

ADVERTISEMENT



The Indian EXPRESS
JOURNALISM OF COURAGE

SUBSCRIBE

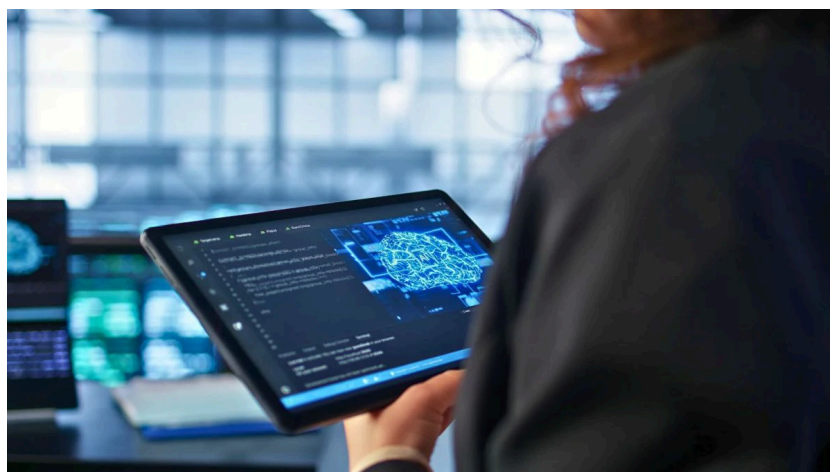
News / Business / Companies / Project Glasswing: Key cybersecurity agencies set to get access to Anthropic's Myt

Project Glasswing: Key cybersecurity agencies set to get access to Anthropic's Mythos

Discussions on to provide AI model to largest IT services companies, too

Written by: **Soumyarendra Barik**

5 min read New Delhi Jun 7, 2026 03:59 AM IST



AI model Mythos can detect critical software vulnerabilities. This matters for India as it shields vital infrastructure like banking and power, even as Anthropic battles the US Pentagon over boundaries of AI misuse. (Representational: FreePik)



US artificial intelligence company [Anthropic is extending access](#) to its closely guarded [cybersecurity initiative, Project Glasswing](#), to a select set of organisations in India, including key government entities that are responsible for safeguarding cybersecurity across sectors like banking, telecom, and power, *The Indian Express* has learned.

Government agencies such as the Indian Cyber Crime Coordination Centre (I4C); Indian Computer Emergency Response Team (CERT-In); National Critical Information Infrastructure Protection Centre (NCIIPC); and the Department of Telecommunications' Digital Intelligence Platform (DIP) are among the state-owned entities that are understood to have received access to [Anthropic's advanced frontier AI model Mythos](#).

Anthropic is also said to have extended access to some cybersecurity-focused research institutions in India, while discussions are underway on providing Mythos Preview to dedicated cybersecurity and AI teams within some of the country's largest IT services companies, a senior government official said on condition of anonymity.

Also Read | [What is Claude Mythos, and why is Anthropic limiting its rollout?](#)

This move comes as part of Anthropic's announcement that it would expand Project Glasswing beyond its initial cohort of participants in the US and UK to more than 15 countries, including India.



Under the programme, vetted organisations are granted access to Claude Mythos Preview, an unreleased AI model that Anthropic says is capable of identifying critical software vulnerabilities at a level that could fundamentally alter the balance between cyber attackers and defenders. The company has so far restricted access to the model, citing concerns that its capabilities could be misused if released publicly.

The official added that NCIIPC, which falls under the National Security Advisor in the Prime Minister's Office, and CERT-In had requested access to Mythos to identify vulnerabilities within India's critical infrastructure such as banking and power. The Indian Express had earlier reported that the Indian government was in conversations with



Also Read | Anthropic launches Project Glasswing to test advanced AI for cybersecurity

“Following several weeks of close collaboration with our Project Glasswing partners, the security industry, open-source software maintainers, and the US government, we’re extending the partnership to approximately 150 new organisations. Each one will need to meet our security requirements before they gain access... The organisations in this new group are based in more than 15 countries, and most provide critical infrastructure to many more,” Anthropic said in a blog post.

STORY CONTINUES BELOW THIS AD

The new entities with which it is planning to share Mythos Preview operate in industries such as power, water, healthcare, communications, and hardware, Anthropic said. And many of the new partners are vendors – companies or non-profits that maintain codebases that are relied upon by lots of other organisations around the world, including governments.

EXPLAINED**Firewalling systems**

AI model Mythos can detect critical software vulnerabilities. This matters for India as it shields vital infrastructure like banking and power, even as Anthropic battles the US Pentagon over boundaries of AI misuse.



along with IT Minister Ashwini Vaishnaw to assess risks posed by the powerful model to the country's banking sector.

Also Read | Anthropic blunder exposes 2,000 lines of Claude Code's internal source code: What it reveals

During the meeting, the banking sector was asked to take pre-emptive steps to safeguard their systems from the AI model. Sitharaman directed the Indian Banks' Association (IBA) to develop a coordinated institutional mechanism to respond swiftly and effectively to any such threat. She also directed banks to engage the best available cybersecurity professionals and specialised agencies "to continuously strengthen the defensive and monitoring capabilities of the banks".

Also Read | Anthropic's Claude can now use your computer like a human: Will it replace OpenClaw?

On June 4, Financial Times reported that Anthropic is helping the US National Security Agency deploy Mythos for "offensive cyber operations, embedding engineers inside the agency." FT quoted a source as saying that "Mythos would be useful for infiltrating the networks of nations such as China or Iran." This comes despite the Silicon Valley start-up's legal battle with the US Defence department, which includes the NSA.

STORY CONTINUES BELOW THIS AD

Anthropic drew a red line around Claude AI models to restrict US government's use for mass surveillance of US citizens and lethal autonomous drones. That prompted a



Last week, Anthropic filed for an initial public offering in the US that is set to value it at more than \$1 trillion.

CURATED FOR YOU

Karnataka KCET Result 2026 Live Updates: Results link active at...

Peddi Box Office Collection Day 2 Live Update: Ram Charan-starrer earns Rs...



© The Indian Express Pvt Ltd

Expand

You May Like

Sponsored Links by Taboola

Act now! Their baby's treatment can cost up to ₹10 lakhs.

Give Hope India

Donate Now

This Bengaluru techie stopped doing SIPs in 2021. Here's what happened next.

Hemant Jain

Learn More

Gold Is Surging in 2026 — Smart Traders Are Already In

IC

Learn More

Mountain Gear for Extreme Conditions

Trek Kit India

Learn More

