Cloudflare ZTNA

Detection Strategy Guide

March 2026

Product Overview

Cloudflare Zero Trust Network Access (ZTNA) is a security solution that allows organizations to securely connect their users, devices, and applications without the need for traditional VPNs or physical network perimeter security. ZTNA is designed to enforce security policies and ensure that users can access only the applications they are authorized to use, from any device or location, with minimal risk.

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 Cloudflare ZTNA

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 Cloudflare ZTNA (via Webhook), you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.Additional Details and Common Questions

Supported event log sources	■ SCIM Logs ■ Risk Score Events ■ Gateway HTTP ■ Gateway Network ■ Access Requests
Cloudflare ZTNA detection rules support	No.
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 Host ■ Query IP ■ Query Risk Events

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).