splunk> turn data into doing™ SOLUTION GUIDE

# Zscaler and Splunk for Security

Identifying and Stopping Threats in a Zero Trust Architecture

Every second counts when dealing with a potential threat, but a deluge of events can easily overwhelm security teams. While logs and events are key elements in detecting and preventing an attack, identifying high-fidelity threats should always be a top priority. Security teams can then hone in on active threats and adversaries, instead of getting lost in a sea of noise. Bottom line? Time spent sifting through countless operating logs takes away from time spent protecting the enterprise.

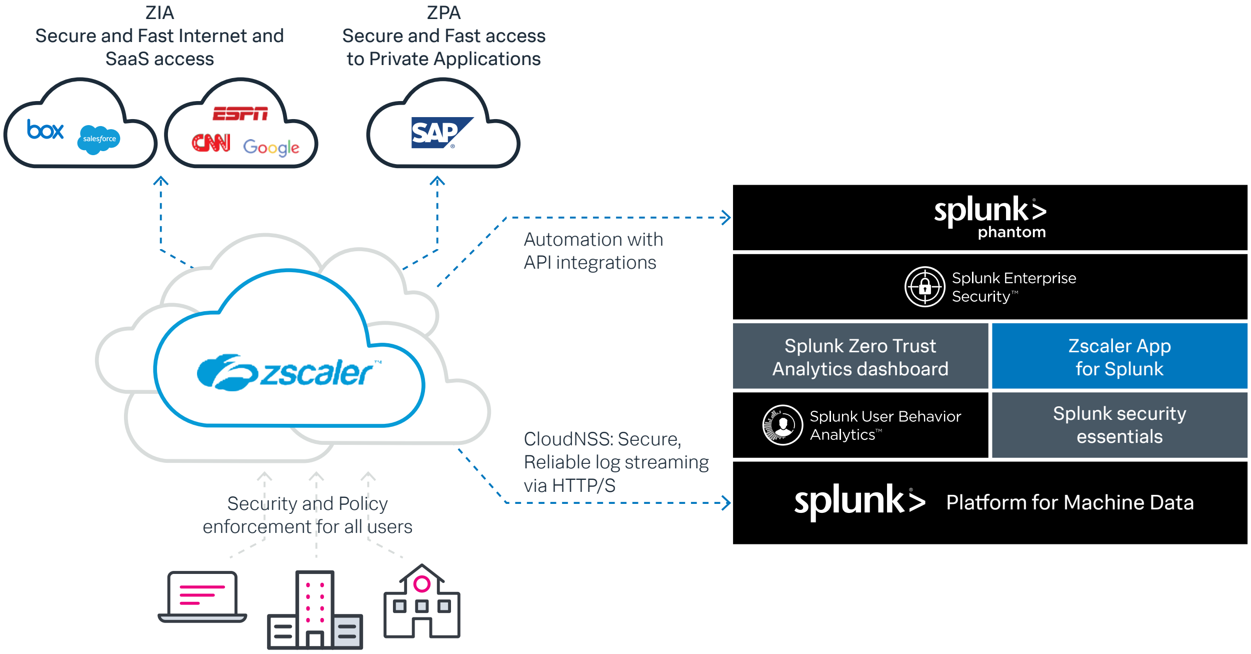
Fortunately, we come bearing good news: Zscaler and Splunk have joined forces to deliver a security and analytics service straight from the cloud. This integrated solution allows security teams to focus on keeping the enterprise secure, while freeing up resources that were previously tied to maintaining infrastructure.

## Best-of-breed cloud security delivers superior cloud-native zero trust

Business initiatives like digital transformation and cloud migration will inevitably increase risk. Traditional security architectures built to keep proprietary data safe are becoming less effective as applications and data move to the cloud. Now, traditional controls are bypassed due to the very nature of remote work — where employees can access precious company resources from literally anywhere. Thankfully, secure access service edge (SASE) with zero trust can help companies address the many challenges that come with this type of change and the collective acceleration to the cloud.

So, what is zero trust exactly? In essence, zero trust assumes that any network or user is hostile until proven otherwise. Access isn't simply given and authorization isn't just assumed — verification has to take place at every access point. This requires the right architecture, analytics, dynamic policy and risk visibility to reduce the attack surface, prevent lateral movement and make real-time threat determinations with each transaction.

Splunk and Zscaler have partnered to deliver this superior approach to security. Our tightly integrated, best-of-breed cloud security and security analytics platforms deliver a cloud experience for the modern, cloud-first enterprise.



ZIA
Secure and Fast Internet and SaaS access
box
salesforce
ESPN
CNN
Google
ZPA
Secure and Fast access to Private Applications
SAP
zscaler
Automation with API integrations
CloudNSS: Secure, Reliable log streaming via HTTP/S
Security and Policy enforcement for all users
splunk> phantom
Splunk Enterprise Security
Splunk Zero Trust Analytics dashboard
Zscaler App for Splunk
Splunk User Behavior Analytics
Splunk security essentials
splunk> Platform for Machine Data

Zscaler securely connects all users — no matter where they're working from — to the internet and private applications. In addition, Zscaler's rich authentication and policy-based controls strengthen an organization's security posture and overall operations. Splunk ingests Zscaler's high fidelity telemetry, giving security teams visibility into their zero trust environment, while enabling them to detect and eliminate emerging threats across the enterprise.

## Zscaler and Splunk securely connect users, apps and entities

Zscaler Internet Access (ZIA) provides a secure connection for all users, regardless of where they are or what device they're using. Users are authenticated and only have access to websites and software as a service (SaaS) applications in accordance with corporate policy. Zscaler's cloud and proxy architecture allows for full secure sockets layer (SSL) inspections to prevent malicious content — at scale — from coming into the enterprise or sensitive data leaking out. ZIA provides a complete security stack, including cloud access security broker (CASB), data loss prevention (DLP) and a sandbox to better stop threats and mitigate risk.

Zscaler Private Access (ZPA) connects users to private applications in the cloud or data center. Their identity and device is validated before connecting to the application in question — but not the network itself. This stops a threat actor from moving laterally across the network after gaining a foothold in the system. Better yet, with ZPA, the application is effectively hidden from the internet, severely reducing the organization's attack surface.

Splunk helps by providing centralized log ingestion and analytics against Zscaler logs that are readily ingested and normalized into Splunk's schema. The metadata and connection activity in Splunk gives your security team visibility, rich telemetry and dynamic integrated risk scoring to intelligently monitor and detect threats, and automate controls for access across your entire security environment.

Splunk's zero trust analytics dashboards reference Zscaler's logs to give the customer greater insight into their usage, access and environment. Splunk Enterprise Security (ES) provides robust analytics with Risk Based Alerting (RBA) and User and Entity Behavior Analytics (UEBA), which identify abnormal patterns and stitch together anomalies for easy detection. Splunk Phantom integrates with Zscaler APIs to automatically trigger event triage, investigations and response actions orchestrated across your security environment.

## Accelerate time-to-value with Zscaler ZIA Cloud to Cloud Log Streaming and Splunk

ZIA Cloud to Cloud Log Streaming provides a simple and fast way to stream logs to Splunk Cloud. Organizations can focus on their data and stop deploying, managing and scaling logging infrastructure. Zscaler logs are sent via a secure HTTP push, ensuring logs are delivered reliably and securely. ZIA Cloud to Cloud Log Streaming is easy to set up and configure. With a few clicks, logs can start streaming to Splunk. Zscaler's logs are readily normalized within Splunk, allowing correlation across the organization's additional data sources. This integration simplifies security operations by providing actionable data within Splunk, reducing the need to pivot across product consoles during investigations. Zscaler's rich security telemetry can enrich investigations and threat hunting activity for cloud-first organizations.

The Zscaler App for Splunk is available on Splunkbase and provides administrators with prebuilt dashboards that provide a quick view into usage, applications, user activity and threats.

See for yourself how Splunk can prevent service interruptions and reduce the mean time to restore service.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com