



# Cloudflare WAF

Detection Strategy Guide

June, 2025

## Product Overview

The Cloudflare WAF provides full security visibility, delivers layered protections against OWASP attacks and emerging exploits, detects evasions and new attacks with machine learning, blocks account takeover, and detects data loss. It also includes both API security and bot management.

For the purposes of this integration, Expel leverages Cloudflare Logpull to pull all Security Events for each site you have onboarded.

## 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 WAF

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**did you expect this**) that we support for Cloudflare WAF, you can visit the [Detections page](#) in Workbench or ask your Sales or Support rep for the most recent download.

<b>Supported event log sources</b>	Expel pulls all WAF Security Events from Cloudflare for each customer domain to query against for adding context and correlation during alert triage.
<b>Cloudflare WAF detection rules support</b>	No.
<b>Detection rules written by Expel</b>	No.
<b>Investigative support through Workbench</b>	<p>Yes. We are able to take the following investigative actions to gather data for triage and investigation of events.</p> <ul style="list-style-type: none"> <li>■ Query IP</li> <li>■ Query Domain</li> <li>■ WAF Timeliner</li> </ul>
<b>Hunting support</b>	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).