Google Unified Security
Recommended

Google Unified Security Recommended Solution Overview with **Palo Alto Networks Cortex XDR**

Accelerating Incident Response with Cortex XDR and Google Unified Security

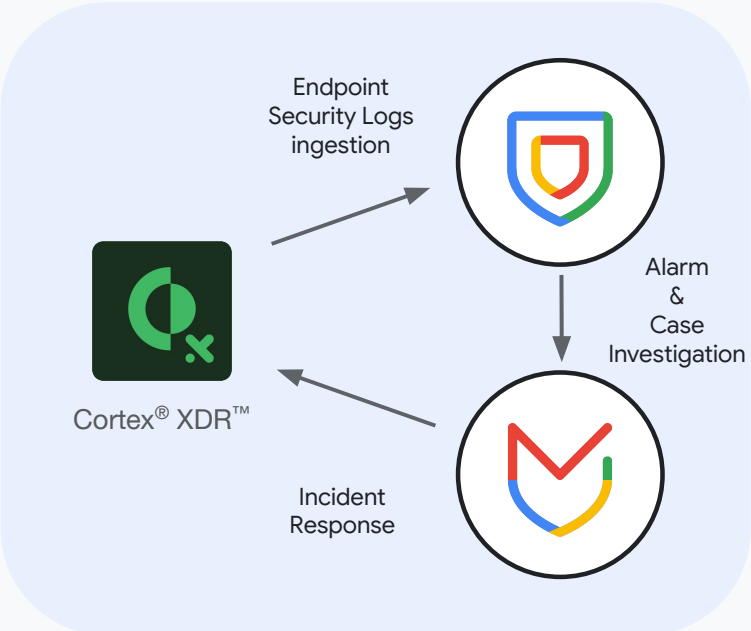
In the face of rapidly evolving cyber threats, modern security operations demand a unified, intelligence-led defense that can shorten the time between detection and remediation. The integration of Palo Alto Networks Cortex XDR with the Google Unified Security portfolio—including Google Security Operations (SecOps) and Mandiant Services—delivers this capability.

This powerful combination allows security teams to validate threats with unparalleled speed and confidence, ensuring rapid, confident decision-making against complex cyber attacks. Cortex XDR integrates with Google Unified Security to dramatically accelerate incident response across the entire IT estate.

Integrating Cortex XDR with Google SecOps and Mandiant Services empowers organizations with a unified, intelligence-led defense.

The joint solution establishes a high-fidelity, automated, and expert-driven security workflow:

- **Cortex XDR** acts as a high-fidelity threat detection and prevention data source providing rich, correlated telemetry from endpoints, networks, and cloud environments.
- **Google SecOps** serves as the hyperscale analytics and orchestration engine, unifying all data under a single model for rapid correlation.
- **Mandiant Services** injects world-class human expertise and threat intelligence for rapid validation and response guidance.



paloalto NETWORKS

Unifying Telemetry and Prevention: Accelerate Incident Response with Cortex XDR, Google SecOps Analytics, and Mandiant Expertise.

Google Security Operations

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

Google Threat Intelligence

Cortex XDR works in tandem with Google SecOps where High-severity alerts from Cortex XDR are ingested and enriched by Google Threat Intelligence data.

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.

chrome enterprise

Chrome Enterprise Premium ingests real-time health signals from Cortex XDR to instantly revoke access for compromised devices to stop lateral movement and data theft in its tracks.

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

Google Unified Security Recommended