Menlo Security Orchestrator for Gemini Enterprise

Agentic Security Operations for Gemini and Chrome Enterprise

The Complexity of AI-Driven Operations

In an AI-powered enterprise, the speed of attack often outpaces the speed of human intervention. Overwhelmed SOC teams already know where the friction is: manually correlating logs across disconnected consoles, chasing down which users hit a malicious URL, and waiting on policy updates that should take seconds but take hours. Traditional systems fail to provide the browser visibility needed to quickly identify the "blast radius" of a threat, leading to delayed remediation. Without a way to orchestrate unified policy enforcement across disparate security tools, the gap between discovery and defense remains dangerously wide.

- **Manual Threat Analysis:** Security teams are often forced to manually correlate logs across multiple tools to identify which specific users were exposed to a threat, a process that traditionally takes hours or days.
- **Friction-Heavy Policy Management:** Managing global security postures typically requires logging into separate consoles, leading to significant delays in blocking newly identified malicious domains.
- **Disconnected Security Ecosystems:** Traditional security tools operate in silos, lacking the "hands" to autonomously coordinate with other specialized agents to execute real-time, cross-platform defense strategies.

The Solution: Agentic Security Orchestration

The Menlo Security Orchestrator for Gemini Enterprise serves as a central intelligence layer that integrates directly with Gemini Enterprise. By moving from manual intervention to "agentic response," it reduces Mean Time to Remediate (MTTR) from hours to milliseconds.

The Menlo Security Orchestrator combines policy orchestration with threat investigation in a single interface — giving security teams the ability to query logs, reconstruct attack paths, and update

SOLUTION BRIEF

global policies using natural language, directly within Gemini Enterprise. Your analysts stay in one workspace. Response times that once took hours drop to seconds. Complex analytical prompts and natural-language queries surface the full attack path — synthesizing visualized threat behavior, identified actors, and known campaign data into reports your team can act on immediately. Stakeholders get real-time context as the threat is contained, without waiting for a manual writeup.

Key Use Cases

- **Real-time Impact Analysis & Threat Hunting:** An admin uses natural language queries like "Show me all users who accessed this URL and visualize the attack behavior" to identify the "Blast Radius" of a threat in seconds. By exposing these deep analytics, teams can instantly correlate exposure without manual log stitching.
- **Conversational Policy & Exception Management:** Security teams can add or remove entries from global blocklists or manage complex exceptions without ever leaving their primary workspace using 'set and forget' logic.
- **Agent-to-Agent (A2A) Automation:** Any A2A compliant agent can coordinate directly with the Menlo Security Orchestrator to update global protections autonomously based on new threat intelligence.

Instant Orchestrated Protection from Menlo

The Menlo Security Orchestrator for Gemini Enterprise replaces manual investigation and policy management with agentic intelligence — so your team spends less time correlating logs and more time closing gaps. Menlo Browser Security Platform customers can deploy it today, directly through the Google Cloud Marketplace. As your threat landscape grows more complex and your AI footprint expands, the Orchestrator scales with you — bringing the speed and context your SOC needs to stay ahead, not catch up.