PARTNER SOLUTION BRIEF

Zscaler and QRadar Solution Brief

SOLUTION OVERVIEW

Zscaler and IBM QRadar have partnered to deliver deeper data analysis, visibility and digital forensics.

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 complements the deep analysis capabilities of Qradar SIEM solution by providing a comprehensive view into user activity.

Zscaler Nanolog Streaming service (NSS) provides real-time and comprehensive log data. IBM QRadar can collect and categorize events from Zscaler NSS log feeds that forward syslog events to QRadar. IBM QRadar's Device Support Module (DSM) for Zscaler, accepts events forwarded in Log Enhanced Event Format (LEEF) by NSS. Zscaler's NSS adds deeper data analysis encompassing all users, across all devices and location into Qradar SIEM platform.

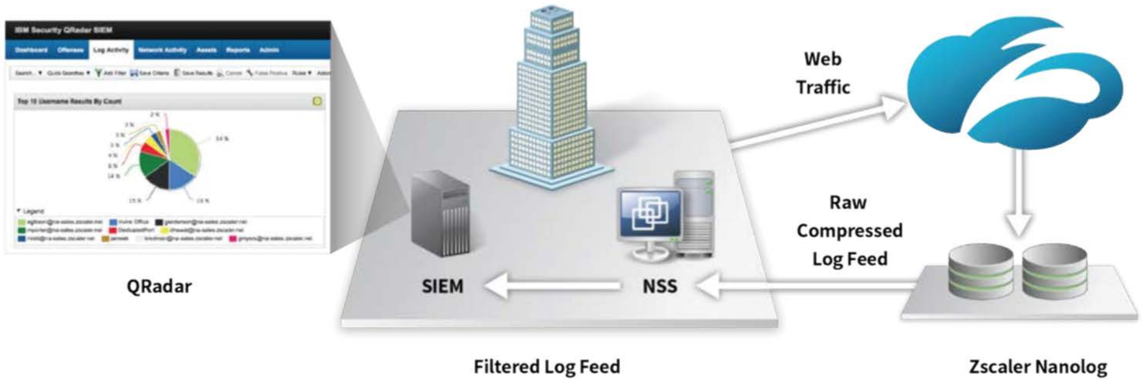
IBM Security QRadar SIEM can serve as the anchor solution within the organization to collect, normalize and correlate available network data using years' worth of contextual insights.

This integration allows IBM QRadar to correlate user specific data into other relevant data feeds that it is collecting, into a single view, combining user, application and security threat anomalies.

HIGHLIGHTS

- Seamless integration with customers existing QRadar SIEM infrastructure.
- Real time visibility for threat detection and prioritization on a single platform across all devices, users and locations.
- Integrate log management and network threat protection technologies within a common database and shared dashboard user interface.

Integrating IBM QRadar with Zscaler NSS



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 QRadar

IBM® Security QRadar® SIEM is a distributed enterprise Security Information and Event Management solution that provides contextual and actionable surveillance across the entire IT infrastructure, helping organizations detect and remediate threats often missed by other security solutions. The software automatically discovers most network log source devices and inspects network flow data to find and classify valid network hosts (assets)— tracking the applications, protocols, services and ports they use. It collects, stores and analyzes data performing real-time event correlation for threat detection and compliance reporting. Billions of daily events and flows are typically prioritized into just a handful of actionable offenses. **www.q1labs.com**

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

QRadar
IBM Corporation , 1 New Orchard Road
Armonk, New York 10504-1722 , US
+1 914.499.1900

www.q1labs.com