

Heimdal AI Containment

Discover AI usage. Restrict unauthorized activity. Reduce exposure.

Solution Brief

INTRODUCTION

AI tools are outpacing security policy: desktop assistants, autonomous agents, browser platforms, and developer tools slip in with little IT visibility, exposing sensitive data and IP.

EU AI Act Article 14 human oversight rules for high-risk AI apply from 2 December 2027 (Annex III) and 2 August 2028 (Annex I products). For financial services, healthcare, education, HR/recruitment, critical infrastructure, and public-sector organizations, governance starts with an AI inventory, an approved-tools list, and enforced restrictions on the rest.

Heimdal AI Containment discovers and contains unauthorized AI across four pillars: identify access to AI services, control what can run, break the action chain, and remove silent privilege escalation (coming soon). Application Control, AppFencing, DNS Security, and CASB identify supported AI platforms, block unapproved apps, and restrict external connectivity while preserving approved tools and suitable offline workflows. This gives security, IT, and compliance teams practical EU AI Act readiness controls within wider governance.

HEIMDAL AI CONTAINMENT AT A GLANCE*

AI Containment combines visibility and targeted enforcement across four pillars, covering different AI application types.



IDENTIFY ACCESS TO AI SERVICES

Identify and govern access to supported AI platforms to reduce unmanaged exposure and shadow AI usage.

- **CASB / DNS Security**

DNS Security's Cloud Access Security Broker (CASB) identifies supported AI platforms through DNS telemetry, categorizes cloud applications, and provides endpoint visibility and DNS-query activity.

DNS Security also blocks access to designated AI service domains, including browser-based platforms that cannot be intercepted through local process-based restrictions.



CONTROL WHAT CAN RUN

Restrict execution of AI-related applications and supporting components on the endpoint.

- **Application Control**

Blocks targeted desktop AI applications and identifiable command-line agents through executable path or appropriate publisher-based rules.



BREAK THE ACTION CHAIN

Let approved AI applications run while cutting off their external network connectivity.

- **AppFencing**

Restricts application connectivity through selective IP blocking or full network isolation, enabling local AI workloads to run without cloud access. Operates at the network level, limiting external destinations rather than inspecting individual AI actions.

KEY AI SECURITY CHALLENGES



Shadow AI adoption

Employees can access AI services and deploy applications without formal approval, creating visibility and governance gaps.



Sensitive data exposure

Unrestricted AI connectivity introduces potential pathways for corporate information and intellectual property to reach external services.



Autonomous agents

Desktop agents and command-line tools introduce execution and connectivity risks that require targeted safeguards.



Browser-based AI access

Web-only AI platforms lack dedicated local processes, making conventional application blocking insufficient.



Changing AI infrastructure

Frequent application updates and dynamic cloud endpoints complicate static execution and network restrictions.



REMOVE SILENT PRIVILEGE ESCALATION (COMING SOON)

Prevent AI-assisted actions from quietly gaining elevated rights or expanding their reach.

- **Privilege Elevation and Delegation Management (PEDM)**

AI-specific PEDM controls coming soon.

**Capabilities depend on the configured Heimdal modules, available telemetry, application characteristics, and enforcement rules.*

UNIFIED VISIBILITY AND ENFORCEMENT



Heimdal Dashboard and CASB*

Provides visibility into supported AI platforms, associated endpoints, and DNS-query volumes. Administrators can use these insights alongside application-level restrictions and DNS Security policies to address unauthorized AI activity.

**CASB requires DarkLayer Guard Endpoint (DNS-E) with Full Logging enabled to discover allowed AI-service activity.*

IMPACT AND BENEFITS



Identify unapproved AI activity

Discover supported AI platforms across managed endpoints and understand where they are being accessed.



Prevent unauthorized execution

Block selected AI applications and agents before they run, reducing exposure from unapproved software.



Limit external connectivity

Restrict specific network destinations or isolate applications entirely while preserving suitable offline AI functionality.



Address browser-based AI risks

Extend protection beyond installed software by blocking designated AI service domains through DNS Security.



Support responsible AI adoption

Apply restrictions according to application type and organizational requirements without unnecessarily prohibiting legitimate AI use.

KEY AI CONTAINMENT FEATURES



AI service discovery and visibility

DNS Security's CASB identifies supported AI platforms using DNS telemetry and provides endpoint information and query activity.



DNS-level access restrictions

DNS Security blocklists restrict designated browser-based AI services that operate without independently identifiable local processes.



Granular process blocking

Targeted rules based on executable paths or publisher information, where appropriate, prevent selected desktop applications and standalone agents from launching.



Flexible network isolation

AppFencing supports selective IP restrictions, complete traffic blocking, and IP-based exceptions to manage application connectivity.

AI CONTAINMENT ACROSS ENVIRONMENTS

Different AI tools require different enforcement methods:



Desktop applications

Block execution or restrict network connectivity.



CLI agents

Target identifiable executable processes.



Local AI models

Preserve suitable offline execution through network isolation.



Browser-based services

Restrict access through DNS Security.

AI extensions embedded within development environments may require separate administrative or IDE-level policies when individual components cannot be isolated safely.

Application paths, signatures, and cloud infrastructure can change over time. Effective protection requires appropriate rule configuration and ongoing maintenance.

CONCLUSION

AI adoption should not come at the expense of security visibility and governance. Organizations need practical ways to understand which AI services are being accessed and enforce policies across applications, agents, and browser-based platforms. With EU AI Act high-risk obligations, including Article 14 human oversight, applying from 2 December 2027, this groundwork is becoming a compliance priority as well as a security one.

Heimdal AI Containment helps businesses identify access to AI services, control what can run, and break the action chain, reducing AI-related exposure while supporting responsible adoption. AI-specific PEDM controls to remove silent privilege escalation are coming soon.



2026 Heimdal® All rights reserved. Registered trademarks and service marks are the property of their respective owners.

Embrace AI. Contain the risks.