Secure the AI You Use, Build, and Run Everywhere.

AI SECURITY SOLUTION BRIEF

AI is transforming how organizations operate, but it also introduces a new and complex attack surface. From unmanaged AI use to data leakage and model manipulation, traditional security tools are blind to the risks AI brings. Security teams must adapt to safeguard sensitive data, ensure compliance, and protect against emerging AI-powered threats.

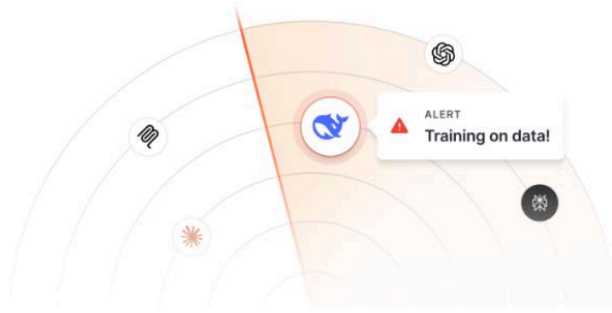
INTRODUCTION

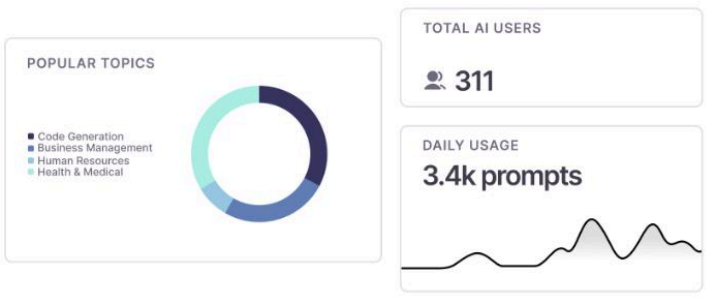
A complete solution to secure every AI interaction

Secure every AI interaction, from 3rd party AI usage to homegrown AI applications and agents. This offering leverages the industry's most advanced AI detection engine and easily integrates with any enterprise environment.

Discover Shadow AI

Identify all AI applications and models used across your organization with their associated risks. Gain visibility into hidden or unsanctioned AI use to prevent data exposure and compliance risks.



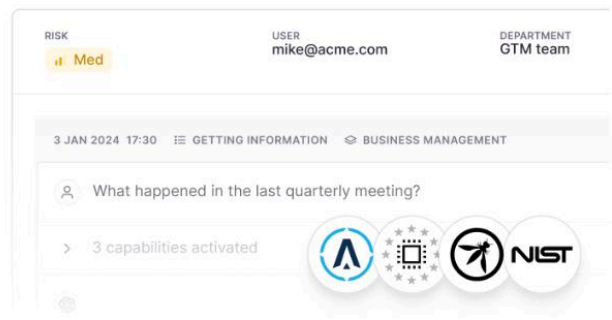


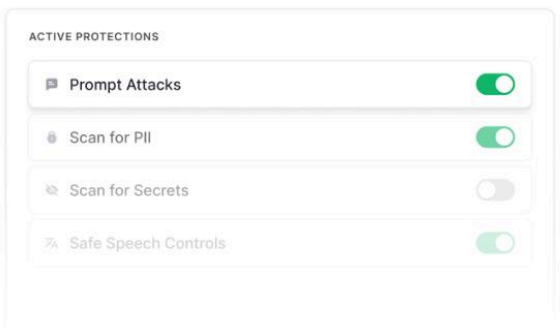
Govern and Secure AI Interactions

Monitor and control employee prompts and system interactions with AI services. Enforce security and data governance policies to prevent the sharing of sensitive information or misuse of AI outputs.

Secure the AI Developments Lifecycle

Continuously assess and harden your AI development cycles. Uncover misconfigurations vulnerabilities in models and pipelines before they reach production



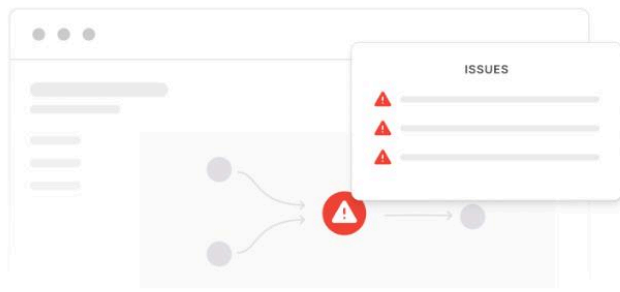


Protect Homegrown AI Applications

Detect and block attacks such as prompt injection, data exfiltration, and malicious payloads with advanced runtime guardrails - ensuring your homegrown AI applications remain trustworthy, compliant, and resilient throughout operation.

Protect AI Agents You Build and Run

Discover and assess risk in your agentic AI systems and applications and deploy cutting-edge runtime guardrails to protect them against prompt injection, data poisoning, and unauthorized access.



"The solution provides immense value to multiple stakeholders in our organization, across security, business, and legal teams. I love the fact that it secures the entire breadth of our GenAI use, no matter where it is applied."

Drew Robertson, CISO — FINANCE of AMERICA

Gartner COOL VENDOR 2025 FOR AGENTIC AI TRISM

Aim Security, now part of Cato Networks, recognized as a Gartner cool vendor in Agentic AI Risk Management.
Gartner, Cool Vendors in Agentic AI TRiSM, 2 September 2025

Contact Us