Google Workspace Alert Center

Detection Strategy Guide

June 2025

Product Overview

Google Workspace is a cloud-based productivity and collaboration suite that includes Gmail, Google Drive, Docs, Sheets, Slides, and Meet. The platform provides real-time collaboration features, shared storage, and communication tools for businesses. Google Workspace includes administrative controls for user management, data loss prevention, security settings, and compliance features, with integration capabilities for third-party applications through Google's marketplace.

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 Google Workspace Alert Center

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 Google Workspace Alert Center, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported event log sources	■ Suspicious logins (as signal against our authentication common detection library) ■ Domain-wide data takeouts (through DUET) ■ Government attack warnings (through DUET) ■ Email malware reclassification
Google Workspace Alert Center detection rules support	Yes.
Detection rules written by Expel	Yes.
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 Raw Logs ■ Query User ■ Query IP ■ Query Cloud User Details
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.

Use Cases Not Supported

Use Case	Description	Reason
Google Operations Alerts	Update reminders and notices for Google Workspace applications.	These alerts generally represent security update reminders.
Google Voice Alerts	Configuration issue alerts for the Google Voice product.	Expel doesn't support investigating Google Voice.
App Maker Alerts	Misconfiguration alerts for the App Maker product.	The only alert that can fire for this technology is a misconfiguration of a SQL device, which doesn't indicate attacker activity.

Mobile Device Suspicious Activity	Google-provided detections regarding suspicious activity on support mobile devices.	Expel lacks the capabilities to support investigating mobile devices.
Apps Outage	A notification of an outage of Google applications.	These alerts represent a service outage, not a security event, so there is no lead to investigate.
User-reported Spam Spike	A user-reported metric referring to an increase in spam messages.	There's little value and a high level of effort involved in investigating spam emails from external sources.
Activity Rule	A custom, user-defined rule.	We don't support custom rules in Google Workspace Alert Center by default. If a customer creates a rule they'd like surfaced through DUET, we can look to do this on a case-by-case basis.
Data Loss Prevention	A custom, user-defined rule.	We don't support custom rules in Google Workspace Alert Center by default. If a customer creates a rule they'd like surfaced through DUET, we can look to do this on a case-by-case basis.
User-reported Phishing	A user reports possible phishing activity.	Expel offers Expel Managed Phishing for this use case, a much more effective and useful solution.
Leaked Password	A user’s password detected by Google as leaked.	Google Workspace automatically forces a password reset on affected accounts, so there's little to investigate here.
Mobile Device Compromised	Alerts on devices that are “rooted” for Android, or “jailbroken” for iOS.	We don't support investigating mobile devices. Organizations may inquire about this, in which case we can evaluate DUETs on a case-by-case basis.