



Palo Alto Networks SaaS Security (formerly Prisma SaaS)

Detection Strategy Guide

July 2025

Product Overview

Palo Alto Networks SaaS Security is a Cloud Access Security Broker (CASB) solution that discovers and controls new SaaS applications, protects against threats, and secures sensitive data. It provides comprehensive visibility into SaaS usage, enabling organizations to identify both sanctioned and unsanctioned applications being used across the network. The solution uses machine learning to classify applications and assess their risk, allowing administrators to enforce granular access policies. It also provides advanced threat prevention and data loss prevention (DLP) capabilities to protect against malware and the exfiltration of confidential information stored within SaaS applications, helping to ensure compliance and reduce the organization's attack surface.

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.

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 Palo Alto Networks SaaS Security

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 Palo Alto

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

Supported event log sources	■ Log Event
Palo Alto Networks SaaS Security detection rules support	No.
Detection rules written by Expel	Yes.
Auto remediations	No.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events.
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 (**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.