securonix + snowflake®

zscaler™

SOLUTION BRIEF

Zscaler Security Analytics with Securonix Powered by Snowflake

Achieve Complete Visibility, Behavior Analytics and Real-Time Reports for Your Zscaler Log Data

Secure Your Modern Enterprise

Zscaler provides easy access to sensitive organizational data to your employees so they can do their job remotely. But remote work should not impede your security team from detecting threats and abnormal user behavior.

With more enterprises embracing cloud and remote work, keeping data from all employee activity on the web requires ingesting and storing large amounts of data. But it is not only about keeping data. Behavior analytics across Zscaler and other data sets enable effective threat detection for the distributed workforce.

Now, you can leverage ZScaler to implement Zero Trust while using Securonix NextGen SIEM to alert you to compromised users and advanced threats. Powered by Snowflake's innovative architecture, there is no need to filter or drop Zscaler logs. Snowflake Data Cloud provides the capacity, performance, and cost-effectiveness that allows you to collect all logs from ZScaler without compromise, expanding your detection visibility and empowering your investigations, threat hunters and executive reports.

Securonix + Snowflake for your Zscaler

Securonix and ZScaler's integration enhances your security posture with advanced analytics within a zero-trust architecture. Zscaler 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 your security team to detect and react to cyber threats using the full set of ZIA logs, without the hassle of standing up and maintaining on-premise NSS infrastructure to relay activity. Triage and incident response leverages Snowflake as the security data lake for quickly investigating issues at massive scale. Insights from Securonix and custom analytics can be reported with Snowflake or and the existing business intelligence (BI) tooling for actionable self-service dashboards across the enterprise.

Detect and Respond to Threats Faster with Securonix Powered by Snowflake

Reduce Risk

Leverage purpose-built threat detection and response for Zscaler deployments. Leverage Securonix advanced analytics to gain real-time risk insights and alert prioritization powered by your existing Snowflake environment.

Fast and Reliable Integration

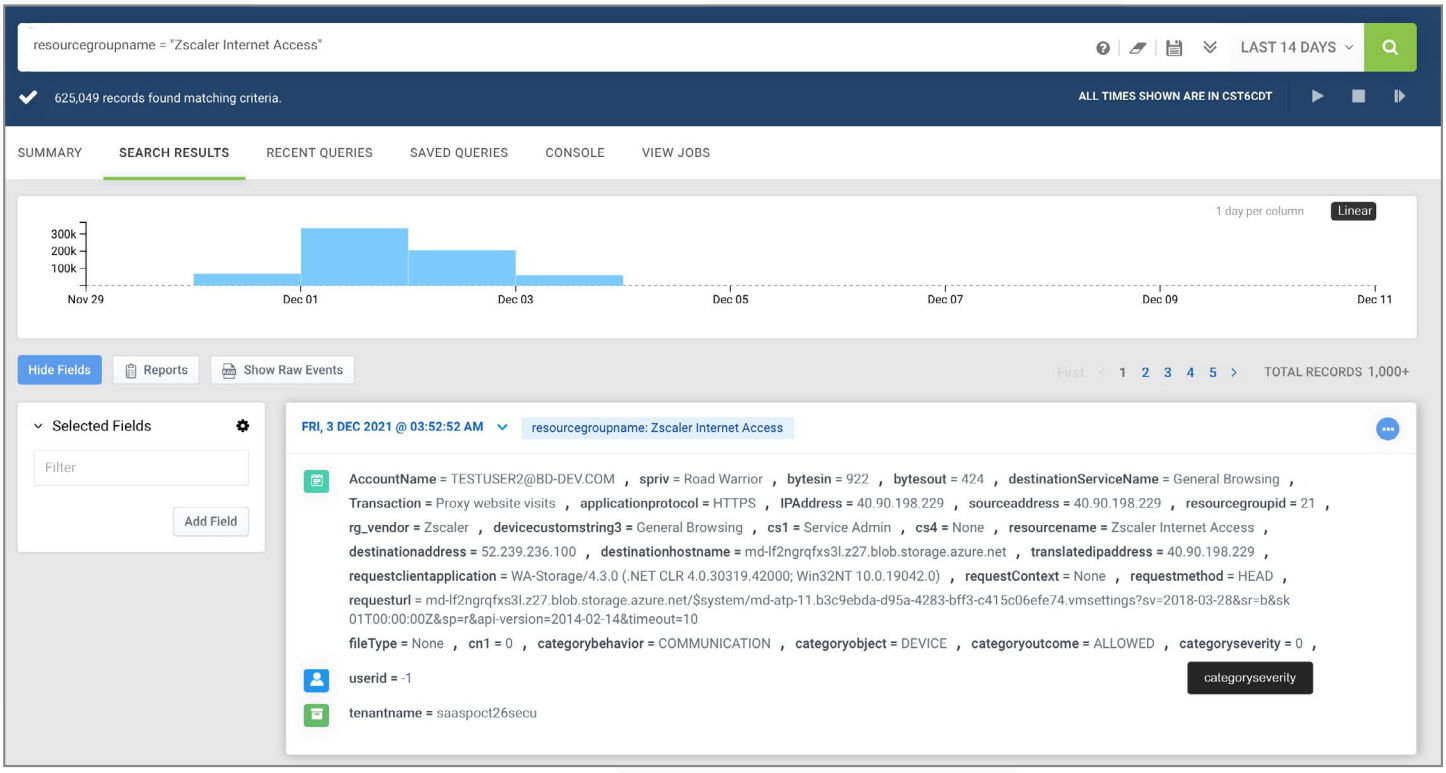
Cloud-to-cloud log streaming provides high-resolution telemetry directly through Securonix to your Snowflake Data Cloud. All communication takes place over a reliable and secure HTTPS channel, with no infrastructure to maintain.

Lower Your Zscaler Monitoring Costs

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

No Need to Filter Web Activity Logs

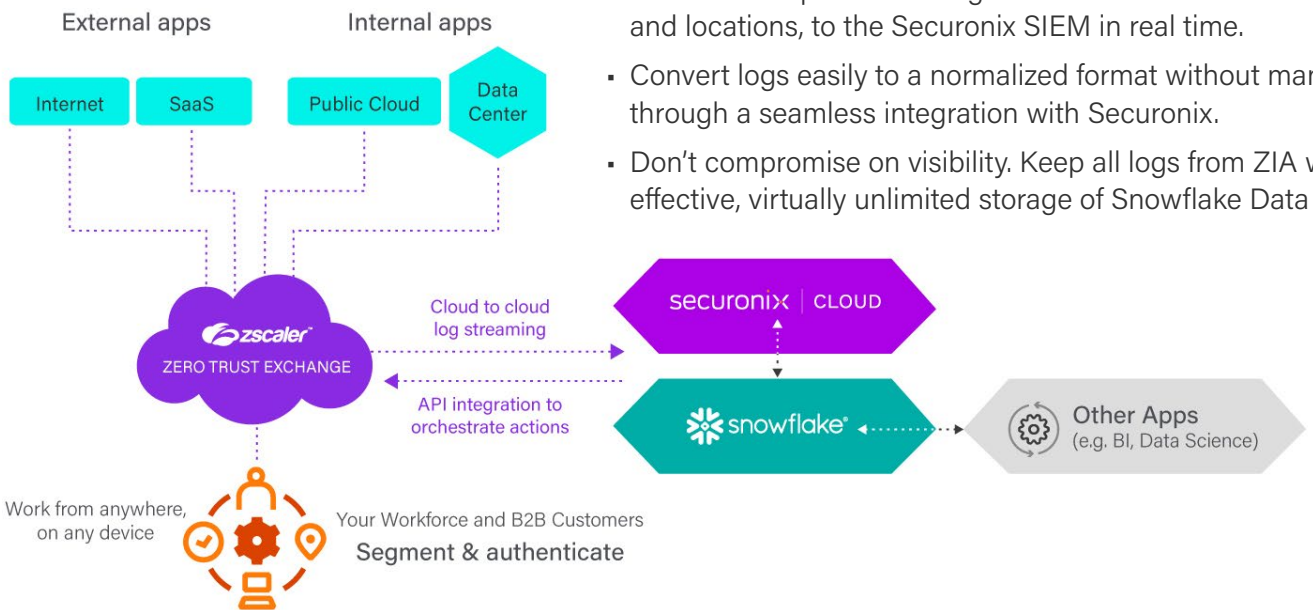
The Snowflake Data Cloud allows you to cost-effectively collect and retain all ZIA logs without daily ingest or retention limitations. No need to identify what is needed in advance, hampering threat hunting and investigation requirements. Collect all and retain for as long as you need.



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 composed of Securonix and Snowflake cloud-native solutions, where analysts can view and mine transaction data by user, device, application and location in real-time and across a year or more. 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.
- Convert logs easily to a normalized format without manual effort through a seamless integration with Securonix.
- Don't compromise on visibility. Keep all logs from ZIA with the cost-effective, virtually unlimited storage of Snowflake Data Cloud.

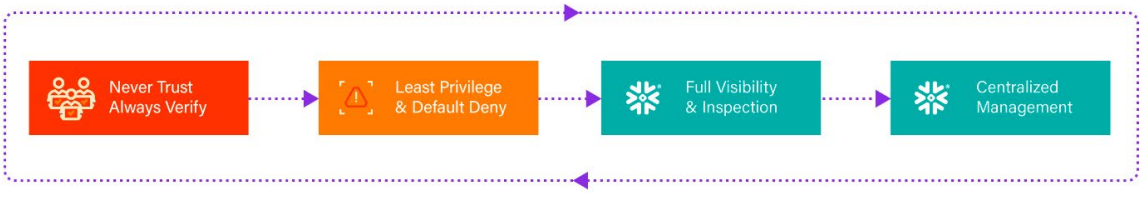


Adopt a Zero Trust Framework

Securonix advanced analytics leverages Zscaler's data to provide better insight into users within a Zero Trust Framework. Securonix provides Zscaler customers with advanced analytics, machine learning algorithms, and user risk scoring to help the organization understand how users are interacting with its sensitive data.

Our analytics allows organizations to identify abnormal behaviors that deviate from baselines by stitching together disparate events into a single thread. Securonix and Snowflake help organizations adopting ZScaler to implement zero trust security by correlating all the data, performing threat detection, and automating incident response.

The open nature of Snowflake's Data Cloud allows organizations to leverage the collection and storage of zScaler data via Securonix for other use cases. All data collected is always available to query in a number of standard analytics languages like SQL and Python.



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

For more information about ZScaler security analytics with Securonix powered by Snowflake, schedule a demo at: www. securonix.com/request-a-demo

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

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.