Microsoft Defender for Cloud Apps

Detection Strategy Guide

September 2025

Product Overview

Microsoft Defender for Cloud Apps delivers full protection for SaaS applications, helping you monitor and protect your cloud app data across the following feature areas:

- Fundamental cloud access security broker (CASB) functionality, such as Shadow IT discovery, visibility into cloud app usage, protection against app-based threats from anywhere in the cloud, and information protection and compliance assessments.
- SaaS Security Posture Management (SSPM) features, enabling security teams to improve your security posture
- Advanced threat protection, as part of Microsoft's extended detection and response (XDR) solution, enabling powerful correlation of signal and visibility across the full kill chain of advanced attacks
- App-to-app protection, extending the core threat scenarios to OAuth-enabled apps that have permissions and privileges to critical data and resources.

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 Defender for Cloud Apps

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

Supported versions	■ All versions supported.
Supported platforms	■ Windows ■ Linux ■ MacOS
Defender for Cloud Apps detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	Yes. Expel analysts are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query IP ■ Query Logs ■ Query User
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.