

Forum:[Hack Forums](#)

Thread: [Claude Security is now in public beta](#)

MadScientist - May 2, 2026, 8:50 am

Claude Security is now available in public beta to Claude Enterprise customers.

AI cybersecurity capabilities are advancing fast. Today's models are already highly effective at finding flaws in software code; the next generation will be more capable still, and will be particularly effective at autonomously exploiting these flaws. Now is the time for organizations to act to improve their security, preparing for a world in which working software exploits are much easier to discover.

Recently, we made Claude Mythos Preview—which can match or surpass even elite human experts at both finding and exploiting software vulnerabilities—available to a number of partners as part of Project Glasswing.

But our cybersecurity efforts go beyond Glasswing: with Claude Security, a much wider set of organizations can put our most powerful generally-available model, Claude Opus 4.7, to work across their codebases. Opus 4.7 is among the strongest models available for finding and patching software vulnerabilities, and for discovering complex, context-dependent issues that might otherwise be missed.

Read More - <https://claude.com/blog/claude-security-public-beta>

webdev77 - May 2, 2026, 12:03 pm

Let the immense amount of zero days grow. Gasoline poured on fire here we go.

HALx86 - May 2, 2026, 12:32 pm

The next few years are going to be wild. Companies and government will have to adopt quicker than the threat actors.

G Reviews - May 3, 2026, 2:19 am

It's fascinating how AI security tools are both a shield and a sword in this arms race. While Claude Security can help organizations find vulnerabilities faster, webdev77 makes an important point about potentially fueling more zero-day discoveries. I wonder how companies will balance deploying these powerful tools without making their own systems more attractive targets to sophisticated attackers?

webdev77 - May 3, 2026, 8:55 am

(May 3, 2026 02:19 AM)G Reviews Wrote: [\[CITE\]](#) It's fascinating how AI security tools are both a shield and a sword in this arms race. While Claude Security can help organizations find vulnerabilities faster, webdev77 makes an important point about potentially fueling more zero-day discoveries. I wonder how companies will balance deploying these powerful tools without making their own systems more attractive targets to sophisticated attackers?

By doing internal security audits against their own platforms with the same tools. If everybody on the internet is going to use Opus or GPT or whatever other model comes along, there's no reason not to integrate these tools into CI/CD pipelines to audit everything all the time. Companies that cheap out on security are accepting that they will be hacked. It's no longer an if they will be hacked. It is a certainty that companies not utilizing LLMs for security will most definitely be easy targets.

Lablear - May 3, 2026, 1:26 pm

I'm looking forward to see if this can be enabled as a mentor in the background for education and teaching, helping you learn security and write more secure code along the way