Google Unified Security
Recommended

# Google Unified Security Recommended Solution Overview with **Palo Alto Networks Next Generation Firewalls**

## Unified Cloud Defense: Palo Alto Networks NGFW & Google Cloud Security

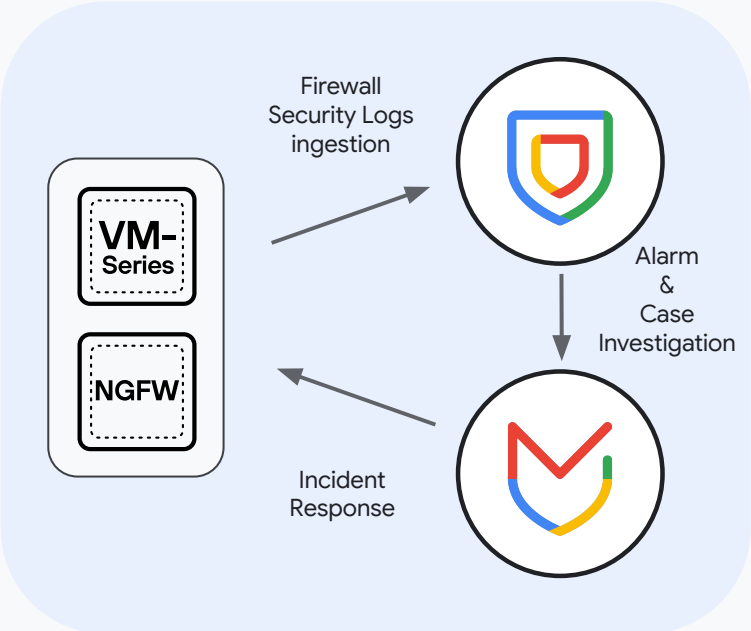
As organizations migrate critical workloads to Google Cloud, traditional network logs are no longer sufficient. Sophisticated attackers hide in encrypted traffic, leverage legitimate applications for lateral movement, and exploit vulnerabilities within your VPCs. To stop these threats, you need visibility that goes deeper than ports and IP addresses.

The Palo Alto Networks and Google Cloud partnership delivers a validated, integrated architecture that combines best-in-class network security with the industry's most advanced security operations platform.

## Unified Security, Instant Telemetry, Accelerated Response.

The joint solution centralizes network security enforcement and leverages the power of Google Cloud's Security Operations (SecOps) and Mandiant Services to dramatically accelerate incident response.

The architecture ensures that rich security logs and telemetry from the Palo Alto Networks Next-Generation Firewalls are streamed directly into Google SecOps SIEM. This immediate visibility is crucial for both automated remediation and expert-driven threat hunting. The result is a reduced investigation time from days to minutes, ensuring Mandiant's incident responders have the critical context needed to stop breaches faster.



paloalto NETWORKS

# Palo Alto Networks Next-Generation Firewalls export telemetry to Google SecOps, enabling Mandiant to perform rapid incident response.

## Google Security Operations

Next Generation Firewalls alerts are immediately contextualized using Google Threat Intelligence, which aggregates insights from Google Threat Intelligence, Mandiant, and Google's vast visibility into the threat landscape.

## Mandiant

Mandiant's frontline experts can analyze Cortex telemetry to determine if an alert represents a false positive or the early stages of a targeted breach.

## Google Threat Intelligence

Google SecOps automatically overlays Google Threat Intelligence onto your firewall logs. Connections to IPs associated with known threat actors are instantly flagged, transforming raw logs into actionable alerts.

Interested in learning more about our Google Unified Security Recommended partnership? Learn more.



Google Unified Security Recommended