Wiz Cloud

Detection Strategy Guide

June 2025

Product Overview

The Wiz Cloud Security Platform is an industry-leading Cloud Detection and Response (CDR) platform that helps customers assess their security and risk exposure across their cloud environments. Wiz provides full coverage across PaaS resources, virtual machines, containers, serverless functions or sensitive data stored in public buckets, data volumes, and databases.

Expel ingests and analyzes Wiz's cloud workload protection platform (CWPP) and Containers & Kubernetes Issues, which provides continuous threat monitoring and protection for cloud workloads across different types of cloud environment (AWS, GCP, Azure, etc), as well as real-time malicious behavior in Kubernetes clusters.

Expel Workbench integrates with Wiz in three ways:

- Issue polling - done through Wiz's APIs so Workbench can evaluate Wiz Issues.
- Direct Wiz console access - Expel analysts have secure access to customers' Wiz console to perform secondary triage and detail log data analysis, not available through APIs.
- Status Synchronization - using Wiz's APIs. Expel populates investigation updates to Wiz Issues throughout the validation process.

Detection Strategy for Cloud Integrations

Detection

Our cloud security detection strategy focuses on two common signal types at the control plane and resource levels: authentication events and API events. In limited cases, we also ingest certain data plane events such as network activity. We do this by integrating directly with cloud providers as well as cloud security service providers to gain a complete view of your cloud footprint.

We consume these events through a mix of raw log analysis and security alert processing, which are then run through our detection engine to look for signs of post-exploitation activity. 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 in order to directly arm analysts with key pieces of investigative information and related events.

Response

In addition to verbose evidence collection for cloud alerts, cloud technologies are useful for triaging SaaS and identity alerts as well. User activities within the cloud providers, along with related alerts for anomalous indicators, help analysts gain a full picture of the activity that occurred within a session.

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

What We Support for Wiz Cloud

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 Wiz Cloud, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Wiz - Advanced Tier License
Wiz detection rules support	No.
Detection rules written by Expel	Yes.
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).

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.

Use Cases Not Supported

- Vulnerability findings
- Host configuration rules
- Data classification rules
- CI/CD & Admission Policies