Enrich Your SOC, Achieve Compliance and Optimize Cost with Zscaler Logging Plane

SOLUTION BRIEF

Enrich Your SOC, Achieve Compliance and Optimize Cost with Zscaler Logging Plane

Reduce MTTR for security threats and IT issues; Improve control over data residency; Integrate Zscaler Logging Plane with Your SIEM

The Challenge: A Perfect Storm of Risk and Complexity

In the age of AI, business continuity and cyber compliance are vital. Traditional, fragmented log management across firewalls, VPNs, and proxies was costly and lacked visibility, diverting IT resources from data analysis and hindering fast Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR). This inefficiency negatively impacted productivity, compliance, and revenue.

Organizations now require an intrinsically resilient platform that enables security operations, mitigates threats, simplifies compliance, and provides real-time and retrospective visibility into traffic and application logs for rapid IT issue resolution.

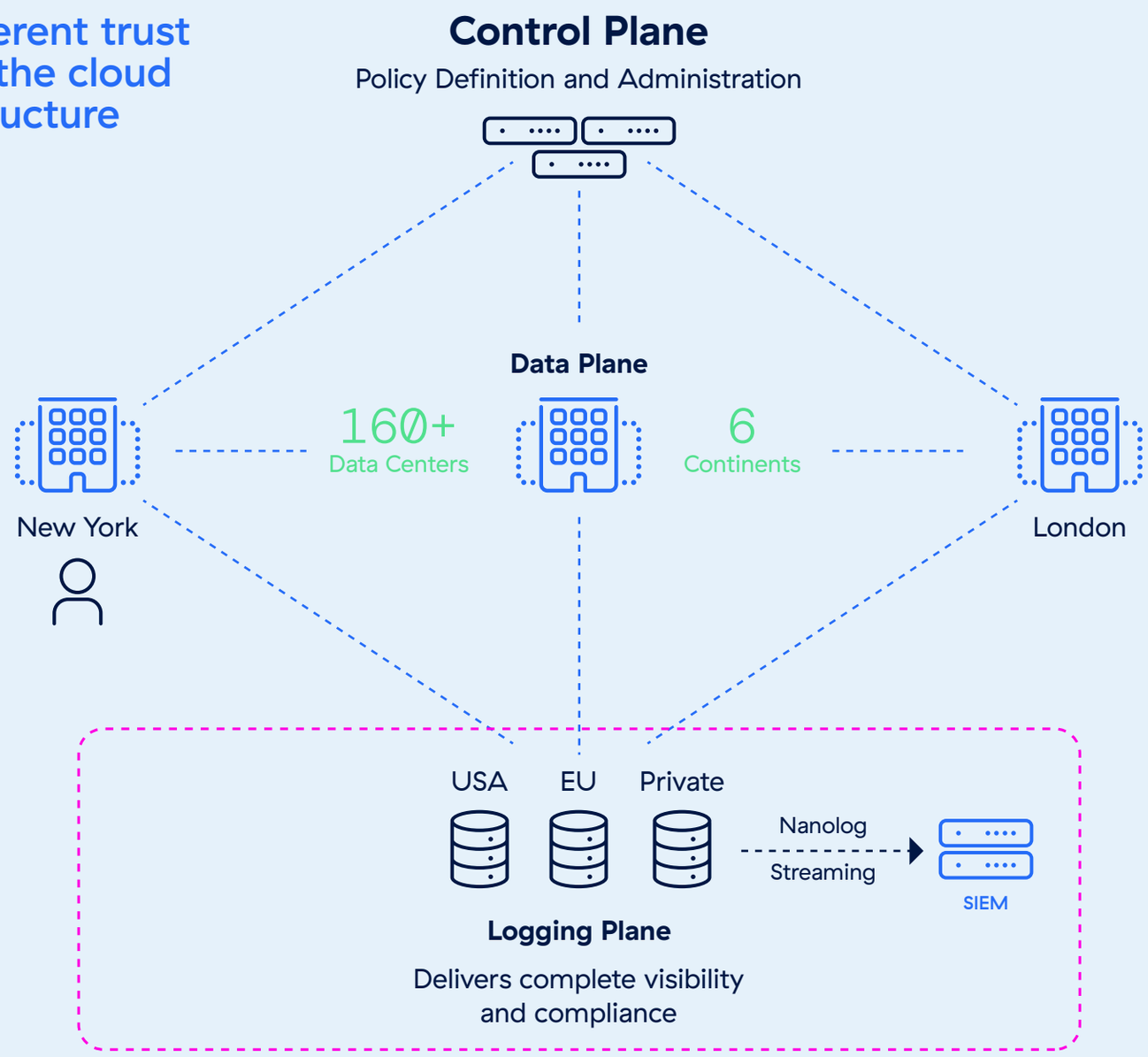
Zscaler Logging Plane: Overview

Zero Trust Exchange Platform by Zscaler, is industry's largest inline and cloud-native cybersecurity platform. Its modular architecture has a control plane, a data plane and a logging plane running separately from each other.

Delivers unprecedented data security and privacy

- Logs only written to disk in a customer selected GEO
- Indexed and compressed logging
- Logs consolidated and correlated in real-time.
- Differential logging: hard to decipher

No inherent trust within the cloud infrastructure



The separation of the logging plane is the key to providing a single, complete and context-rich source of truth for all user, application and device activity, transforming logging from a costly operational burden into a strategic asset for visibility, compliance and cost control.

As policies are managed in the control plane, traffic is inspected and policies are enforced in the data plane, detailed logs are generated, enriched and stored in the logging plane. This cloud-native or on-prem logging service is purpose-built to capture, correlate and store trillions of logs per day without ever impacting user experience or security performance. The stored logs are normalized and enriched for query, use, and display within the platform UI. These logs can also be streamed using Streaming Service (Nanolog Streaming Service / Log Streaming Service) to either a cloud-native SIEM or an on-prem SIEM.

Key Benefits

While infrastructure uptime is critical, a true organizational resilience requires deep visibility for security operations (SecOps), IT support, and compliance teams. Without comprehensive, easily accessible logs, threat hunting is impossible, troubleshooting is slow, and audit-readiness and compliance is a constant struggle. Zscaler addresses this with a powerful, flexible logging and SIEM integration ecosystem that provides the following key benefits.

Faster Investigation and Resolution of treats and Network Issues

Every Zscaler log entry is enriched with a wealth of information, eliminating the need for manual correlation. Instantly see the Who (user, department), What (application, URL, threat), Where (location, device), and Security Verdict (policy, action, sandbox result etc) in a single entry. With all the context you need at your fingertips, your SOC analysts and IT operations teams can investigate alerts, and hunt for threat, or IT issues faster than ever before, reducing MTTD and MTTR for threats and IT issues.

Full Control Over Data Residency

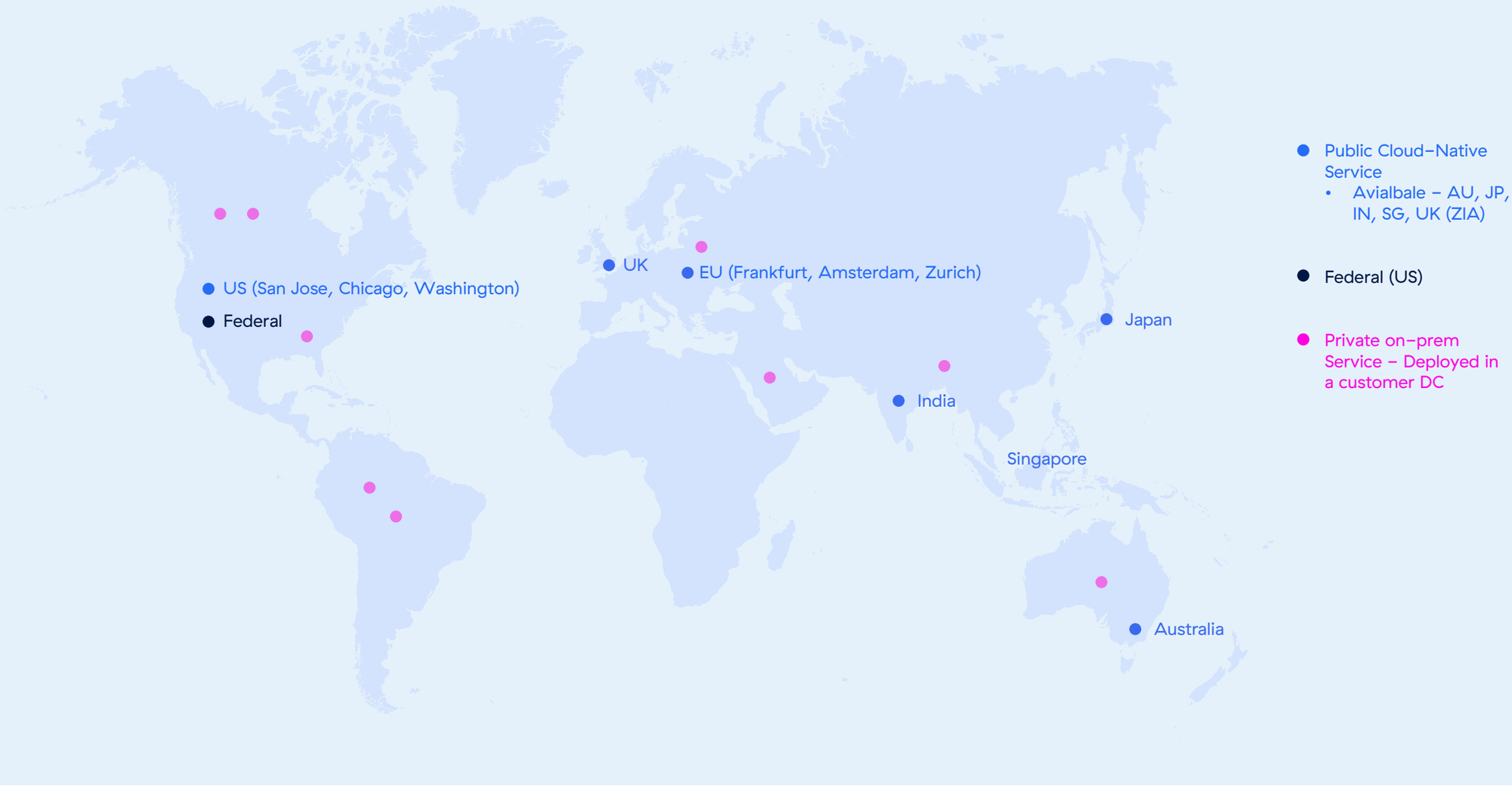
To meet the rising global demand for data locality and residency requirements, which is driven by national laws and institutional regulations, Zscaler offers flexible logging options. Customers can choose to have logs stored within a specific set of countries, or they can opt for a private logging plane infrastructure to keep logs within their own data centers (DCs).

- Public Cloud-Native Service: Available in specific locations (United States, UK for ZIA only, EU, Australia, Japan, India, and Singapore) and offers customers with control over data flow and residency.

- Private on-prem Service: Offered to all ZIA customers, this option is deployed in the customer's data center, providing geofencing control and ensuring adherence to local privacy requirements.

- Federal: Only for the US government, this options ensure meeting federal goverment standards and geofencing controls.

Logging Plane Residency



Meet retention goals for compliance and audit reporting

Log retention periods are often insufficient for meeting regulatory requirements or conducting effective post-breach forensic analysis. Storing years of detailed logs in a high-performance SIEM is often cost-prohibitive.

Zscaler solves this with extended log retention that currently allows organizations to store their traffic logs for up to 1 year (for ZIA) in cloud or can be longer if you choose to store on-premises, and up to 6 months (for ZPA) in cloud. This helps with achieving audit readiness, enable long term threat hunting, and accelerate incident response as you now have immediate access to a complete and detailed record of all user, application, and device activity in a single place.

Accelerate your migration to cloud

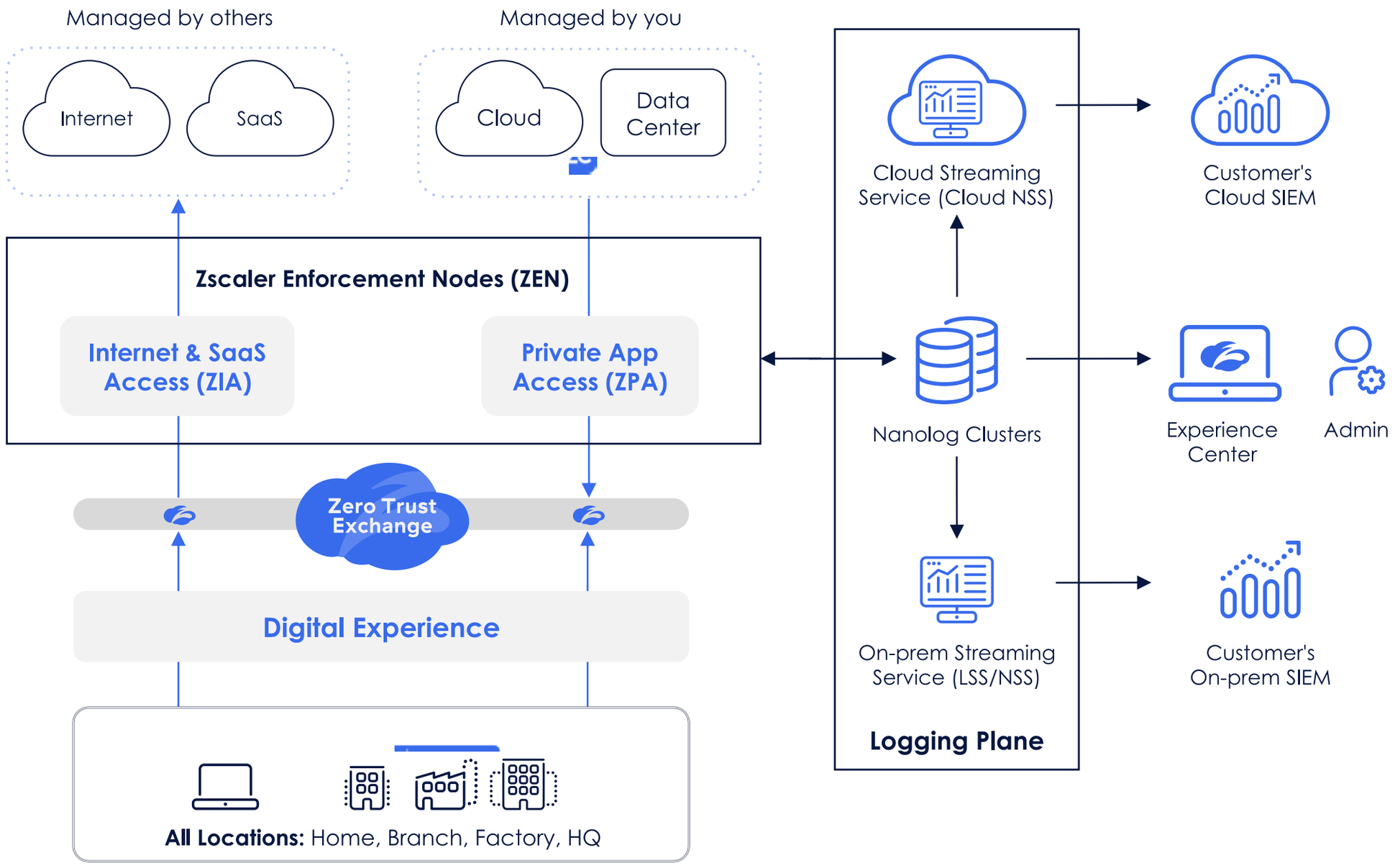
SOC teams gain enhanced visibility and context for quicker, more effective threat identification and triage by streaming log data to a SIEM. The Cloud Nanolog Streaming Service facilitates streaming logs directly to your cloud-native SIEM, eliminating the need for on-premises log data storage. The Zero Trust Exchange's cloud-native logging plane manages the high-scale collection, aggregation, routing, load balancing, and compression of this data. This architecture removes the necessity for on-premises infrastructure like syslog collectors and load balancers, significantly lowering management overhead and accelerating the transition to a fully cloud-native solution.

Dramatically Reduce SIEM storage Costs

The Zscaler Zero Trust Exchange Platform provides an effective strategy for optimizing costs associated with logging data. Instead of overpaying for ingesting vast amounts of logging data into a cloud SIEM, customers can leverage Zscaler's cloud storage for logs at a significantly lower price. Using flexible formatting options with the Streaming Service, customers can send only critical events/fields to their SIEM, thereby reducing SIEM ingestion volumes and costs.

Logging Plane Components

Zscaler's logging plane has the following major components that communicate over an encrypted TLS tunne



Logging Plane Components	Function in Logging Plane	Use Case
Nanolog Clusters	Nanolog clusters ingest and store logs and provide metrics, reports and dashboards. Each cluster is configured in high availability (HA) mode consisting of one primary node server and two secondary nodes. Additional nanolog clusters can be added to a tenant to meet any scalability requirements.	Enables high resilience in case the primary node server goes down. Storage and log retention of all of ZIA, Data Protection, Branch Connector, Cloud Connector, ZCC flow logs, Admin audit logs and a subset of ZPA logs.
Logging Zone	Logging Zone ingests and stores logs, provides metrics, reports and analytics for ZPA. All of the ZPA logs are currently stored in the Logging Zone for a period of 14 days. A copy of the subset of these logs are stored in nanolog clusters for up to 6 months.	Storage and Full log retention for ZPA for 14 days.

Logging Plane Components	Function in Logging Plane	Use Case
Cloud Nanolog Streaming Service	A Zscaler-managed service that streams logs directly to a public cloud storage like AWS S3 or a cloud SIEM.	Serverless integration with cloud-native SIEMs like Microsoft Sentinel and Crowdstrike etc. Zero infrastructure to manage.
Streaming Service (Log Streaming / Nanolog Streaming Service)	A virtual appliance deployed in your environment that receives a real-time stream of logs and forwards them to your SIEMs. Log Streaming Service (LSS) streams ZPA logs, while Nanolog streaming service (NSS) streams logs from ZIA, data protection, admin audit logs etc.	Integration with on-prem or IaaS-based SIEMs (like Splunk, QRadar etc). Full control over data privacy and residency.
Experience Center	Unified platform user interface with interactive and customizable dashboard views that provide a single management experience for analyzing data and transaction details across the Zscaler cloud.	Perform quick analysis, ad-hoc queries, drill-downs, view customizable dashboards, and run custom or pre-built reports to understand your data without leaving the Zscaler console.

How it works

The architecture can be broken down in three distinct stages: Capture, Centralize and Correlate, and Deliver.

1. **Capture: Inline and Out of band processing**

- This is at the edge or out of band, where your traffic and assets are inspected or processed.
- Log to RAM results in higher performance: When Zscaler processes traffic or digital assets, it enforces the policy and simultaneously generates a log entry that is written to a system memory (RAM) and not the disk. This is order of magnitude faster and has zero impact on performance in the data plane and the ongoing user traffic.
- Tokenization and Compression: The log isn't written as a long text string. It's created in a highly optimized, tokenized binary format. For example, instead of writing "User: johndoe@xyz.com, Deptt: sales," it uses small numerical tokens that represent the value. Compression helps improve the performance of transmission and reduce the cost of storage while tokenization reduces the risk of exposing sensitive data to insiders and IT support teams.

2. Centralize & Correlate: The Nanolog Clusters

The compressed logs from all 160+ Zscaler data centers are streamed to a central, globally distributed system we call Nanologs.

- Purpose-Built Database improves speed: This is not an off-the-shelf system. It's a proprietary, big-data platform designed specifically for this task and built for massive write-ingestion rates and fast querying.

- Decompression & Correlation: The Nanolog clusters receive the compressed and tokenized streams, decompress them, and then store the data in a partitioned way to improve performance, manageability performance and manageability.

- Experience Center: The Zscaler portal you use for analytics and reporting is itself a "customer" of the logging plane. When you run a report or view logs in the UI, you are directly querying the logging plane. The Logging Plane decompresses, detokenizes, enriches the log with all the context: user identity, location, threat intelligence, policy action, etc., and displays in the form of dashboards and reports in Experience Center. Global Single Pane of Glass: This process is what allows you, from your Experience Center, to see the logs, all in one place and within seconds.

3. Deliver: Streaming Service (NSS / LSS) & Experience Center

Once the data is in the Nanologs, it needs to be made available and actionable.

- Nanolog Streaming Service (NSS) and Log Streaming Service (LSS): This is the primary mechanism for customers to get logs into their own systems (SIEMs). As we discussed, NSS VMs or Cloud NSS establish a persistent connection with Nanolog clusters (LSS connects with Logging Zone), correlate the data it receives from nanolog clusters or Logging Zones into a single, cohesive log for each transaction. It then streams logs in real-time and as required by a customer in a specific format that is compatible with the customer SIEM. This enriches a customer's SOC with a lot more context and helps them identify and triage threats faster. During this process, no data is stored on NSS/LSS services, and is temporarily kept in its RAM for faster and a secure transmission to a customer SIEM. For further details about our integration with on-prem and cloud-native SIEMs, see our next section.

Integration of Zscaler logs with both on-prem and cloud SIEMs

NSS breaks down data silos by feeding a single source of truth into your existing SIEMs, whether they are on-premises or in the cloud. Zscaler's logging plane integrates with both cloud-native SIEMs as well as on-prem SIEMs, providing high fidelity and contextual data to transform raw logs into actionable security intelligence.

The heart of the integration is the Streaming Service (NSS/LSS). This is not a simple syslog forwarder, but is a patented, purpose-built service designed for the scale of the Zscaler cloud. It provides near real-time, highly compressed and tokenized transaction data from the Zscaler Nanologs to the customer's SIEM, over a reliable TCP or HTTPS connection. NSS and Cloud NSS have built-in resiliency to ensure there is no data loss in case the connection cannot be established between the SIEM or with Nanolog clusters. The data is provided in various industry-standard formats (CEF, LEEF, JSON) and can also be customized, ensuring plug-and-play compatibility with any SIEM.

- On-Premises SIEM Integration: For organizations with established investments in platforms like Splunk Enterprise, Microsoft Sentinel, Exabeam, etc., Zscaler uses a lightweight virtual machine (VM) to stream logs via a TCP connection. This provides real-time data for your Security Operations Center (SOC) without requiring complex agents or log forwarders. You can customize the output format to match your SIEM's specific ingestion requirements, accelerating time-to-value. Take a look here for a complete list of integrations with on-prem SIEMs.

- Cloud-Native SIEM Integration: As organizations embrace cloud-native SIEMs like Microsoft Sentinel, Splunk Cloud, Google SecOps, Crowdstrike, etc., Zscaler's Cloud NSS sends data to SIEMs HTTPS endpoint using direct API integrations to offer a frictionless, cloud-to-cloud solution. You can customize the output format to match your SIEM's specific ingestion requirements, accelerating time-to-value and your migration to cloud. Take a look here for a complete list of integrations with cloud-native SIEMs.

- Why Zscaler? The Foundation for a Resilient Enterprise

- Zscaler provides the critical trifecta of modern security: an architecture that eliminates downtime, deep visibility that empowers your security and IT teams, and a simplified approach to achieving and proving compliance. By leveraging the Zscaler Zero Trust Exchange with its integrated NSS and extended log retention capabilities, you build a more resilient, efficient, and secure enterprise.

- To learn more about how Zscaler can enhance your organization's resiliency and compliance posture, visit www.zscaler.com or contact your Zscaler representative today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.