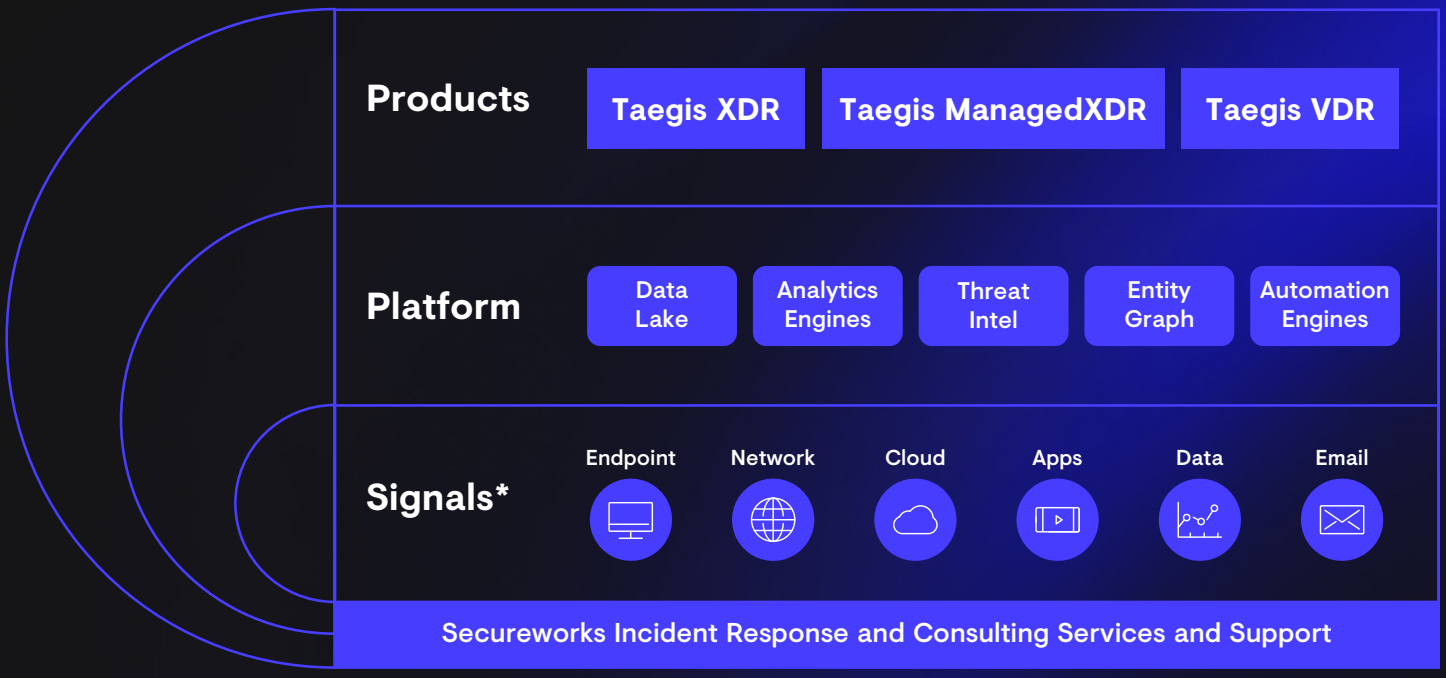
technology, threat research, and best practices to protect themselves—with our services or on their own (but always one short click away from a Secureworks expert). Today, Taegis is at the heart of security operations at organizations all over the world.

Own your attack surface

As a security leader, you have finite resources to protect a continuously expanding attack surface from progressively sophisticated threats. Maximize the effectiveness and efficiency of security operations across your organization's entire IT footprint with Secureworks Taegis. The Security Operations and Analytics Platform brings together extended detection and response (Taegis XDR or Taegis ManagedXDR), vulnerability management (Taegis VDR), and continuously curated threat intelligence.

The Culmination of Our Security Expertise

Taegis Cloud-Native Security Operations and Analytics Platform and Products



* - Signals represent telemetry and logs from your existing security tools

The Secureworks Taegis Security Operations and Analytics Platform: attack-vector coverage, components, and products.

Secureworks®

Maximize security effectiveness

Detect More Threats That Matter

Achieve comprehensive attack-surface coverage

Having a holistic view of IT infrastructure is key to security efficacy. Gain single-pane-of-glass visibility and control over your attack surface with the Taegis platform that aggregates network, cloud, endpoint and vulnerability data with curated threat intelligence and signals from your existing security tools. Detect, understand, and stop sophisticated attacks with actionable insight from the Taegis AI analytics engines continuously updated with threat indicators, countermeasures, and purpose-built analytics from the Secureworks Counter-Threat Unit™ (CTU), incident response, and adversary-simulation teams.

Give advanced threats undivided attention

An unmanageable number of alerts causing missed true positives has been at the root of multiple headline-making breaches. With comprehensive coverage of your organization's security fabric, Taegis correlates threat intelligence, vulnerability data, logs and events from different security tools to validate alerts. As a result, your analysts spend less time dealing with false positives and more time addressing real threats.

Investigate and Respond to Incidents Faster

Advanced attacks are stealthy in nature: it takes organizations an average of 280 days to identify and contain a breach*. Taegis collects data from across your environment and incorporates a comprehensive threat-hunting toolkit, including MITRE ATT&CK tactics, techniques, and procedures. Accordingly, your analysts get a holistic view of your security infrastructure and can perform all investigations within the platform, without having to manually stitch data or bounce between tools. Add Taegis response-action recommendations and automated playbooks informed by over 1,400 customer incident-response engagements per year—and your team will accelerate investigations and incident response, reducing dwell times down to hours or minutes.

Intelligently Prioritize and Manage Vulnerabilities

Take the guesswork and pain out of vulnerability management (VM). Arm your team with Taegis VDR to automate discovery and scanning of endpoints, servers, IoT devices and web applications. Rationalize and expedite VM and remediation efforts with AI-driven vulnerability prioritization (based on 47 internal and external factors, including the context of your environment and curated threat intelligence) and remediation-management capabilities.

* - 2020 Cost of a Data Breach Report, IBM / Ponemon Institute, 2020

Original threat intelligence—a crown jewel of the Taegis platform—uniquely combines research from the Secureworks Counter-Threat Unit with real-life insights from tens of thousands of consulting, incident response, and adversary-simulation engagements we have performed over 22 years. It is not just about indicators of compromise.

"We generate around 2 billion events each month. With Secureworks, we are able to crunch down that number to 20-30 high fidelity alerts — and that makes my team's job much easier."

-Sunil Saale,
Head of Cyber and Information Security,
Minter Ellison

Secureworks

Partner with Secureworks Experts

Take advantage of Secureworks Taegis ManagedXDR extended detection and response services that leverage the Taegis platform to augment and assist your security team 24x7x365. According to a Total Economic Impact™ study by Forrester Consulting, a midsize organization can expect a 413% ROI on Taegis ManagedXDR due to a reduction in costs (lower expected cost of a breach and savings on Level 1 security operations) and productivity gains for both the security operations team and business users.

Your analysts can reach a Secureworks expert in as quickly as 60 seconds directly from the Taegis console, whether your organization employs our services or not.

Increase the efficiency of security operations

Protect Your Existing Security Investments

Unlike single-vendor, closed XDR solutions that require ripping and replacing your existing security tools, Taegis is an open platform that complements your security infrastructure, ensuring comprehensive coverage and protecting your investments.

Automate!

Taegis leverages AI and automation to rid your security operations team of repetitive and error-prone manual tasks. Help your staff spend more time on high-value work with the platform's automation capabilities ranging from human-triggered automatic containment workflows to automatic correlation and grouping of events and data from multiple threat vectors.

Taegis response-action recommendations and automated playbooks are informed by over 1,400 customer incident-response engagements per year.

Eliminate the Burden of Platform Administration

As a cloud-based software-as-a-service (SaaS) platform, Taegis is maintained, updated, and upgraded by Secureworks on an ongoing basis, so your teams can focus on security operations. Plus, onboarding is fast and simple allowing you to derive security value from the platform within hours.

Efficiently Retain Data

Reliably collect, store, and access events, alerts, and logs from a variety of data sources for forensic investigations, threat hunting, log retention and reporting. Retain data at no extra cost for the first year.

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

About 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.