sumo logic | zscaler

SOLUTION BRIEF

Modern Security Ops with Zscaler and Sumo Logic

With enterprises embracing cloud resources and SaaS services, the attack surface has grown. This becomes even more challenging as employees are working from everywhere. Users go directly to the internet, bypassing traditional security controls found in the data center. A new approach is needed to provide security and visibility for the enterprise.

Solution Overview

Zscaler provides security and policy enforcement through the Zero Trust Exchange while Sumo Logic provides analytics and visibility. Both services are delivered 100% in the cloud.

Zscaler and Sumo Logic have partnered to integrate rich web, social and mobile user and security event data to provide actionable, single views across all elements in an environment. Organizations seek to gain a unified view of log data across an increasingly complex and heterogeneous environment to effectively detect and respond to indicators of compromise (IOCs) in their web traffic and identify anomalies and security vulnerabilities. Organizations may also have regulatory compliance requirements around centralized logging and data retention.

Sumo Logic App for Zscaler Internet Access

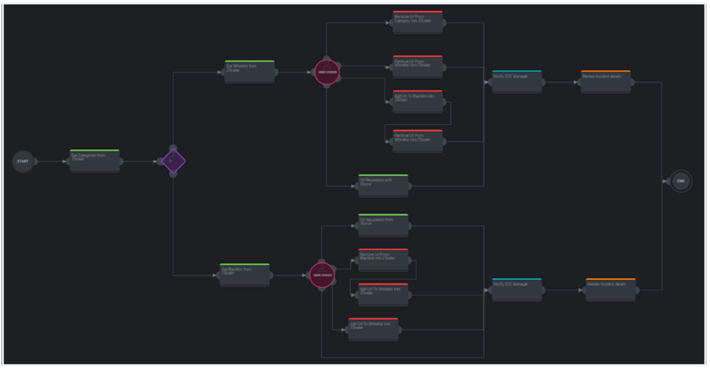
Zscaler Internet Access (ZIA) delivers world-class threat protection and policy control over all of your web traffic. The solution sits inline between your company and the Internet, protecting your enterprise from cyberthreats, stopping intellectual property leaks, and ensuring compliance with corporate content and access policies. It monitors your network and user activity, secures roaming users and mobile devices, and manages all of this globally from a single management console. Zscaler's security capabilities provide defense-in-depth, protecting you from a broad range of threats including malicious URL requests, viruses, Advanced Persistent Threats, zero-day malware, adware, spyware, botnets, cross-site scripting, and more.

Sumo Logic App for Zscaler Private Access

The Zscaler Private Access App collects logs from Zscaler using the Log Streaming Service (LSS) to populate pre-configured searches and dashboards. The dashboards provide easy-to-access visual insights into user behavior, security, connector status, and risk. Security teams can use the findings from the app to monitor and alert on the status and availability of Zero Trust Network Access deployments for apps running in the private cloud and datacenter. Monitor ZPA health and keep your ZPA infrastructure operating smoothly by keeping a close eye on connector health and performance. Easily visualize all the changes that have occurred on the ZPA infrastructure to assure compliance with policy and identify suspicious activity.

Sumo Logic Cloud SOAR integration with ZScaler security gateway for secure access to the Internet

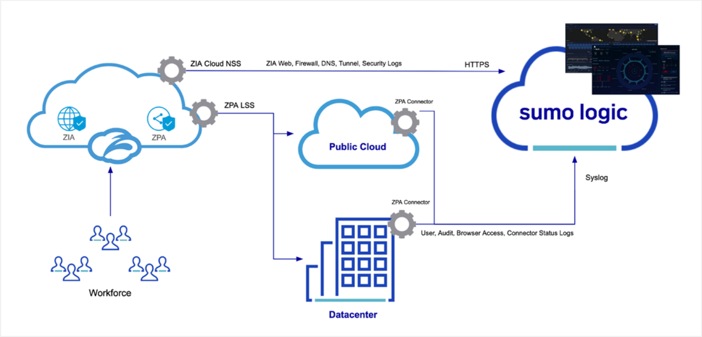
Orchestrate ZScaler technology inside your ongoing processes and automate threat response using Cloud SOAR. Playbooks highlight appropriate courses of action, reducing the time needed to remediate incidents and can be easily modified by adjusting tools in relation to processes. For example, when a user tries to view a particular website and Cloud SOAR receives input that generates an incident, you can activate a playbook to collect categories present on ZScaler. Once the playbook obtains the necessary information, if a category is allowed, it checks the whitelist from ZScaler and creates a User Choice. The User Choice invites the SOC Analyst to perform the action they consider to be the most appropriate. If the category is not allowed, the playbook gets the ZScaler blacklist.


START
Get Categories from ZScaler
Get Whitelist from ZScaler
USER CHOICE
Remove Url From Category into ZScaler
Remove Url From Whitelist into ZScaler
Add Url To Blacklist into ZScaler
Remove Url From Whitelist into ZScaler
Url Reputation with Xforce
Notify SOC Manager
Review Incident details
END
Get Blacklist from ZScaler
USER CHOICE
Url Reputation from Xforce
Remove Url From Blacklist into ZScaler
Add Url To Whitelist into ZScaler
Add Url To Whitelist into ZScaler
Notify SOC Manager
Review Incident details

Benefits of this joint integration include:

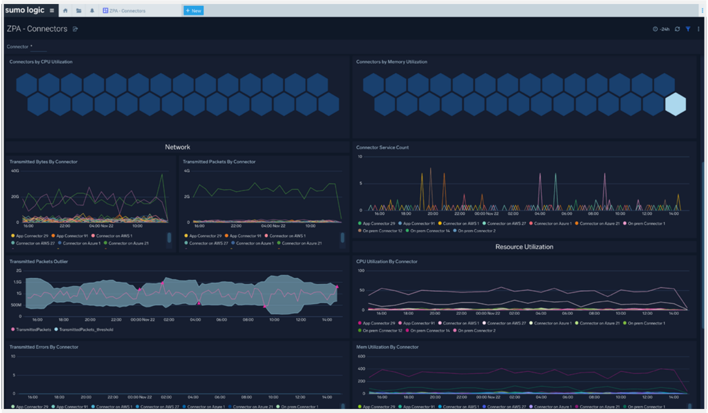
- Seamless integration with customers' existing Sumo Logic deployment.
- Real time, unified visibility of threat detection and prioritization on a single platform across all devices, users and locations.
- Automatically discover useful security information embedded in your data across heterogeneous environments.

ZIA Cloud NSS streams real-time and comprehensive log data to Sumo Logic. The Sumo Logic App for Zscaler gives the security practitioner visibility into security-relevant data captured, correlated and indexed within Sumo Logic.



Full Security Stack Integration with Sumo Logic

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



Moving to the cloud does not require sacrificing visibility or control over your infrastructure and applications. Sumo Logic and Zscaler have partnered to provide modern tools and services designed for the volume, variety and velocity of hybrid cloud-generated data and provide real-time operational and security visibility into your modern application stack.

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.

Sumo Logic

Sumo Logic, Inc. (NASDAQ: SUMO) empowers the people who power modern, digital business. Through its SaaS analytics platform, Sumo Logic enables customers to deliver reliable and secure cloud-native applications. The Sumo Logic Continuous Intelligence Platform™ helps practitioners and developers ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. Customers around the world rely on Sumo Logic to get powerful real-time analytics and insights across observability and security solutions for their cloud-native applications. For more information, visit www.sumologic.com.

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com

Updated 07/2022