



Monitoring and stopping AI-powered threats

Strategic Brief

Google Cloud
Security

Using AI to outpace adversaries

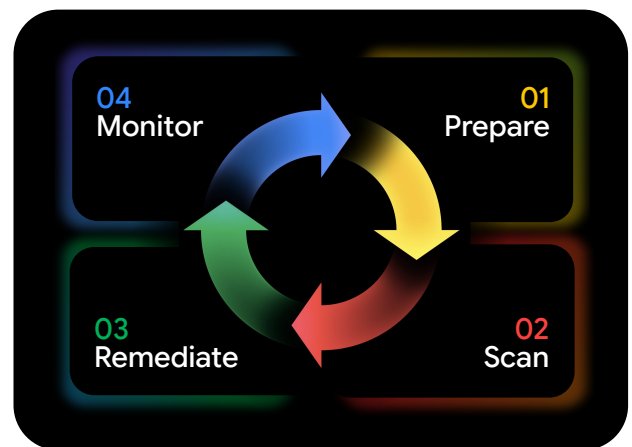
AI has fundamentally rewritten the enterprise threat landscape. Frontier models can now autonomously discover zero-day vulnerabilities and chain complex exploits at machine speed, compressing the window between disclosure and weaponization from weeks to minutes.

To protect modern enterprise applications, security teams must move past manual triage and deploy an always-on, machine-speed defense.

Google AI Threat Defense

Fuses the reasoning power of Gemini and other frontier models, contextual risk prioritization, code remediation, and frontline security expertise. By connecting real-world exposure directly to AI-driven code fixing, AI Threat Defense helps security teams discover potential attack paths and deploy verified fixes faster than adversaries exploit them.

[Learn more](#)



Google Security Operations

Works with AI Threat Defense to monitor, detect, and respond to threats across two difficult environments: external code the organization does not own, and proprietary code they do own but cannot safely patch due to legacy dependencies, fragility, or uptime constraints. Protecting both helps enterprises close the remediation gap, which by itself represents a critical vulnerability.

[Learn more](#)



Close the remediation gap with Google Security Operations

Google Security Operations works with AI Threat Defense to shift operations from manual oversight to machine-speed detection using autonomous agents. Google Security Operations enables teams to leverage AI to hunt for hidden threats and respond to new and novel threats in real time.

Using compensating controls to strengthen operational resilience, **Google Security Operations is built on a three-part approach to cross-environment visibility across the entire attack surface:**

1. Continuous and autonomous coverage analysis and detection generation
2. Autonomous investigation, containment, and response
3. Retroactive hunting

1. Apply continuous coverage analysis and generate detections



While AI Threat Defense can identify vulnerabilities before they can be exploited, there may be applications that cannot be patched, as well as potential gaps in the time it takes to remediate vulnerabilities. Google Security Operations includes a Detection Engineering agent that can automatically translate new exploitation patterns of unpatched vulnerabilities into custom detections for specific environments. It analyzes a diverse array of input sources to quickly and effectively recognize malicious activity to uncover novel attack patterns evolving from new and unpatched vulnerabilities.

The agent's sources include Google Threat Intelligence (such as emerging threat intelligence, new attack patterns curated by Mandiant, offensive tool repositories, red and purple team reports, autonomous malware analysis, open-source detection repositories and blogs), and internal security telemetry. To automatically find and fill coverage gaps tailored to each environment, the agent proactively builds new rules and validates them with synthetic events to help ensure the environment is covered before an exploit hits.

2. Investigate, contain, and respond to threats autonomously



If a threat is detected, immediate and autonomic assessment and response is needed. Google Security Operations brings together visibility from cloud and enterprise assets, including endpoints, on-premises firewall, identity, network, and custom application logs to provide full context of an attack, and unify disparate signals into a complete, actionable narrative the moment an adversary strikes.

The Triage and Investigation agent in Google Security Operations then reduces time to respond by investigating alerts, gathering evidence for analysis, and providing verdicts with comprehensive explanations. It can help security analysts automate decision-making, alert closure, and remediation flows, allowing them to spend more time prioritizing high-priority threats instead of false positives.

3. Hunt for the threats that have evaded other defenses



Even with autonomous detections and rapid-response handling of active threats, adversaries and zero-day exploits can sometimes bypass frontline controls. Security teams must also look backward through their data to uncover hidden compromises.

The Threat Hunting agent in Google Security Operations can help teams proactively hunt for novel attack patterns and stealthy adversary behaviors that bypass traditional defenses. By scouring petabytes of enterprise telemetry (including historical logs) for subtle anomalies, the agent shifts the security operations center (SOC) posture from reactive to proactive.

Outpacing adversaries with AI Threat Defense and Google Security Operations

Google AI Threat Defense is an autonomous system that combats AI-driven attacks by combining Gemini, CodeMender, and Wiz. Through a four-step framework—prepare, scan, remediate, and monitor—it identifies exposures, validates risks, and delivers verified fixes into developer workflows to reduce vulnerability backlogs.

Google Security Operations works alongside AI Threat Defense to help close the remediation gap for unpatched code using specialized agents. The Detection Engineering, Triage and Investigation, and Threat Hunting agents autonomously generate rules, orchestrate containment, and find hidden compromises, ensuring a proactive defense against automated adversaries. By integrating these Gemini-native agents directly into workflows, organizations can maintain a resilient defense at machine-speed.

[Learn more](#)
about Google AI
Threat Defense