Heimdal CEO: AI labs can choose their pace, defenders can't

Jesper Frederiksen argues that slowing frontier AI won't slow attackers, so the discipline has to come from security teams.



LONDON, UNITED KINGDOM, September 30, 2026 / EINPresswire.com/ -- Slowing frontier AI won't slow attackers, and defenders can't choose their pace, argues Heimdal CEO Jesper Frederiksen in a response to Anthropic CEO Dario Amodei's essay on pacing AI development. He ties the debate to the EU Cyber Resilience Act (CRA), whose vulnerability reporting rules took effect the day before the essay appeared.

In the article, "Slow is a design principle, not a delay," Frederiksen notes that two developments landed one day apart. On September 11, the CRA's reporting obligations came into force. Manufacturers of products with digital elements must now send an early warning within 24 hours of learning about an actively exploited vulnerability, and a fuller notification within 72 hours.
On September 12, Amodei published his essay. Most security teams use these products rather than make them, but the new clock now runs on the vendors they depend on.

Frederiksen sees two responses to the same problem from very different directions: technology is moving faster than our ability to understand, test, and control it.

"Slowing the frontier won't slow attackers," said Jesper Frederiksen, CEO of Heimdal. "They're already working with open-weight models, commercial APIs, and freely available orchestration tools. The labs can choose their pace. Defenders don't get that choice, which is why the discipline has to come from us."

Why defenders bear the gap

Frederiksen points to an asymmetry in failure tolerance. An attack agent that succeeds occasionally is still effective when it can make thousands of low-cost attempts. A defensive agent that's wrong even 10% of the time, to take an illustration, risks isolating the wrong device, revoking legitimate credentials, or flooding teams with false positives. Better evaluations, clearer model behavior, and stronger controls are defender requirements more than attacker ones.

Pacing is already security practice

Most of the pacing debate exists in security engineering under other names, the article argues: independent evaluators are separation of duties, capability gates are change control, staging comes before production, and consequential actions get the four-eyes principle.

How Heimdal approaches AI-enabled defense

Frederiksen outlines three principles:
- Assisted versus autonomous: Customers should know when AI is recommending and when it is acting.
- Customer control over consequential actions: Isolating hosts, revoking credentials, and granting elevated privileges should follow the customer's own judgment on automation versus human approval.
- Transparency on inference: Customers should know which model providers are involved, which regions are used, and what customer data leaves the environment.

"AI amplifies whoever has the data and the discipline to use it well," Frederiksen added. "It amplifies everyone else's mistakes just as fast."

The full article is available at: https://heimdalsecurity.com/blog/ai-pacing-cybersecurity-defense/

About Heimdal
Heimdal is a global cybersecurity provider delivering a unified security and compliance platform that brings together prevention, detection, and response across endpoint, identity, email, network, and access security.

With more than 12 fully integrated products protecting over 4 million endpoints, Heimdal helps enterprises and MSP partners reduce risk, strengthen operational resilience, and consolidate their security stack. Trusted by more than 20,000 organizations and 2,000 MSPs in more than 40 countries, Heimdal's platform helps prevent threats, detect breaches, and automate response without the need for a SIEM or multiple point solutions.

Danny Mitchell
Heimdal Security
+44 7999 498241

email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/946338060

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.