Hunters and Zscaler

Joint Solution Brief

Comprehensive Cloud and Network Security for Modern Enterprises

In today's cloud-first, mobile-centric world, securing data across cloud environments, networks, and applications is paramount. The integration between **Hunters Next-Gen SIEM** and **Zscaler** offers organizations a seamless and powerful solution to enhance threat detection, investigation, and response. By combining Zscaler's industry-leading zero trust exchange with Hunters' advanced threat detection, automatic investigation, and multi-source correlation, this partnership delivers real-time, high-fidelity insights that empower security teams to detect, investigate, and mitigate threats more effectively and efficiently.

Joint Solution Overview

Hunters Next-Gen SIEM automates the entire threat detection, investigation, and response process, utilizing AI-powered correlation, enrichment, and triage capabilities. Hunters integrates telemetry data and alerts from **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)** into its platform, correlating the activity with other security data sources (EDR, Cloud, and Identity logs). This integration delivers an enriched context and deeper insight into cloud-based threats, enabling faster and more accurate incident response.

Benefits of the Hunters and Zscaler Integration

Seamless Data Ingestion and Management

Data Ingestion: ZIA's Cloud Nanolog Streaming Services (Cloud NSS) and ZPA's Log Streaming Services (LSS) offer robust log forwarding capabilities to the Hunters platform. Hunters utilizes AWS S3 for Zscaler raw logs storage and provides self-service and fast onboarding to ingest this data into a data lake, normalizes it, and correlates it with other security telemetry. Analysts are empowered with enriched context.

Log Retention and Management: Hunters offers flexible data management, allowing organizations to either retain logs in an open, scalable security data lake or opt for a "bring-your-own-data lake" model. This ensures that all relevant data is available for threat hunting and regulatory compliance.

Faster, More Effective and Less Noisy Threat Detection

Out-of-the-box Detections: Hunters integrates with ZIA and ZPA to automate and augment the detection process by running Hunters out-of-the-box detectors on top of Zscaler built-in alerts. Leveraging AI, Hunters identifies suspicious activities from Zscaler data, prioritizes high-fidelity alerts, and initiates automatic investigations without human intervention.

Correlated Attack Stories: Hunters builds correlated attack stories by connecting Zscaler data with other sources such as EDR (Endpoint Detection and Response), cloud, identity, and network telemetry. This reduces investigation time by surfacing only high priority alerts and providing full threat context.

Improved Threat Hunting and Investigations

Hunting and Investigations: ZIA and ZPA logs provide critical insights into user activity and application traffic, allowing security analysts to perform advanced threat hunting and incident response. Hunters leverages investigation tools such as OCSF-based search and IOC search to easily correlate Zscaler data with other data sources, thereby offering a complete picture of an attack across devices, applications, and networks.

Key Use Cases

Advanced Cloud & Network Detections

Zscaler's **DLP** and detect and block suspicious web traffic and data transfers. Hunters ingests this data to further enrich threat stories, providing detailed alerts around C2 communications, malware spread, and lateral movement within the network.

Comprehensive Attack Investigation

Hunters correlates Zscaler data with other security tool data such as EDR telemetry, Windows Event Logs, Firewall, Cloud, and Identity logs providing contextual triage and investigation for the analyst reducing MTTR. For example, a malicious connection originating from the internal network and logged by Zscaler will be correlated to the EDR to reveal the malicious binary initiating the connection.
In addition, Hunters offers simple investigation tools based on OCSF, allowing analysts to navigate through Zscaler data quickly and easily.

Zero Trust Network Access (ZTNA)

The combined solution ensures secure access to internal applications using ZPA. Hunters offers an additional out-of-the-box detection layer on top of ZTNA preventive mechanism to ensure attacks are detected and remediated. In addition, Hunters correlates ZPA logs with other telemetry to detect anomalies in user behavior, such as abnormal location-based access or simultaneous logins, ensuring that even authorized users are monitored for malicious activities.

The integration between Hunters and Zscaler provides organizations with a powerful, scalable solution for securing cloud and network environments. By combining Zscaler's leading cloud security platform with Hunters' advanced detection and investigation capabilities, organizations can accelerate their incident response times, reduce false positives, and gain a deeper understanding of threats across their entire infrastructure.

To learn more about how Hunters and Zscaler can improve your security operations, contact us for a demo or consultation.

About HUNTERS

Hunters Next-Gen SIEM automates threat detection, investigation, and response, freeing analysts to proactively protect their organizations. Hunters deploys in days and eliminates repetitive work with out-of-the-box integrations and detection rules. High priority alerts are surfaced based on risk and confidence scoring, and similar alerts are clustered together, reducing alert triage by 80%. Customers can build an open, scalable data lake at a predictable cost, and bring their own data lake or leverage Hunters'. Team Axon provides rapid response to emerging threats, incident investigation, proactive threat hunting, and security posture and hygiene reporting.

About zscaler™

Zscaler accelerates digital transformation so 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, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.
Learn more at www.Zscaler.com