AI Threat Defense

An automated security system designed to stop AI-powered threats before they can impact your business

Google Cloud

Security

Executive summary

Google AI Threat Defense provides customers with an autonomous security system designed to outpace AI-driven attacks.

It fuses the reasoning power of Gemini and other frontier models, the contextual risk prioritization of Wiz, the code remediation capabilities of Gemini and CodeMender, and the frontline expertise of Mandiant.

The ability to connect real-world exposure directly to AI-driven code helps security teams discover potential attack paths and deploy verified fixes faster than adversaries can exploit them.

AI is changing the threat landscape

Speed

The velocity of attacks is accelerating, particularly with agentic workflows. For instance, the handoff time between an initial access discovery and a secondary threat actor plummeted from 8 hours down to just 22 seconds last year.

Scale

Bad actors are scaling their operations through AI-driven automation and machine-speed processing. AI helps attackers scale and automate their operations, rapidly scan massive networks, automatically discover vulnerabilities, and execute multi-stage attacks without human intervention – drastically increasing their reach while using fewer resources.

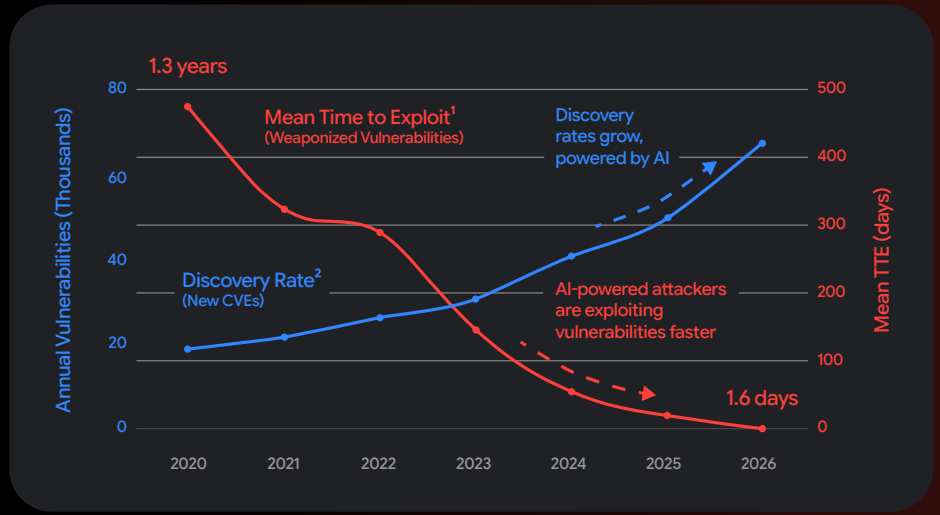
Sophistication

Adversaries are using AI to chain together multiple vulnerabilities into single, complex exploits. They are also deploying novel attack methods, including multimodal phishing, executive impersonation, and direct threats against enterprise AI infrastructure.

AI accelerates the discovery and exploitation of code vulnerabilities

As AI drives a massive surge in newly discovered vulnerabilities, it simultaneously empowers attackers to execute with unprecedented speed.

With annual CVEs skyrocketing and the mean time-to-exploit plummeting to just 1.6 days, enterprises face a critical risk window that human-speed patching simply cannot close.



Enterprises face a critical risk window that human-speed patching simply cannot close

[1] zerodayclock.com
[2] National Vulnerability Database (NVD); 2026 estimated

Google Cloud
Security

Transforming how we manage code vulnerabilities with AI

Proven four-step framework based on Google's own approach

01 Prepare
Reduce the attack surface area by eliminating unnecessary exposure

02 Scan
Find and validate software vunerabilities with AI agents

03 Remediate
Accelerate the resolution of high-priority issues

04 Monitor
Detect and respond to threats. Establish machine-speed detection and response against automated adversaries

01

Prepare: Reduce the attack surface area by eliminating unnecessary exposure

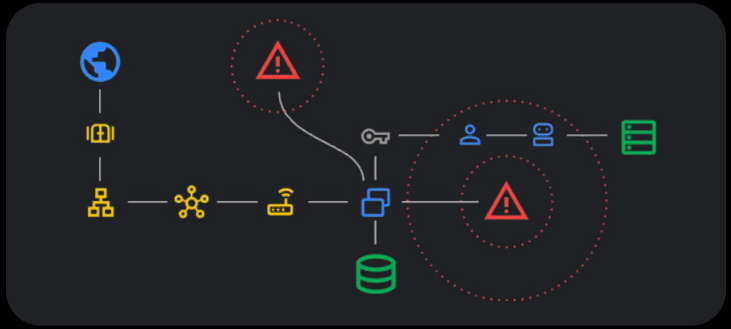
Key products & solutions

Wiz | Mandiant Consulting | Google Threat Intelligence

The objective

Proactively discover points of real exposure to improve your security posture

1. Map the environment and identify possible attack paths



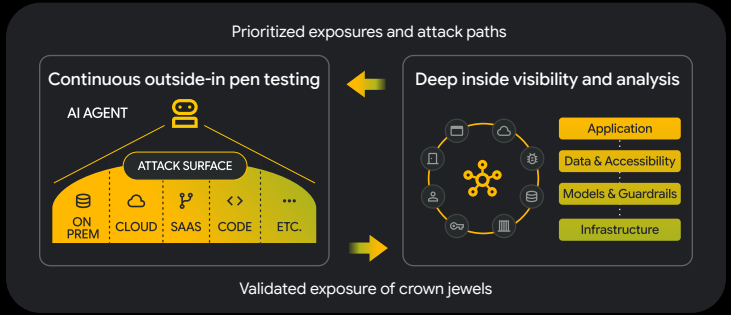
Continuously discover and inventory sensitive assets exposed to external attackers

Map relationships for applications, software dependencies, and ownership to understand the full architecture

Analyze the blast radius of a potential attack

Prioritize findings based on reachability and business impact

2. Assess exploitability



Use AI penetration testing to continuously analyze whether an exposure can be exploited

Enrich penetration test findings with context to understand severity

Prioritize issues most exposed to external attack

Google Cloud Security

The objective

Identify software vulnerabilities and assess their impact on your environment.

Scan

AI security agent that can autonomously find, verify, and fix deep vulnerabilities in code, including zero day ones

Enrich

Enrich results with Wiz context to link code vulnerabilities to real exposure

Validate

Validate external risk with Wiz Red Agent, an AI-powered continuous penetration tester

02

Scan: Enrich and validate vulnerabilities

Key products & solutions

- Wiz
- CodeMender
- Gemini Enterprise Agent Platform

Google Cloud Security

The objective

Implement high-speed workflows to autonomously generate, verify, and deploy fixes at scale directly within the developer's tooling.

How we do it

Automated Investigation

Wiz Green Agent analyzes a security graph to identify the exact code repository, infrastructure, and responsible developer.

Remediation Routing

The Green Agent determines the fastest safe action and triggers Wiz Workflows to alert the owner via ticketing systems.

Agentic Code Fixing

The remediation plan is sent to CodeMender/Gemini, which authors the specific code diffs and tests the fix within a secure sandbox to prevent regressions.

1-Click Deployment

A standard patch is staged as a Pull Request in the version control system, allowing the developer to review and click to deploy.

03

Remediate: Accelerate resolution of high-priority issues

Key products & solutions

- Wiz
- CodeMender
- Gemini Enterprise Agent Platform
- Mandiant Consulting

04

Monitor for current exploits

The objective

Establish machine-speed detection and response against automated adversaries

1. Compensating Controls

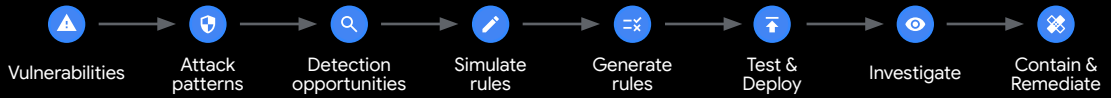
When you can't fix the lock, AI improves the alarm system.

2. Agentic Workflows

Autonomous Analysis → Simulation → Detection Rule Generation.

3. Real-Time Defense

Rules generated for unpatched systems and deployed in real time



Mean time to Detect and Respond in minutes, not hours

Key products & solutions

Wiz | Mandiant Consulting | Google Security Operations*

*Works in concert with AI Threat Detection to monitor, detect, and respond to threats.

Google Cloud Security

Google is here to help throughout your journey

04 Monitor

Transition to continuous detection & rehearsed, active response playbooks

- Wiz
- Mandiant Consulting
- Google Security Operations

01 Prepare

Harden your foundation & operationalize framework for machine-speed prioritization and response

- Wiz
- Mandiant Consulting
- Google Threat Intelligence

03 Remediate

Implement a workflow to autonomously verify & patch vunerabilities quickly

- Wiz
- CodeMender
- Gemini Enterprise Agent Platform
- Mandiant Consulting

02 Scan

Conduct deep-dive analysis & AI-driven posture validation

- Wiz
- CodeMender
- Gemini Enterprise Agent Platform

Outpace cyber adversaries

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.

Learn more about Google AI Threat Defense

Google Cloud Security