Frontier AI

AI-Accelerated Exploitation Has Arrived

⚠ CRITICAL THREAT

ACTIVE • AI ACCELERATED • GLOBAL

NETSYNC

AI-ACCELERATED EXPLOITATION HAS ARRIVED

What Claude Mythos and frontier cyber models mean for patch management at scale.

For years, cybersecurity leaders have relied on a simple assumption: when a critical vulnerability is disclosed, there will be time to evaluate the risk, test a patch, and deploy a fix before attackers can weaponize it.

That assumption no longer holds.

Frontier AI models have crossed a threshold that fundamentally changes the economics of cyberattacks. Vulnerability research, exploit development, and attack execution can now occur at a speed that outpaces traditional security operations. The gap between disclosure and weaponization—once measured in weeks or months—is now measured in hours.

Attackers are no longer constrained by human speed. Most enterprise patch programs still are.

Legacy patch programs were built for a human-paced threat landscape. Today's adversaries are increasingly operating at machine speed.

THE SHIFT

MONTHS TO HOURS

Time-to-exploit for known vulnerabilities. *Verizon 2026 DBIR*

32.1%

of exploited CVEs weaponized on or before disclosure — zero warning. *VulnCheck*

7 DAYS

Mean time-to-exploit in 2025 — attackers were active before a patch existed. *Mandiant M-Trends 2026*

HOURS

Oracle EBS and React2Shell weaponized within hours of disclosure. *Cisco Talos*

WHAT CHANGED

Anthropic's **Project Glasswing** — with Cisco, AWS, Microsoft and CrowdStrike as launch partners — was formed after Anthropic observed that its frontier model, **Claude Mythos**, reached a level of coding capability surpassing all but the most skilled human researchers at finding and exploiting software vulnerabilities.

Anthropic states that within **6–12 months**, other AI developers are expected to reach Mythos-class capability — potentially without the safeguards Anthropic built into its platform.

Cisco, a named Glasswing partner, summarized the challenge clearly: "The old ways of hardening systems are no longer sufficient."

This is not a future risk. It is the current operating environment.

10,0000+

High- and critical-severity flaws Mythos has already surfaced that scanners missed for years.

6–12 MONTHS

Until Mythos-class capability is expected to reach other AI developers.

NETSYNC

For more on Netsync CyberSecurity, contact us at info@netsync.com and see us online at netsync.com/cybersecurity/

WHY EVERY UNPATCHED SYSTEM IS NOW A BOARD ISSUE

For the first time in 19 years, vulnerability exploitation has overtaken stolen credentials as the leading breach entry point.

The exposure is no longer a single CVE, a single zero-day, or a single threat actor. The exposure is the growing mismatch between attackers operating on an hourly clock and patch programs operating on a monthly one.

Every unpatched server, unsupported device, delayed firmware update, and aging application now represents a potential entry point that AI-assisted adversaries can discover, prioritize and exploit at unprecedented speed.

Cybersecurity leaders are no longer being measured by whether they can detect threats.

They are increasingly being measured by how quickly they can remove exposure.

THE REAL EXPOSURE - TECHNICAL DEBT

Frontier AI doesn't need to discover a new vulnerability to create risk.

It simply needs to find the vulnerabilities you haven't patched yet.

Unpatched, end-of-life and long-tail infrastructure represent the attack surface AI-augmented adversaries are best equipped to exploit at scale.

53% High- and critical-severity flaws Mythos has already surfaced that scanners missed for years.

261 DAYS High- and critical-severity flaws Mythos has already surfaced that scanners missed for years.

46% High- and critical-severity flaws Mythos has already surfaced that scanners missed for years.

44% High- and critical-severity flaws Mythos has already surfaced that scanners missed for years.

> The math is **structural, not cyclical**. Attackers now operate on a clock measured in hours. Most enterprise patch programs still operate on a clock measured in months. That mismatch — not any single CVE — is the actual risk.

THE NEW STANDARD - PATCH AT MACHINE SPEED

Cisco's own Glasswing commitment establishes the new operational standard:
Accelerate patch testing and deployment. Harden default configurations. Enforce MFA and least-privilege access. Reduce the gap between discovery and remediation as a standing capability measured in hours, not weeks.

Cisco is embedding these capabilities into **Catalyst Center**, **ISE** and **SD-WAN Manager**, while **Cisco Live Protect** is specifically designed to bridge the critical window between disclosure and patch deployment.

THE NEW QUESTION

Can we deploy a validated fix across our entire environment inside a six-hour window when it matters?

Most organizations cannot answer yes.

And that answer is quickly becoming one of the most important indicators of cyber resilience.

HOW NETSYNC HELPS

1 **Technical Debt & Exposure Assessment**
A complete inventory of unpatched, end-of-life and Smartnet-lapsed Cisco assets across your environment, prioritized by exploitability rather than CVSS score alone.

2 **Patch Orchestration at Scale**
Deployment and validation across Catalyst Center, ISE, SD-WAN Manager and multi-vendor environments engineered to compress remediation cycles from weeks to hours.

3 **Zero Trust Containment**
Cisco Secure Access, Duo and AI Defense solutions designed to reduce blast radius and contain exposure while remediation efforts are underway.

4 **24×7 Managed Detection & Response**
Continuous monitoring and threat detection that identifies and addresses exposure windows before AI-augmented adversaries can exploit them.

5 **AI Defense for Your Own AI Agents**
As organizations adopt AI-driven automation, Cisco AI Defense helps secure MCP-connected tools, coding assistants and agentic workflows operating within the enterprise.

DON'T WAIT FOR THE HEADLINES

Mythos-class capability is expected to reach other AI developers within the next 6–12 months. The organizations that succeed in this new threat landscape will not necessarily be those with the most security tools.

They will be the organizations capable of identifying, validating and deploying remediation at machine speed. The question is no longer: "Are we vulnerable?"

The question is:
"How quickly can we eliminate exposure before AI finds it first?"

Book a Technical Debt & Patch-Velocity Assessment

Contact your Netsync Account Manager or email info@netsync.com

NETSYNC

Netsync Network Solutions is a premier IT solutions provider focused on helping public and private organizations architect, deploy, and support complex technology initiatives. As a top-tier Cisco 360 Partner spanning Enterprise Networking, Security, Data Center, Cloud, Collaboration, Managed Services, Customer Experience, and Optical/WAN, Netsync also maintains elite partnerships with AWS, HP, Intel, and other leading technology manufacturers. Backed by deep technical expertise and a customer-first approach, Netsync has earned industry recognition for delivering scalable solutions and exceptional customer satisfaction.

Netsync Corporate HQ
2500 West Loop South
Suite 410
Houston, TX 77027
sales.netsync.com
Tel: 713.218.5000
Fax: 713.664.9964

Netsync Dallas
2304 Tarpley Road
Suite 114
Carrollton, TX 75006

Netsync Austin
Netsync San Antonio
Netsync McAllen
Netsync El Paso

Netsync Long Beach
Netsync Tampa
Netsync Chicago

Learn more about Netsync at netsync.com and on our social channels.