PARTNER SOLUTION BRIEF

Zscaler and Splunk Solution Brief

SOLUTION OVERVIEW

Zscaler and Splunk have partnered to integrate rich web, social and mobile application user and security event data to provide a actionable, single view across all elements in a environment.

Organizations seek to correlate log data across multiple devices to effectively analyze its traffic patterns across its network to identify anomalies and security vulnerabilities. Organizations may also have compliance or operational requirements to store data on-premise for future audit and analysis.

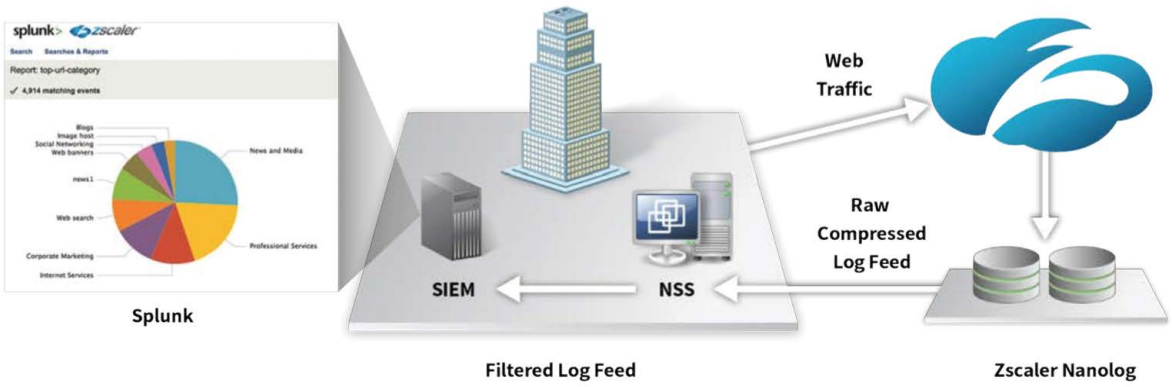
Zscaler Nanolog Streaming service (NSS) streams real-time and comprehensive log data to Splunk. Zscaler uses Splunk Common Information Model (CIM), which provides a standard method of parsing, categorizing and normalizing data. Data imported from Zscaler NSS conforms to the Splunk CIM format, so that the data is properly reported and correlated. The Splunk App for Zscaler gives the security practitioner visibility into security-relevant data captured, correlated and indexed within Splunk.

Splunk App for Zscaler reports and correlation searches are designed to present a unified view of security across heterogeneous vendor data formats. Administrators can leverage dashboards and reports in Splunk to track security compliance. Splunk App for Zscaler not only enables organizations to visualize user web, mobile, application logs but also correlate logs & events from other data sources.

HIGHLIGHTS

- Seamless integration with customers existing Splunk SIEM infrastructure using CIM format.
- Real time, unified visibility for threat detection and prioritization on a single platform across all devices, users and locations.
- Automatically discover useful security information embedded in your data across heterogeneous environment.

Splunk App for Zscaler



About Zscaler

Zscaler is revolutionizing Internet security with the industry's first security-as-a-service platform, used by more than 5,000 leading organizations, including 50 of the Fortune 500. Zscaler is a Gartner Magic Quadrant leader for Secure Web Gateways and delivers a safe and productive Internet experience for every user, from any device, and from any location — 100% in the cloud. Zscaler delivers unified, carrier-grade Internet security, next-generation firewall, web security, sandboxing/advanced persistent threat (APT) protection, data loss prevention, SSL inspection, traffic shaping, policy management, and threat intelligence — all without the need for on-premises hardware, appliances, or software. To learn more, visit us at **www.zscaler.com**.

About Splunk

Splunk Inc. (NASDAQ: SPLK) provides the engine for machine dataTM. Splunk® software collects, indexes and harnesses the machine-generated big data coming from the websites, applications, servers, networks, sensors and mobile devices that power business. Splunk software enables organizations to monitor, search, analyze, visualize and act on massive streams of real-time and historical machine data. 5,600 enterprises, universities, government agencies and service providers in over 90 countries use Splunk Enterprise to gain Operational Intelligence that deepens business and customer understanding, improves service and uptime, reduces cost and mitigates cybersecurity risk. Splunk Storm®, a cloud-based subscription service, is used by organizations developing and running applications in the cloud. To learn more, please visit **www.splunk.com/company**

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

CONTACT US

Splunk Inc.
270 Brannan Street
San Francisco, CA 94107
+1 415.848.8400

www.splunk.com