PARTNER BRIEF

Securing the Enterprise with Zscaler™ and Splunk

Traditional perimeter security can expose the enterprise

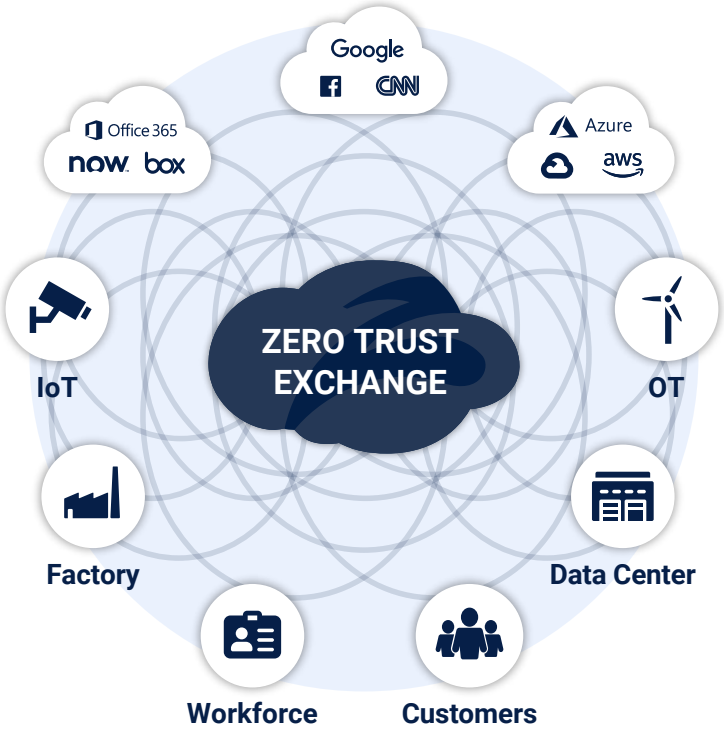
The COVID-19 pandemic accelerated organizations' digital transformation initiatives as employees began to work from home on a large scale. Remote employees now access applications and data in the cloud directly, often bypassing traditional security controls. When devices connect directly to the internet, the attack surface of the enterprise becomes much larger, making it more difficult for security teams to maintain visibility and consistent protection against threats. In this cloud-centric world, outdated perimeter-based security architectures are no longer effective. Organizations need a cloud-native zero trust architecture in order to protect their workforce and sensitive data.

Splunk and Zscaler have partnered to protect the workforce by providing a tightly integrated cloud security and analytics platform. Zscaler and Splunk customers realize the benefits of SASE (Secure Access Service Edge), zero trust, and analytics from cloud-native solutions, enabling them to reduce risk by minimizing the attack surface and providing greater visibility and control.

Zscaler + Splunk = zero trust

Zscaler's cloud-native security platform is delivered on a custom-built zero trust architecture that securely connects users to apps, apps to apps, and machines to machines over any network, in any location. Traffic that moves through the Zscaler Zero Trust Exchange (ZTX) is continuously scanned and authenticated, including inline SSL inspection, without the need for any expensive hardware. Applications aren't exposed to the internet, dramatically reducing the attack surface. By connecting users directly to applications rather than a network, malicious actors aren't able to move laterally, limiting the damage they are able to cause in the event of a breach.

The ZTX is built around the model of cloud-delivered, zero trust connectivity that scales with business demands, reduces the risk of a distributed digital business, and increases user productivity by providing a fast, easy, and reliable user experience.



While ZTX provides security, authentication, and policy controls over transactions, Splunk provides the analytics for defense in depth–both key components of zero trust. Splunk correlates all data, performs threat detection, and automates incident response.

Because Zscaler logs conform to Splunk's schema, it makes correlation searches easy. The metadata and connection activity provided by Zscaler gives security teams visibility, rich telemetry, and dynamic integrated risk scoring to intelligently monitor and detect threats, while also automating controls for access across the entire security environment.

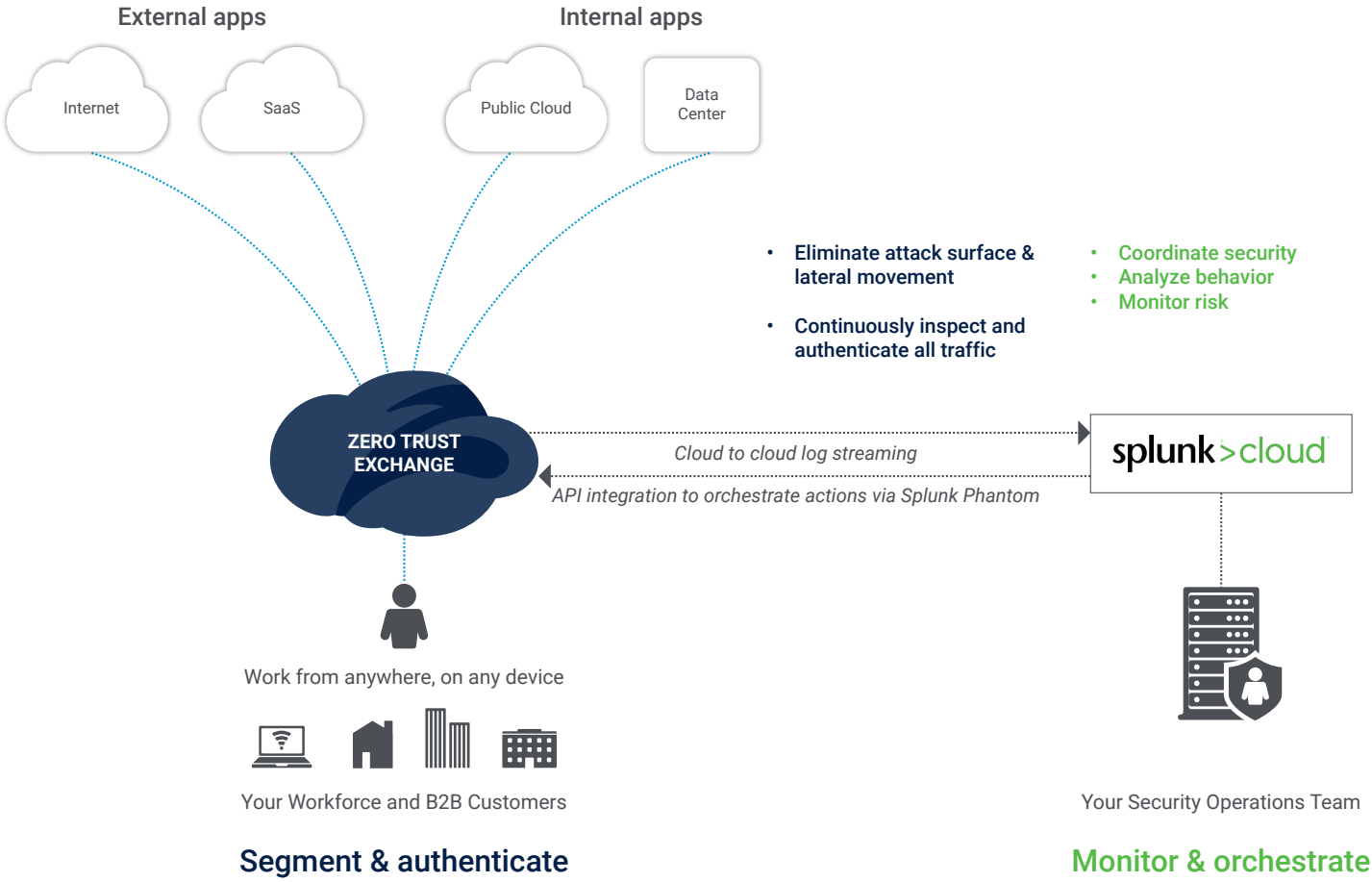
What is Zero Trust?

Zero trust is based on the principle of least privileged access. It asserts that entities should not be inherently trusted.

Zscaler Zero Trust Exchange (ZTX) is used to securely connect user and apps using business policies over the internet.

The tenets of ZTX are–

- Connect user to specific resources, not a network, preventing lateral movement of threats.
- The attack surface should be reduced by making the application invisible to the internet.
- Use a proxy architecture -- not a passthrough -- for effective content inspection and security.

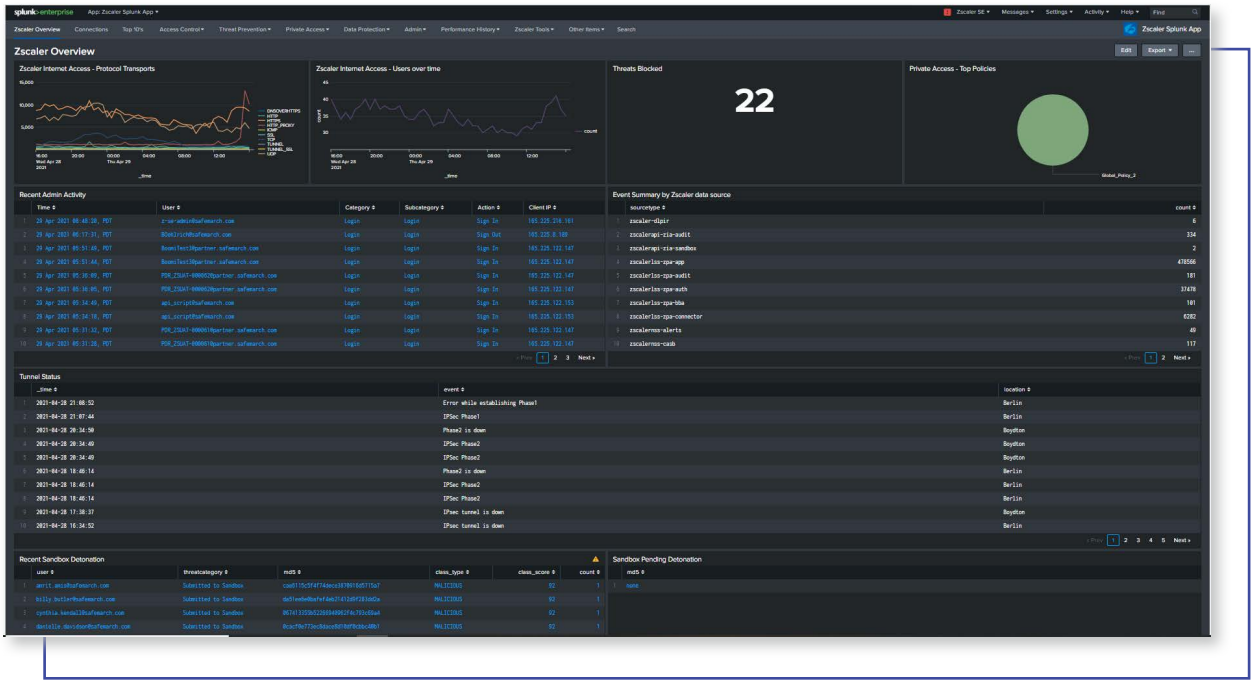


Accelerate time-to-value with ZIA cloud-to-cloud log streaming

Zscaler Cloud NSS builds on the foundation of the Nanolog Streaming Service (NSS) to provide a simple and fast way to perform cloud-to-cloud log streaming to a SIEM. Zscaler Cloud NSS provides a direct, one-click integration with Splunk Cloud, allowing organizations to focus on data insights instead of maintaining logging infrastructure. Zscaler logs are sent via a secure HTTP push, ensuring logs are delivered reliably and securely. This feature is easy to set up and configure–with a few clicks, logs start streaming and are normalized within Splunk, allowing correlation across the organization's additional data sources.

The tight integration between Zscaler and Splunk 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, and is stitched together with other security data to provide SecOps teams with real-time visibility into ongoing threats, violations, and vulnerabilities.

The Zscaler app for Splunk provides administrators with prebuilt dashboards to give a quick view into usage, security, activity, and threats. Administrators have a view of Zscaler activity across the enterprise, regardless of user location. Admins can also drill into the dashboards to create more complex correlation searches.



Zero trust analytics

Splunk's zero trust analytics dashboards leverage 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). This enables the identification of abnormal patterns by stitching together anomalies for easy detection. Splunk's zero trust analytics incorporate data from multiple sources to provide end-to-end visibility.

Zero trust orchestration and automation

Splunk Phantom is able to perform automated remediation or repetitive tasks by leveraging Zscaler APIs to block URLs, perform reputation lookups, and run queries against the Zscaler sandbox. Phantom is able to orchestrate across tools and platforms, using playbooks to provide automation of zero trust-related incident response, including malware containment and response and active directory reset password/ lock account functionalities.

Summary

Zscaler integration with Splunk enables organizations to strengthen their security posture by delivering zero trust security and analytics, all from the cloud. Leveraging Zscaler's high-resolution telemetry, Splunk is able to monitor, detect, investigate, and remediate threats using automated security operation workflows. Contact Zscaler or visit www.zscaler.com for more information.

Integration Benefits

- **Fast, Reliable Integration:** ZIA cloud-to-cloud log streaming provides high-resolution telemetry directly into Splunk over a reliable and secure HTTPS channel
- **Zero Trust Analytics Dashboard:** Leverage Zscaler's logs to give the customer better insight into their usage, access, and environment
- **Zscaler App for Splunk:** Provide administrators with prebuilt dashboards that provide a quick view into usage, applications, user activity, and threats
- **Orchestration:** Splunk Phantom integrates with Zscaler APIs to automatically trigger event triage, investigations, and response actions orchestrated across your security environment
- **Compliance and Threat Research:** Data warehousing within Splunk for historical analysis

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 Splunk
Splunk is the world's first Data-to-Everything Platform designed to remove the barriers between data and action, so that everyone thrives in the Data Age. We're empowering IT, DevOps and security teams to transform their organizations with data from any source and on any timescale.

zscaler™ / splunk>

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com