Google Unified Security
Recommended

CROWDSTRIKE

Google Unified Security Recommended Solution Overview with **CrowdStrike**

Delivering AI-powered, unified protection across endpoint, identity, cloud, AI, and data to stop breaches in hybrid and multi-cloud environments.

Unified Protection. Simplified Security.

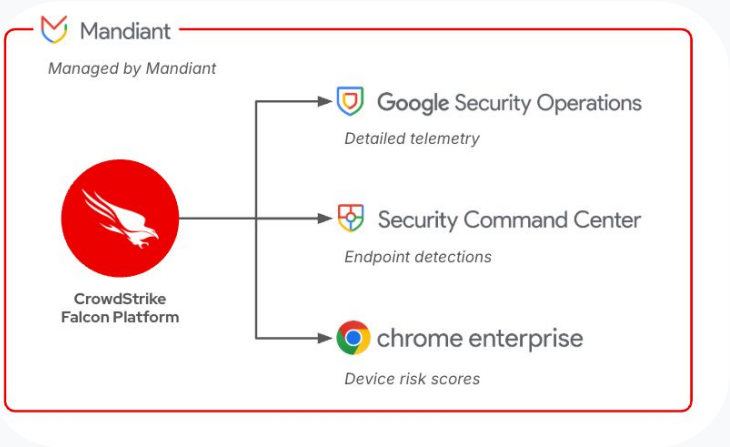
With the fastest eCrime breakout time of just 51 seconds[1], traditional security methods are failing. Disconnected tools create visibility gaps, allowing sophisticated threats to exploit weaknesses rapidly.

CrowdStrike and Google Unified Security offer unparalleled protection by unifying threat intelligence, security operations, and response across hybrid and multi-cloud environments. Together, we autonomously investigate alerts, enrich findings, and orchestrate rapid responses, transforming fragmented security into a cohesive, breach-stopping defense.

Key benefits of CrowdStrike

CrowdStrike integrates seamlessly with Google Security Operations to deliver unified threat detection, investigation, and response across endpoint, identity, cloud, AI and data—enabling security teams to **identify** and **neutralize** threats with AI-powered precision.

The integration extends to Google Threat Intelligence, **enriching** alerts with **real-time context** that helps **prioritize** critical threats while supporting Mandiant Incident Response and Managed Detection and Response services for **comprehensive protection.**



1 - CrowdStrike 2025 Global Threat Report

CROWDSTRIKE

CrowdStrike seamlessly integrates with Google's Unified Security ecosystem to deliver an AI-native defense fabric that unifies endpoint, identity, cloud, AI and data protection.

Google Security Operations

Full telemetry and detections delivered to Google Security Operations, plus automation of CrowdStrike response actions, enable a seamless end-to-end experience for SOC analysts for their most critical endpoint telemetry source.

Security Command Center

CrowdStrike detections presented in Security Command Center as a third party finding. Automatically deploy CrowdStrike endpoint agents across all of your Google Cloud VMs.

Mandiant

Mandiant Threat Defense monitors, hunts, and responds using Falcon Endpoints for enterprise organizations.

Google Threat Intelligence

CrowdStrike findings are natively enriched with additional intelligence on files, URL's, and IP addresses from GTI in the Falcon Platform.

chrome enterprise

CrowdStrike device risk scores are used to set Context-Aware conditional access policies in Chrome Enterprise Premium.

> "Through the Google Unified Security Recommended program, we're partnering with trusted leaders like CrowdStrike to help customers strengthen their defenses with unified, AI-driven protection," said Chris Corde, Senior Director of Product Management, Google Cloud. "CrowdStrike's integrations with Google Cloud products and services and commitment to open innovation exemplify what this program was built for – helping enterprises achieve better security outcomes and protect every environment from endpoint to cloud."

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

Google Unified Security Recommended