Zscaler Internet Access (ZIA)

Detection Strategy Guide

July, 2025

Product Overview

Zscaler is a cloud-based information security platform delivered through more than 100 global data centers and more than 1,000 points of presence. To use Zscaler, internet traffic from fixed locations is routed through Zscaler points of presence before going on to the public internet. Localized data centers store security policies that can be pushed worldwide in seconds, following users as they travel around the globe to enforce these policies without latency.

Zscaler serves as a cloud-based proxy and firewall, routing all traffic through its software. It centralizes administration of users and policies on a single web interface with a simple visualization, provides comprehensive user reports in near real-time, and constantly gathers global threat data.

Detection Strategy for Network Integrations

Detection

Network traffic monitoring is a critical element of our detection strategy, offering insight into the activity of data as it moves across an organization's systems. The network traffic data source focuses on network connection creation (the initial construction of a network connection such as socket information, and src and dst IP and Ports), network traffic content (logged network traffic data showing both protocol header and body values like PCAP), and network traffic flow (summarized network packet data, with metrics, such as protocol headers and volume like netflow or http logs).

We pull this information into our detection pipeline as events in the form of both security alerts and raw telemetry (depending on the integration). When a threat is detected, our automated response bot, Ruxie, takes action by enriching evidence fields with first- and third-party threat intelligence. Additional Ruxie actions query a wide span of technologies directly to arm analysts with key pieces of investigative information and related events.

Response

Network technologies are utilized for support across many types of Expel Alerts such as endpoint and cloud. The main focus of the response strategy is on source IP, destination IP, and domain tracking to identify related connections, along with user activity summaries to give extra alert context.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Zscaler Internet Access (ZIA)

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Zscaler Internet Access (ZIA), you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported platforms	■ Sumo Logic ■ Splunk ■ Microsoft Sentinel
Supported event log sources	■ Malware Protection ■ Advanced Threat Protection / Malicious Active Content Protection ■ Advanced Threat Protection / Botnet Protection ■ Sandbox ■ URL control
Zscaler Internet Access (ZIA) detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query by IP Address ■ Query by Domain Name ■ Query by Hostname ■ Query by Username ■ Search Raw Logs

Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).