Secureworks®

SOLUTION BRIEF

GET NEW LEVELS OF NETWORKING DEFENSE ON THE SECURITY SERVICE EDGE WITH SECUREWORKS® AND NETSKOPE

BENEFITS

- Minimize risk from unseen threats originating at the edge
- Perform edge investigations using a single, integrated solution
- Increase security maturity of the enterprise and its environments
- Enhance compliance posture with 365-day minimum data retention

Secureworks and Netskope work together to provide a comprehensive security framework in open extended detection and response (XDR). Now, enterprises can defend key business assets and address growing threats all the way to the edge. Bring telemetry and event threat data into a single view, enabling your security team to centrally manage activity at every corner of your infrastructure, helping you to concentrate on vulnerabilities that really matter.

SECURITY SERVICE EDGE (SSE) CHALLENGES

The surge in new users, devices, applications, and data residing outside your network is significantly expanding attack surfaces and impacting analyst workloads. Most security products create silos and operational inefficiencies, forcing analysts to monitor multiple disparate consoles and spend valuable time filtering out noise and investigating false positives. Legacy security tools weren't developed with the intent to work in a cloud-first and remote-work world, so many organizations have begun seeking out a new kind of technology that will enable a more comprehensive view of their environment — one that is analyst-centric, understands the language of the cloud, and helps evaluate and prioritize security alerts.

To address growing edge computing challenges, many companies turn to Security Service Edge (SSE) technology to modernize security controls, improve user performance, and mitigate risk across internal and external IT landscapes. To enable additional context, a SSE solution can then be integrated with an intrusion detection solution. Combined with normalized event data that provides additional contextual events from your existing security products, this delivers a single, holistic view of your defensive posture.

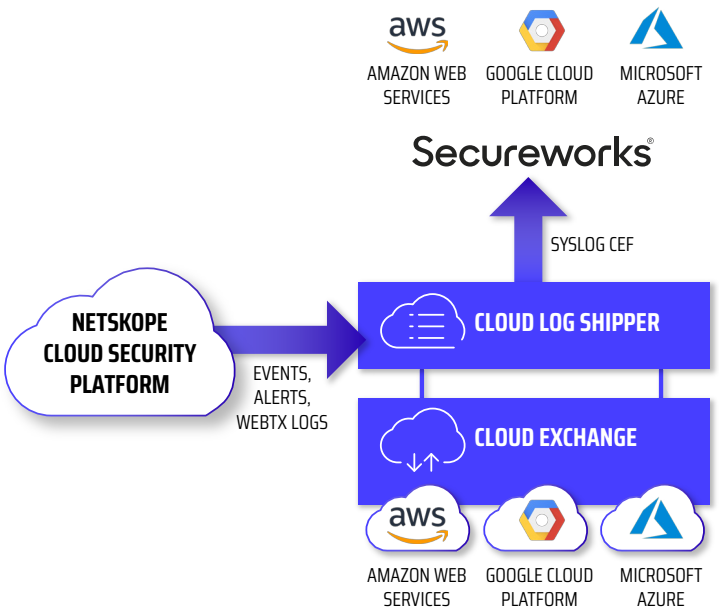
INTEGRATE SECUREWORKS AND NETSKOPE TO PROTECT DATA WHEREVER IT IS ACCESSED OR STORED

Enterprises can integrate Secureworks Taegis™, a leading cloud-native XDR solution, with their Netskope SSE products to reduce the risk of threats originating at the edge and gain the context to perform edge investigations using a single, integrated solution. As a leader in SSE solutions, Netskope offers unrivalled edge visibility and a unique approach for defending data and people across devices and applications, inside and outside the traditional company network. Secureworks Taegis XDR can ingest and normalize Netskope SSE event data with speed and agility, from any device or location. The integration extends the open XDR concept all the way to the service edge, bringing a unified, multi-layered defensive stack and practical value to security operations.

With Secureworks and Netskope solutions working together, enterprises benefit from fast, reliable networking, with complete zero trust security to support cloud services and hybrid workforces with superior threat detection, unmatched response, an open-without-compromise architecture, and a higher return on investment.

HOW IT WORKS

Netskope SSE decodes applications, cloud services, and web traffic from thousands of activity types, producing rich metadata for real-time analytics. Edge event data is then ingested through Netskope's API-driven Cloud Log Shipper to the Secureworks Taegis XDR Data Collector. Taegis XDR then maps the event data to six XDR data schema and presents it in context with other contributing XDR data sources. All other event types are normalized to the GENERIC schema, so nothing is left out — resulting in better edge visibility, streamlined investigations, and accelerated incident response.



INCOMING NETSKOPE SSE EVENTS AND SCHEMA

EDGE SECURITY EVENT TYPES	XDR DATA SCHEMA
• Audit • Compromised Credential • Connection • DLP • Malsite • Malware • Network • Policy • Remediation • User Behavior Analytics (UBA) • Watchlist	• Antivirus • Auth • HTTP • Netflow • NIDS • ThirdParty

Secureworks

Your security team gets a single, centralized view of the security posture and can manage alerts and perform investigations without manually assembling data or shifting between separate tools and platforms. When an alert is closed in one platform, it is closed in the other platform to help reduce alert fatigue, increase efficiency, and improve outcomes. Other benefits include:

- Pattern identification from a variety of hosts and destinations
- Custom alerts for specific risk profiles, tactics, and techniques
- Defense against threat actors encroaching from beyond the network
- Greater security maturity across the enterprise digital infrastructure

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

secureworks.com

WHAT IT DELIVERS

SECUREWORKS AND NETSKOPE HELP YOU DEFEND KEY BUSINESS ASSETS ACROSS THE ENTERPRISE AND ALL THE WAY TO THE SERVICE EDGE.

Real-time edge device and service threat detection: Leverage inline, real-time protections to stop malware and ransomware before it reaches users or spreads across the network.

Secure edge configuration: Prevent cloud or SaaS application misconfigurations with continuous alerts and visibility for step-by-step remediation.*

Simplified threat remediation: Alerts and restricts unauthorized data movement and exfiltration; monitors and acts on devices, users, and applications that exhibit risky behavior.

The web, cloud, and private networks and applications, data, and users are vulnerable to a range of cyber threats especially outside the protection of the enterprise network. With telemetry from the Netskope SSE platform, Taegis XDR helps you defend against advanced and cloud-enabled threats and safeguards data across any cloud, connection, application, and user.

**Secureworks Taegis alerts not yet available.*

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 Netskope

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

**Secureworks Taegis alerts not yet available.*

Secureworks®