Microsoft 365

Detection Strategy Guide

June 2025

Product Overview

Microsoft 365 provides email and productivity applications as a service. Microsoft 365 is a popular option for enterprises looking to minimize their on-prem footprint and avoid the costs that come along with managing infrastructure. Although organizations using Microsoft 365 don't have to worry about managing infrastructure, security is still a shared responsibility between Microsoft and their customers. Microsoft is responsible for physical security and ensuring systems are patched behind the scenes. Organizations are responsible for ensuring they are not putting their users and data at risk with insecure configurations or compromised credentials.

The Microsoft 365 detection and response strategy aims to help organizations gain visibility into active threats that must be remediated. Additionally, Expel provides resilience recommendations that help organizations lock down the platform and reduce the risk of a compromise.

Expel collects data through direct API integrations with the Microsoft 365 platform. Expel supports authentication with a Microsoft Entra ID Application with a set of read-only permissions. This integration allows Expel to collect alerts and audit logs from Microsoft and leverage that data for detection and response.

Detection Strategy for SaaS Integrations

Detection

Our SaaS detection strategy is designed to identify and respond to suspicious user activity across cloud-based applications. By integrating directly with SaaS platforms, we continuously monitor user behavior and focus on activities such as unusual login patterns, excessive data downloads, or unauthorized access to sensitive files.

In addition to user activity, we also detect other key SaaS-related events such as changes to administrative settings, the creation or modification of privileged accounts, and unexpected data sharing with external parties. These events are processed through our detection engine, which leverages behavioral analytics and threat intelligence to flag potential risks. When anomalies are 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

Similar to identity technologies, SaaS apps can hold valuable information such as user roles, location, and other metadata that helps analysts triage Expel Alerts of all types that contain source user information.

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

What We Support for Microsoft 365

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 Microsoft 365, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Microsoft 365 detection rules support	Yes.
Supported event log sources	■ M365 Audit Log ■ Azure Sign-In Events (P2) ■ Security & Compliance Alerts
Detection rules written by Expel	Yes.
Auto remediations	Yes. Expel supports automatic execution of some remediation actions for this integration when you follow our setup guide to update the permissions in your vendor device, and then enable the auto remediation in Workbench. The available auto remediations for this integration include: ■ Remove Malicious Email ■ Disable Accounts ■ Reset Credentials To enable auto remediations for your environment, see Enable an Auto Remediation in Workbench in the Help Center.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage

	and investigation of events. ■ Query Logs ■ Query User ■ Query IP
Hunting support	Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help 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 (**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.

Microsoft 365 Data Loss Prevention (DLP)

Expel doesn't triage or investigate Microsoft 365 data loss prevention alerts. In our experience, these alerts require a level of business context that only your internal team has. Without that context, Expel doesn't add value beyond what Microsoft 365 is already doing (alerting you of a potential policy violation).