

Proactive cyber defense for governments and enterprises

2.9.2026 - Four Flynn | Google Italia

Today, we're launching our Fairwind Program, a limited access program for governments and trusted partners to use our most advanced cyber defense capabilities.

Defenders wanting to use advanced AI have faced a difficult dilemma: adopt enormous frontier models that could be expensive to deploy and difficult to control across enterprise codebases, or turn to smaller open-weight models that might struggle with complex vulnerability remediation and require teams to build their own tooling and infrastructure from scratch. Until now.

Today, we're launching our Fairwind Program to bring the best of Google's AI and cyber defense capabilities to a trusted group of Google Cloud customers, government agencies, and cybersecurity partners, to help them proactively solve cyber risks at scale. As a first step, the Fairwind Program will give defenders access to powerful and advanced Gemini models to help them autonomously find and fix vulnerabilities, protecting critical infrastructure, public services, and national security.

Finding and autonomously fixing vulnerabilities

The Fairwind Program offerings bring together our most advanced cyber model, Gemini 3.8 Flash Cyber, with our CodeMender harness, to help defenders find, verify, and fix vulnerabilities at agentic scale. Spotting weaknesses creates awareness and fear; autonomously finding and fixing vulnerabilities delivers security.

CodeMender with Gemini 3.8 Flash Cyber delivers the specialized reasoning to write and validate code fixes, at a fraction of the operating cost of traditional frontier models. Instead of taking weeks to manually fix vulnerabilities, defenders can now generate verified, deployment-ready patches in minutes — within an organization's secure cloud environment.

Scaling frontline defense

Providing early access to these powerful cyber capabilities gives trusted defenders a vital adaptation window to harden their systems before bad actors have a chance to exploit new capabilities. We're staging initial access to government and enterprise partners most critical to society's resilience:

- Governments and national cyber authorities: Hardening public-sector networks and citizen services against targeted intrusions.
- Critical infrastructure operators: Protecting essential services across healthcare, telecommunications, energy, and financial networks from operational disruption.
- Core technology platforms: Securing widespread software foundations to uplift digital security for millions of downstream users at once.

To ensure these powerful AI capabilities are used responsibly, participating organizations agree to strict operational standards, including limiting access to employees within their internal cybersecurity, incident response, or penetration testing teams and deploying protections like multi-factor authentication.

We have more than 650 participating partners globally, including:

What our Fairwind Program partners are saying

Trusted defenders and industry leaders are already putting Gemini 3.8 Flash Cyber into practice:

The Fairwind Program will evolve alongside our partners and users' needs. We will adapt our product offerings and expand partner access, collaborating closely with industry, governments, and open-weight community leaders to strike the right balance between open access and robust security.

While we are prioritizing Gemini 3.8 Flash Cyber access for customers in the Fairwind Program, any Google Cloud customer can proactively secure their code by using CodeMender with publicly available models hosted on Gemini Enterprise Agent Platform, in combination with industry-leading solutions offered through AI Threat Defense.

Making an ecosystem-scale impact on cyber defense

Years of Google's pioneering zero-trust architecture, advanced AI defenses, and built-in security allow us to protect billions of accounts daily – keeping more people and organizations safe online than anyone else. The Fairwind Program builds on this experience and is part of our broader commitment to global cyber resilience across the entire digital ecosystem, including helping to fortify grassroots cyber defense.

Through Google.org, our latest commitment brings our total cybersecurity funding to more than \$100 million globally. We're pleased to release our 2026 Google.org US Cybersecurity Impact Report, which details \$36 million in funding for 35 cyber clinics to date, providing free, hands-on security support to over 1,250 hospitals, public school districts, and municipal utilities in the U.S.

Providing a security advantage

The defender's edge comes from shrinking the time between detecting a flaw and patching it. Through Google's Fairwind Program, government and enterprise partners gain autonomous tools to repair systems faster and at scale, keeping them one step ahead of agentic-speed threats.

<https://blog.google/innovation-and-ai/technology/safety-security/fairwind-program>