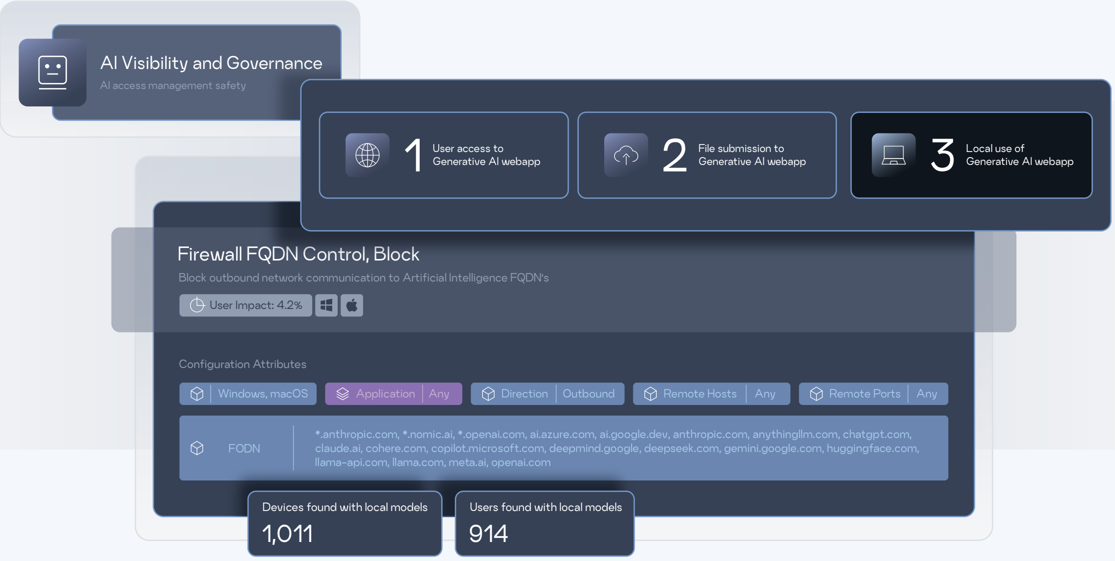
Reach

Solution Brief

Visibility and Governance of Generative AI Apps

AI Is Already Inside and You're More Prepared Than You Think



AI Visibility and Governance
AI access management safety

1 User access to Generative AI webapp

2 File submission to Generative AI webapp

3 Local use of Generative AI webapp

Firewall FQDN Control, Block
Block outbound network communication to Artificial Intelligence FQDN's
User Impact: 4.2%

Configuration Attributes

Windows, macOS	
Application	Any
Direction	Outbound
Remote Hosts	Any
Remote Ports	Any
FQDN	*.anthropic.com, *.nomic.ai, *.openai.com, ai.azure.com, ai.google.dev, anthropic.com, anythingllm.com, chatgpt.com, claude.ai, cohere.com, copilot.microsoft.com, deepmind.google, deepseek.com, gemini.google.com, huggingface.com, llama-api.com, llama.com, meta.ai, openai.com

Devices found with local models
1,011

Users found with local models
914

The challenge

Corporate leadership teams are encouraging people to increase productivity with AI, and that's putting security leaders in a difficult position. They must be enablers of innovation while also minimizing risk. From data leakage and compliance violations to intellectual property risks, the use of third-party AI applications is putting security teams into reactive mode and forcing a familiar, urgent question:

"How do we ensure our employees use AI safely, responsibly, and in line with business goals?"

Modern enterprises are navigating four primary risks associated with third party AI:

Data leakage through unvetted AI tools.

Intellectual property exposure to external systems.

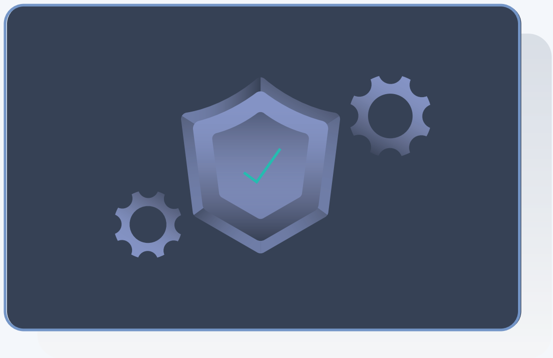
Non-compliance with data protection and privacy regulations.

Shadow AI usage that circumvents policy and governance.

reach.security

sales@reach.security

The solution



Immediate visibility and control into Generative AI App usage using existing tools

Use your existing tools to understand which applications employees are using on your network and endpoints.

Governance and control of external and local applications

Alert on and control usage to keep your company competitive, secure and compliant.

Immediate Visibility into Generative AI App usage

The foundation of any governance strategy is visibility. Enterprises need to understand:

- Which generative AI tools are being used?
- Who is using them?
- What data is being input and returned?
- Where AI activity is occurring—on the web or on local devices?

Reach connects the dots to give you a full picture of AI usage using your existing infrastructure. By integrating with widely deployed tools such as firewalls, secure web gateways, SASE/SSE platforms, EDR, and device management solutions, Reach helps security teams:

- Discover both sanctioned and unsanctioned AI applications in use
- Monitor usage trends and patterns
- Identify potential policy violations or risky behavior

Governance and control of external and local applications

Once visibility is achieved, organizations must define and enforce policies that align AI usage with business goals, security standards, and compliance requirements. With Reach, enterprises can:

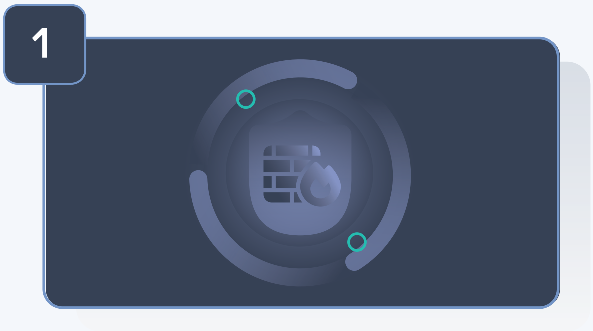
- Establish policies governing acceptable use of AI
- Enforce application-level access controls
- Define user-specific rules (e.g., developers vs. HR personnel)
- Implement controls for both web-based and local AI tools

Through policy automation and integration with corporate approval workflows, Reach ensures governance is not only effective, but also scalable.

You're More Prepared Than You Think

Most enterprises already have the necessary tools in place—they just need to activate them for AI visibility and control.

Reach connects with:



Network Security Tools

Firewalls, secure web gateways, SSE/SASE solutions

Endpoint Security Tools

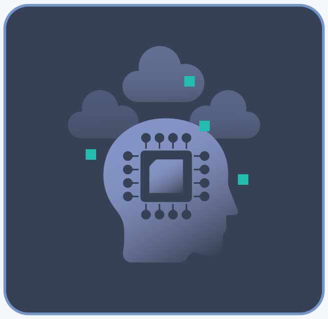
EDR, MDM, and device management platforms

This enables enterprises to govern AI usage without deploying additional agents or infrastructure.

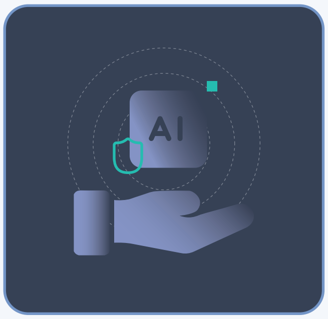
The benefits are immediate:

Accelerated time to value with no new deployments

Improved compliance through enforceable, policy-driven governance



Reduced risk by closing the AI visibility and control gap



Empower innovation by enabling safe and responsible AI usage

Getting Started with Reach

Join the companies already gaining visibility and control over Generative AI apps with Reach.

Reach.Security/try-reach.