Fortinet FortiCNAPP (formerly Lacework)

Detection Strategy Guide

July 2025

Product Overview

Fortinet FortiCNAPP delivers security and compliance for the cloud. With Fortinet FortiCNAPP, leading enterprises and innovative companies get build-time to run-time threat detection, UEBA, and cloud compliance across multi-cloud environments, workloads, containers, and Kubernetes. Customers who use Fortinet FortiCNAPP significantly drive down costs and risk by freeing themselves from the burden of unnecessary hardware, rule writing, and inaccurate alerts. The overall Expel strategy is to support the Fortinet FortiCNAPP native breach detection service for cloud workloads in AWS and GCP. The Fortinet FortiCNAPP Polygraph breach detection service includes their proprietary innovations:

- Capturing behavior at process/container-level
- Separating interactive and non-interactive traffic
- Alert generation at the analysis group-level
- Advanced deductive analysis that does not rely on heuristics

At its core, Fortinet FortiCNAPP applies machine learning analysis to identify anomalous behavior that poses threats.

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.

What We Support for Fortinet FortiCNAPP

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

Supported event log sources	■ Security Events Monitoring through Events API for Workload Events.
Fortinet FortiCNAPP detection rules support	Yes. We ingest and analyze the security alerts generated by Fortinet FortiCNAPP's native detection rules and its Polygraph machine learning engine.
Detection rules written by Expel	Yes. We apply our own detection logic in Expel Workbench to correlate Fortinet FortiCNAPP's alerts with signals from your other integrated technologies to find threats.
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 ■ List Sources
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.

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.