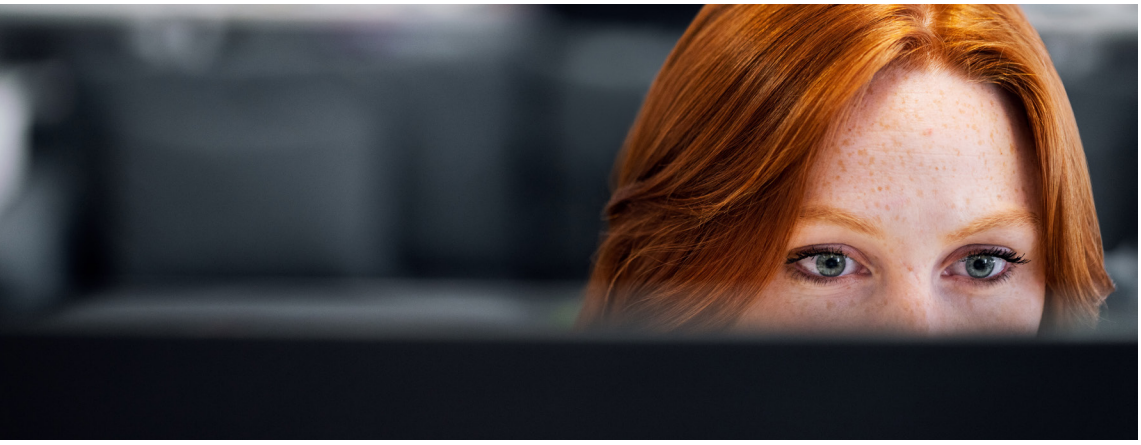
SOLUTION BRIEF

Secureworks® Taegis™ Delivers Security Analytics with Zscaler™



Security Challenges

- Limited visibility and protection against threats beyond the perimeter
- Lack of trusted Threat Intelligence and inability to monitor beyond basic IOCs
- Security team is drowning in noise and struggles to identify actionable alerts
- Security teams pivoting across too many consoles to find emerging threats

Secureworks integration with Zscaler helps you outpace and outmaneuver adversaries with precision, so you can adapt and respond to market forces and meet real-world business needs. Providing a unique combination of AI-powered insights and unrivaled Threat Intelligence with advanced correlation and analytics, you can experience better security, improved visibility, and rapid remediation, so you can get back to business.

The Challenges

With the sharp increase in remote workers connecting back to corporate networks for applications and data, the attack surface for cyber threats has expanded beyond the controlled corporate environment. In turn, detecting and responding to cyber threats has become increasingly difficult across the global business community.

Organizations are experiencing an increase in both threat volumes and complexity, leaving corporate security teams with the ongoing challenge of balancing workloads across a broader attack surface. Many organizations are burdened with manual processes, disparate or disconnected security tools and a lack of trained IT security staff. In addition, IT and security leaders are being tasked with implementing security programs that reduce risk and show value, but often lack the technology and resources to do so. Prioritizing security objectives and improving threat detection and response capabilities to reduce risk is imperative.

These trends have driven Secureworks to create cloud-native security software and technology integrations informed by our 20+ years of hands-on security operations and research experience.

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.

Better Together Secureworks and Zscaler

Zscaler Zero Trust Exchange protects users, applications and devices with a complete security stack delivered as a service, from the cloud. Together, Secureworks and Zscaler improve threat detection and response across endpoint, network, and cloud, to drive more efficient security operations and better security outcomes. With Zscaler, we collect, correlate, and analyze multiple types of security and operational data from your environment. XDR continuously combines and analyzes this data across your security tools to alert you to suspicious activity that needs attention. This reduces false positives, improves time-to-detect and respond, and provides your security analyst with the relevant user and asset context they need to protect your business.

XDR includes continuously updated Detectors, which identify and prioritize security alerts to help you find known and unknown threats. These detection use cases are built into XDR and leverage threat intelligence and advanced analytics, so your investigations are better informed. Cloud-native XDR allows Secureworks to continuously update Detectors as adversary tactics change. XDR provides prioritized alerts with the context to drive investigations that allow you to respond to threats quickly and with confidence. Our "Ask an Expert" chat feature provides real-time collaboration with an experienced Secureworks analyst, to help with an investigation or to recommend a response.

Zscaler Internet Access[1] (ZIA) provides critical telemetry components of user, IP, domain, and indicators of compromise. This, combined with a robust set of XDR data models and Detectors, provide high fidelity threat alerts and automation that makes your SOC more efficient and effective. XDR Detectors use Zscaler data to deliver enhanced detection of Punycode, Domain Generation Algorithm (DGA), and other domain-based attacks. This

[1] Taegis XDR integration currently includes the Zscaler Cloud Firewall and Zscaler Secure Web Gateway components of ZIA.

Secureworks Differentiators

20+
Years of attack & threat data

1,400
IR engagements performed in the last year

300+
Expert security analysts, researchers & responders

52,000
Database of 52k unique threat indicators managed & updated daily

[1] Taegis XDR integration currently includes the Zscaler Cloud Firewall and Zscaler Secure Web Gateway components of ZIA.

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.

Secureworks®

powerful combination also allows us to identify attack sequences not previously seen. By correlating against the MITRE ATT&CK framework we provide the information necessary for an analyst investigation to quickly move from exploitation to root cause identification.

At-A-Glance

Secureworks XDR and Zscaler deliver informed security for better business outcomes:

1. **Advanced Analytics:** Powered by machine learning, deep learning, and statistical analysis, we unify detection and response across the entire ecosystem so you can reduce risk and mitigate advanced threats.
2. **Accelerated Investigation & Response:** The Zscaler Zero Trust Exchange plus Secureworks XDR Detectors, and "Ask An Expert" chat simplify security operations so you can detect suspicious activity that often evades legacy security tools.
3. **Threat Intelligence:** Secureworks Community-Applied Intelligence, Incident Response findings, Threat Intelligence from the Secureworks CTU ™ and, third-party intelligence are combined to keep your SOC informed.
4. **Zero Trust Exchange:** Zscaler cloud-native foundation for secure digital transformation, delivering the agility, security, and experience you need to move your organization ahead.

Together, Secureworks and Zscaler strive to provide improved security, visibility, and time to remediation so you can reduce risk and more confidently run your business. For organizations without a SOC or enough skilled analysts, Secureworks can manage the solution for you with Secureworks Taegis ManagedXDR.

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.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Learn more at zscaler.com or follow us on Twitter @zscaler.

For more information, visit **secureworks.com**

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.