



Microsoft Azure

Detection Strategy Guide

May 2025

Product Overview

Microsoft Azure is a large cloud infrastructure service that is rapidly growing in popularity as it provides an enterprise platform for business solutions and a comprehensive set of cloud computing services, many with security monitoring built-in. Azure has over 100 cloud service offerings across a range of classes, such as computing, databases, storage, networking, analytics, application services, deployment, management, mobile, and developer tools. Expel focuses detection and response efforts on Azure services with built-in security logging, including but not limited to Active Directory Identity Protection, Monitor Log Analytics, and Security Center.

Detections documented here serve to support the security posture of the cloud core platform. Expel uses Azure's various log sources to produce unique detections without having to leverage additional security products.

Detection Strategy

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 Microsoft Azure

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 Microsoft Azure, you can visit the [Detections page](#) in Workbench or ask your Sales or Support rep for the most recent download.

<p>Supported versions</p>	<ul style="list-style-type: none"> ■ Virtual Machines ■ KeyVault ■ Entra ID ■ Network ■ Storage Accounts ■ Automation Accounts ■ SQL DB ■ Cosmos DB ■ AD Identity Protection ■ Security Center ■ Blob Storage logs* <p>* Azure Blob Storage logs are utilized as an investigative source only, not for lead alert generation.</p>
<p>Microsoft Azure detection rules support</p>	<p>Yes.</p>
<p>Detection rules written by Expel</p>	<p>Yes.</p>
<p>Investigative support through Workbench</p>	<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"> ■ Azure Log Analytics Search ■ Azure Log Analytics Query ■ Search Sumo
<p>Hunting support</p>	<p>Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help</p>

understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see [Hunting Techniques in the Help Center](#).

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 (**did you expect this**) 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.