securonix

SOLUTION BRIEF

Securonix and Zscaler

Better Visibility for Enhanced Threat Detection

Secure Your Modern Enterprise

With more enterprises embracing cloud and remote work, detecting malicious activity also needs to evolve. Your employees need easy access to sensitive organizational data to do their job remotely. But, remote work should not impede your security team from detecting threats and abnormal user behavior. Now, you can maintain zero trust while using a Next-Gen SIEM to alert you to advanced threats. That's why Securonix is partnering with Zscaler to help extend visibility across the environment for threat detection and response with minimal noise.

Securonix + Zscaler Joint Solution

Securonix and Zscaler's integration enhances your security posture with advanced analytics within a zero-trust architecture. Zscaler Cloud Nanolog Streaming Service (NSS) gives Securonix Next-Gen SIEM direct cloud-to-cloud log integration streaming for detection and response to advanced threats. This integration makes it easier for Securonix Next-Gen SIEM to alert your security team to possible cyber threats without the hassle of standing up and maintaining on-premises NSS infrastructure to relay activity.

Detect and Respond to Threats Faster with Securonix and Zscaler

Reduce Risk

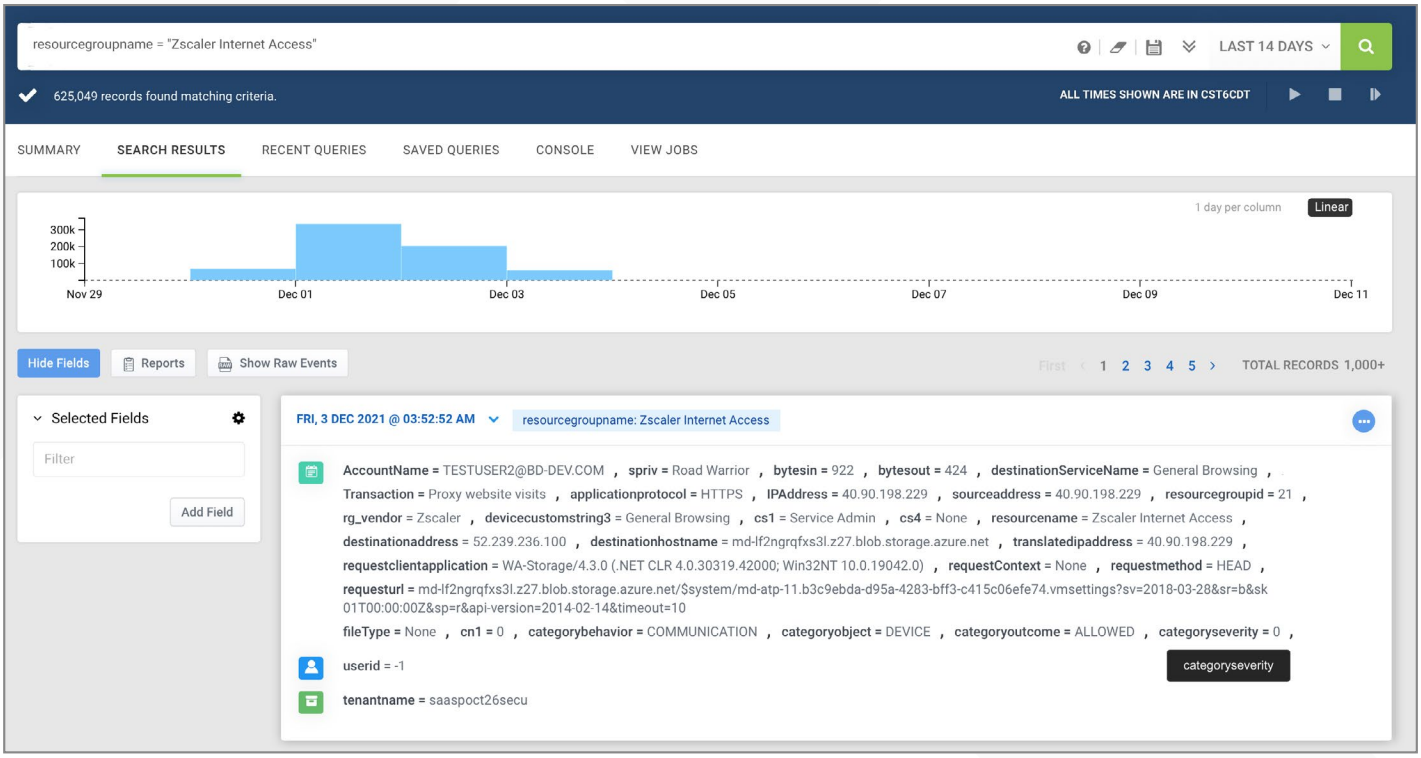
Get the same level of fast threat detection and response, everywhere. Our joint solution leverages Securonix advanced analytics to give you real-time insights for threat detection and prioritization on a single platform across all devices, users, and locations.

Fast and Reliable Integration

Cloud-to-cloud log streaming provides high-resolution telemetry directly into Securonix over a reliable and secure HTTPS channel, with no infrastructure to maintain.

Lower Costs, Higher ROI

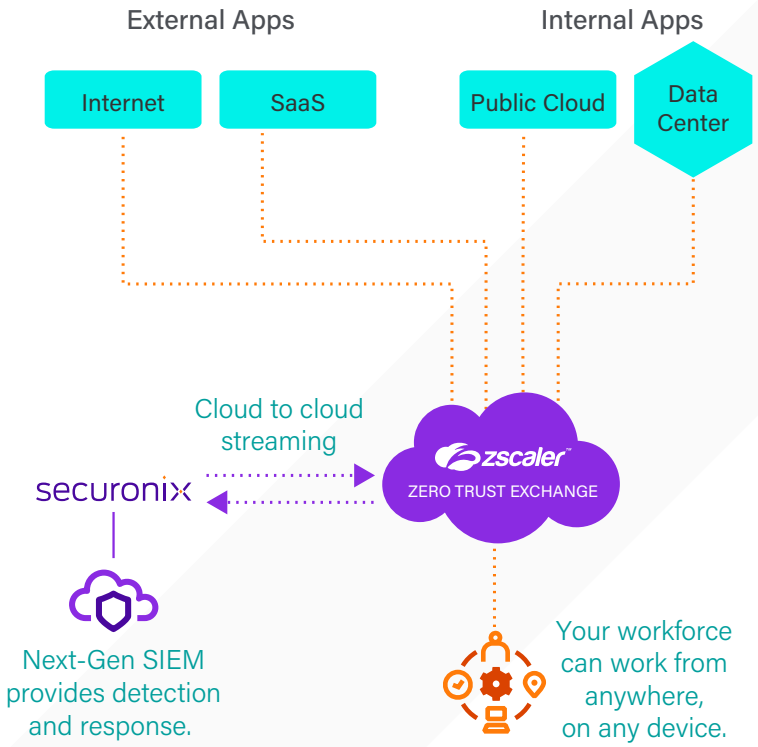
Eliminate appliances and reduce costs. Rather than deploying, managing, and monitoring an on-premises NSS virtual machine, you can easily configure an HTTPS API feed that will push logs from the Zscaler cloud service directly into your SIEM.



How it Works

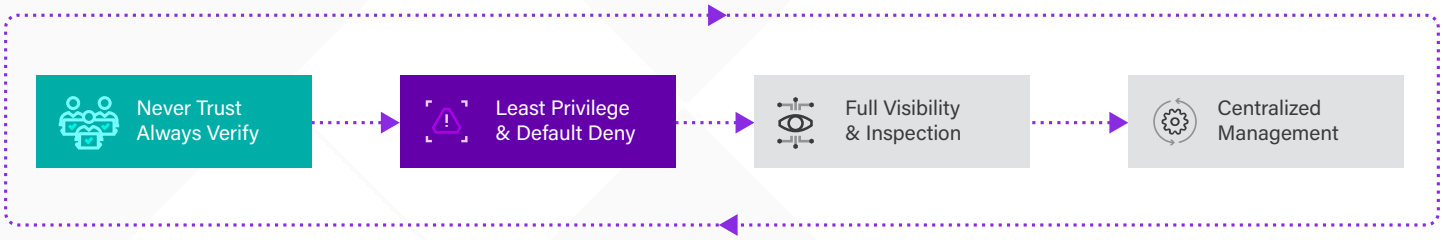
Zscaler's Cloud NSS allows direct cloud-to-cloud log streaming for all types of logs into the Securonix platform. Cloud NSS consolidates logs from Zscaler activity for all users, globally, and pushes them into a central repository, where administrators can view and mine transaction data by user, device, application and location in real time. Features of this joint solution include the ability to:

- Transmit comprehensive logs from all users and across all devices and locations, to the Securonix SIEM in real time.
- Customize and configure your filters to send only relevant logs (on criteria such as user, data type, etc.) to the Securonix SIEM.
- Convert logs easily to the correct format without manual effort through a seamless integration with Securonix.



Adopt a Zero Trust Framework

Securonix advanced analytics leverages Zscaler's data to give you better insight into your users within a zero trust framework. Securonix provides Zscaler customers with advanced analytics, machine learning algorithms, and user risk scoring to help you understand how users are interacting with your organization's sensitive data.



Our analytics allows you to identify abnormal behaviors that deviate from baselines by stitching together disparate events into a single thread. We help you work towards achieving zero trust security by correlating all the data, performing threat detection, and automating incident response.

Cover Top Security Monitoring Use Cases

Securonix has over 120 out-of-the-box use cases to monitor Zscaler events for cyber threats. This includes monitoring for:

- Authentication anomalies
- Malicious inbound and outbound connections
- Suspicious application access
- Data exfiltration attempts
- Web traffic anomalies
- Phishing attempts

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. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.
Learn more at zscaler.com or follow us on Twitter @zscaler.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com