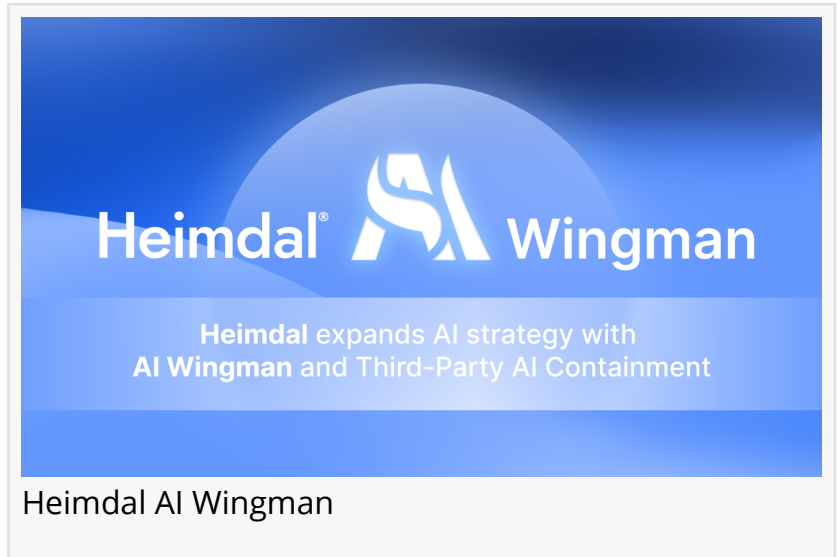


Heimdal Expands AI Strategy with AI Wingman and Third-Party AI Containment

New AI Wingman layers for guidance, investigation and SOC acceleration, plus Third-Party AI Containment, help customers use AI safely and defend faster.

COPENHAGEN, DENMARK, April 21, 2026 /EINPresswire.com/ -- [Heimdal](#) today unveiled the next phase of its AI strategy, expanding AI Wingman with three new layers - Assist, Triage and SOC - alongside the introduction of Third-Party AI Containment.



Together, these capabilities build on Heimdal's existing AI-powered protection and give organisations a clearer way to manage AI safely, speed up investigations and strengthen defence as the threat environment becomes faster, more automated and harder to contain.

Recent developments around frontier models have sharpened a question many CISOs are now being asked: what happens when attackers gain access to a new step-change in capability?

Heimdal's view is that the answer is not another standalone assistant bolted onto the edge of the stack. It is AI built into the platform itself, where the data, control layers and response workflows already sit.

One umbrella, three layers, plus containment

AI Wingman is Heimdal's umbrella for how AI is being brought into the platform. Its purpose is simple: help customers get value faster, make better decisions and strengthen security operations over time.

It breaks into three practical layers, which, together with Third-Party AI Containment, will roll out in stages across 2026:

1. AI Wingman Assist

The platform guidance layer. It helps customers use Heimdal better, understand what they are seeing, apply best-practice settings and get faster value from setup through day-to-day operation.

2. AI Wingman Triage

The investigation support layer, powered by Heimdal's multi-agent engine. It helps teams assess suspicious signals faster, validate what is real and move more quickly to the right next step.

3. AI Wingman SOC

The managed service layer brings AI acceleration into Heimdal's SOC, helping analysts investigate faster, prioritise better, and cut defensive response time for managed SOC customers. The initial release covers 15 SOC-relevant protection features across the platform (including network firewall telemetry) and is expected to reduce L1 triage time by around 25%.

Third-Party AI Containment

Heimdal's current answer to unmanaged AI use in the business. It uses existing control layers and supporting capabilities to improve visibility into shadow AI, reduce unmanaged exposure, limit unsafe actions and lower data leakage risk.

These capabilities sit alongside Heimdal's existing AI-powered protection, including its patented AI and ML-based DNS capability and AI-powered email fraud protection, as well as wider work on AI-enhanced investigation, automation and defensive workflows.

Why now?

The pace of change is no longer gradual.

Customers are now dealing with two pressures at once. AI is showing up inside the business faster than policies and controls can keep up, while attacks are becoming faster, more automated and more capable. That means security teams need a clearer answer on both sides of the challenge: how to govern AI safely inside the organisation, and how to use AI to investigate and defend faster.

"Heimdal's AI strategy is about practical advantage, not theatrics," said Jesper Frederiksen, Chief Executive Officer at Heimdal. "Customers need clear visibility, tighter control and the ability to make decisions in minutes rather than hours as AI starts to change both how organisations operate and how they are attacked. Our focus is to help them use AI safely, move faster defensively and get more value from one unified platform."

"We have moved well beyond AI as a productivity add-on," said Morten Kjaersgaard, Founder and Chairman of Heimdal. "The real question now is how customers govern it, contain it, investigate

faster with it and defend against what comes next. AI is only as strong as the foundation underneath it. That is why we are building it into the core of our platform, not bolting it onto the edge.”

Availability

The new AI Wingman layers and Third-Party AI Containment will arrive in stages throughout 2026, with some capabilities launching independently before being brought together more fully over time.

For customers, partners and MSPs, the takeaway is simple: AI now sits on both sides of the security equation. A modern security platform needs to help govern it, contain it and use it to defend faster.

To learn more about Heimdal’s AI direction, join our upcoming reveal [webinar](#). For partner enquiries, email us [here](#).

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 and over 17,000 customers worldwide, Heimdal helps enterprises and MSP partners reduce risk, strengthen operational resilience and consolidate their security stack.

Organisations in more than 40 countries rely on Heimdal’s platform to prevent threats, detect breaches and automate response without the need for a SIEM or multiple point solutions.

For more information, visit Heimdal.

Daniel Mitchell
Heimdal Security
+44 7999 498241

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

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.