PRAGATIX PERSPECTIVE

PRAGATIX

Inside Shadow AI

A Concise Intelligence Brief

Security First AI • November 2025 Edition

Pragatix Perspective is a recurring intelligence series designed to help enterprises navigate the fast-changing landscape of AI governance, Shadow AI, and Private AI strategy.

- Security-first AI platform.
- On-prem or cloud.
- Ready to use and ready to build.
- Designed for governance.

Unmonitored AI tools can quietly erode compliance, expose data, and compromise your governance stack. This in-depth guide explores advanced Shadow AI detection and containment strategies for enterprises, with insights drawn from recent Gartner, ISACA, and Harvard research.

Enterprises are now expected to demonstrate clear oversight, auditability, and control across every AI interaction. This edition provides a practical lens on what that standard looks like in real environments, highlighting the governance gaps most teams overlook and the operational safeguards that materially reduce risk. The goal is to equip leaders with a sharper understanding of how to maintain discipline, preserve data integrity, and strengthen trust as AI continues to accelerate inside the enterprise.

See a Guided Demo of AGAT's Secure AI Platform

Why Shadow AI Has Become the New Insider Threat

Shadow AI is now recognized by enterprise security leaders as one of the fastest-growing internal risks. According to Gartner's 2025 AI Risk Report, over **72% of organizations** reported AI tools in use outside sanctioned IT policies. Employees are integrating LLMs, code assistants, and automation platforms, without formal approval, creating visibility gaps that rival those once seen in the early days of cloud sprawl.

In essence, Shadow AI is today's unmonitored AI stack, AI operating without oversight, policy enforcement, or data control.

PRAGATIX PERSPECTIVE

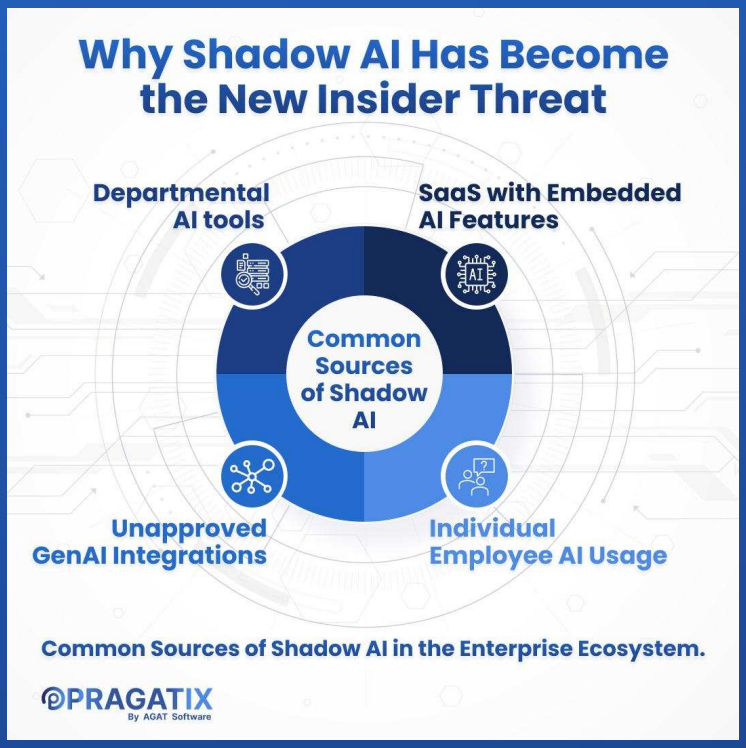
What Is Shadow AI and Why It's Growing

Shadow AI refers to the unsanctioned use of AI tools, models, and integrations that fall outside an enterprise's formal governance perimeter. This includes everything from ChatGPT-like interfaces to embedded AI in SaaS platforms used for analytics, HR, and customer engagement.

The proliferation is being driven by:

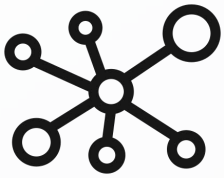
- The availability of free or consumer-tier AI tools
- Departmental AI adoption without cross-functional review
- Lack of visibility into API-based integrations
- Rapid growth of GenAI applications across workflows

As organizations accelerate AI adoption, most underestimate the non-malicious nature of Shadow AI, employees often use these tools to improve productivity or innovation.
Yet, the absence of control mechanisms exposes sensitive data and weakens compliance postures.



See a Guided Demo of AGAT's Secure AI Platform

The Hidden Risks of Unmonitored AI Tools



Data Exposure

AI models, particularly LLMs, process and temporarily store user prompts. Inputting regulated or proprietary information into third-party AI systems risks leaking confidential data.

Compliance Violations

Under frameworks like GDPR, HIPAA, and ISO/IEC 42001, organizations remain accountable for how data is shared with external AI providers, even if shared unknowingly.

Operational Drift

Shadow AI introduces inconsistent model outputs, leading to discrepancies in reporting, analytics, and automated decisions.

Governance Breakdown

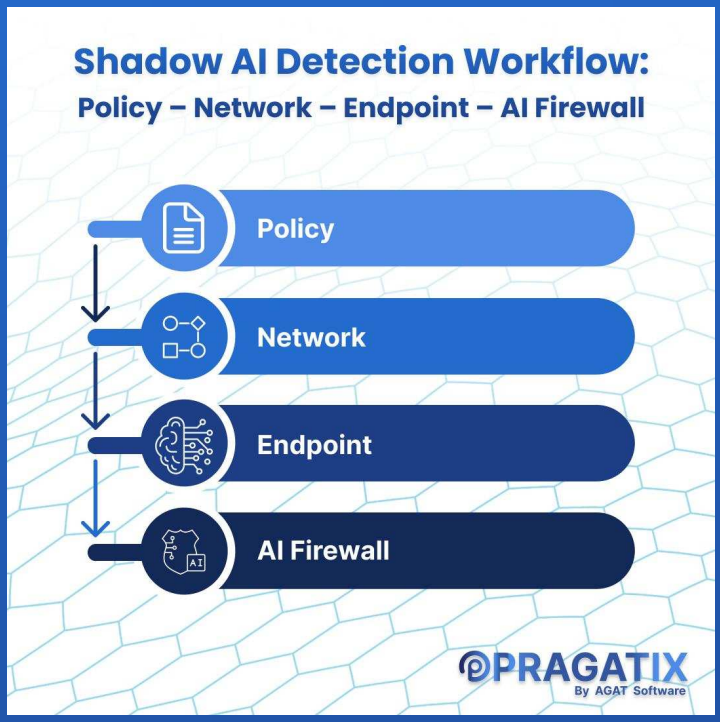
Without visibility, AI usage cannot be audited or explained. This undermines transparency, an essential principle in trustworthy AI management.

PRAGATIX PERSPECTIVE

Detection Frameworks: From Policy Gaps to Behavioral Analysis

Shadow AI detection begins with aligning internal controls with enterprise AI governance models, such as the NIST AI Risk Management Framework (AI RMF) and ISO/IEC 42001.

Step 1: Identify Gaps
Conduct an AI audit to inventory tools currently used across departments. Use network logs, app discovery tools, and policy review mechanisms to map unapproved access.



Step2: Establish Detection Protocols
Deploy real-time monitoring for anomalous AI activity:

- Pattern-based monitoring for external LLM API calls
- DLP-enabled prompts scanning
- Privilege-based AI access mapping

Step 3: Integrate AI Firewalls
Modern AI firewalls, such as those in AGAT's Secure AI Platform, provide contextual filtering, prompt governance, and visibility into cross-departmental AI usage.

Containment and Governance Strategies

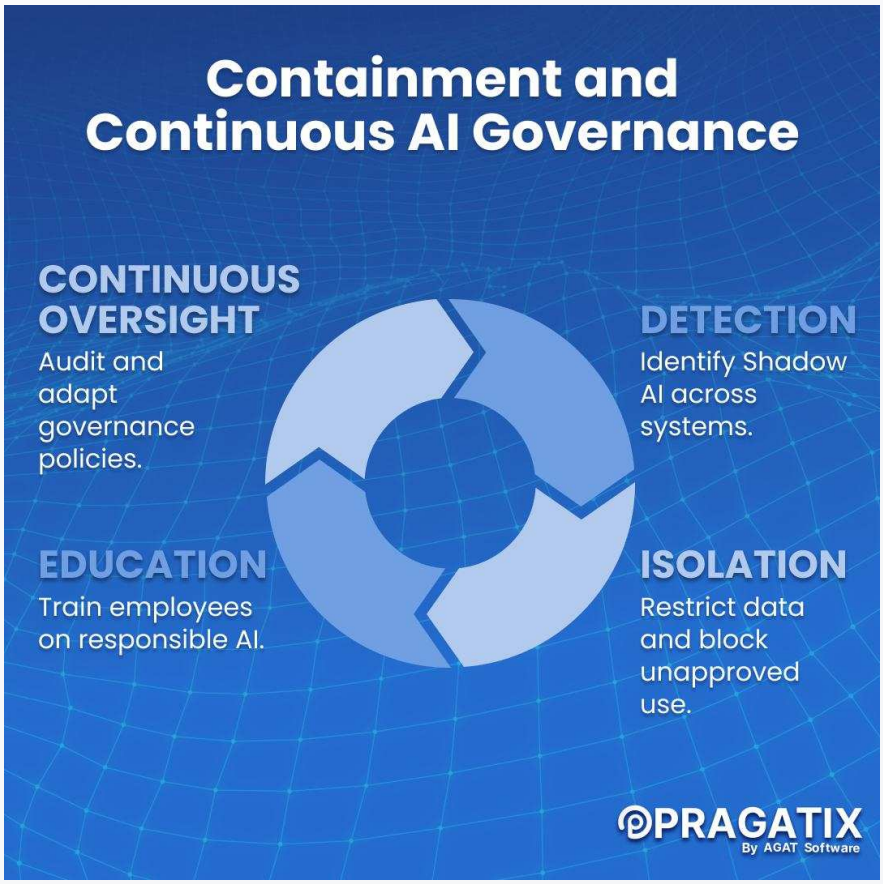
Once Shadow AI instances are detected, enterprises must transition to containment and structured governance.

Key Containment Actions:

1. Isolate Data Access: Restrict access to systems exposed via unauthorized AI use.
2. Policy Enforcement: Integrate adaptive DLP rules that automatically block sensitive prompts.
3. Educate Users: Create awareness campaigns and training sessions for responsible AI usage.
4. Centralize AI Oversight: Introduce an AI Governance Council or cross-departmental steering committee.

Governance Best Practices

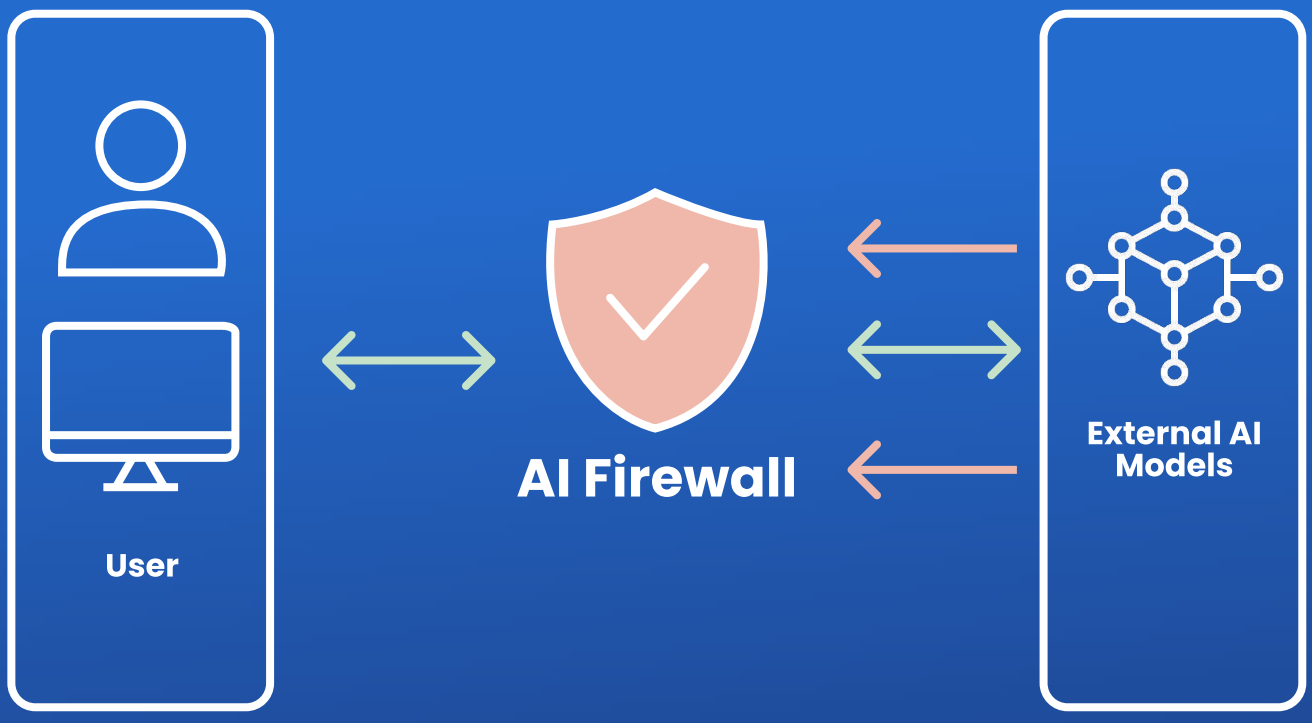
- Establish AI model approval workflows
- Mandate third-party AI risk assessments.
- Integrate continuous compliance testing (e.g., NIST AI 600-1).
- Employ internal AI agents for usage auditing.



Integrating AI Firewalls and Monitoring Systems

AI Firewalls serve as policy enforcement layers that sit between enterprise users and generative AI systems. They filter sensitive data, log interactions, and enforce compliance standards across all channels, whether web, chat, or API.

For example, AGAT's Secure AI Platform offers visibility into AI behavior across Teams, Slack, and enterprise endpoints. It applies DLP, ethical walls, and content filtering to ensure AI usage aligns with enterprise policy and jurisdictional requirements.



PRAGATIX PERSPECTIVE

Key Industry Benchmarks and Research

Recent studies from ISACA, Gartner, and Harvard Business Review emphasize the urgency of AI risk management.

- ISACA's 2025 report found that 61% of enterprises have no formal framework for governing AI usage.
- Harvard researchers highlight that data leakage from prompt injection has emerged as a leading cause of inadvertent data loss.
- Gartner predicts that by 2027, 80% of enterprises will deploy AI monitoring systems as part of digital risk management.

AI Risk and Governance Benchmarks 2025

61%
of enterprises lack a formal AI governance framework

ISACA, 2025

Data leakage from prompt injection is a top cause of unintentional loss

Harvard Business Review, 2025

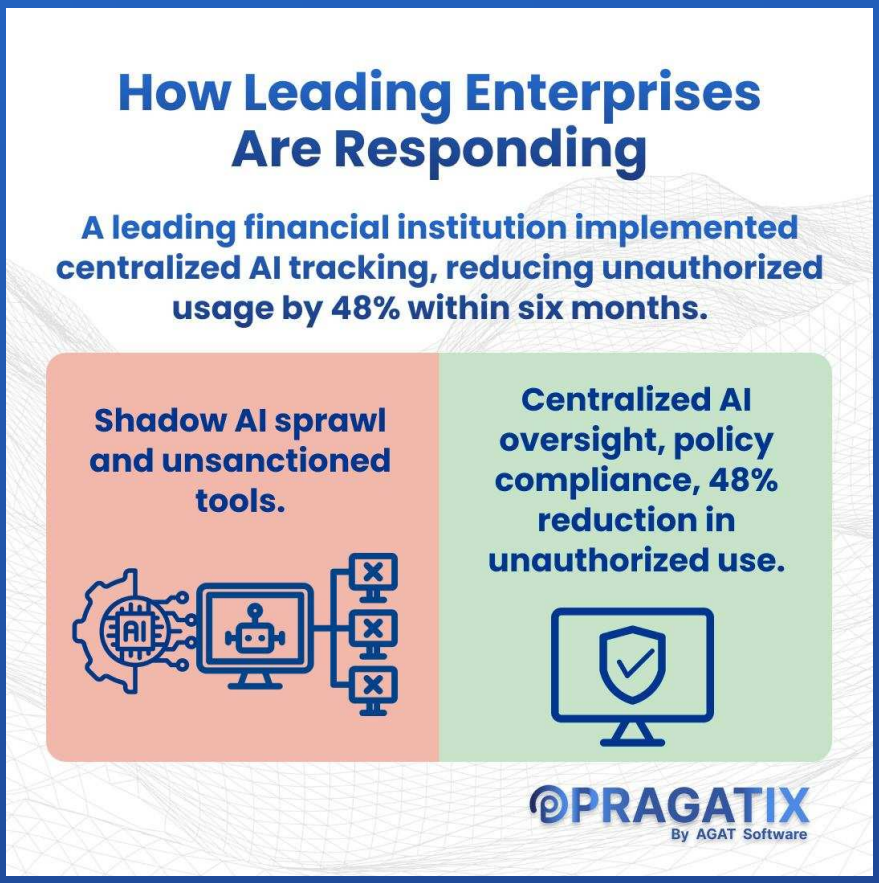
By 2027,
80%
of enterprises will deploy AI monitoring systems

Gartner, 2025

How Leading Enterprises Are Responding

Enterprises in finance, law, and government sectors are adopting Private AI strategies, integrating AI Firewalls, and deploying in-house LLMs to ensure data sovereignty.
Example: A leading financial institution implemented a centralized AI usage dashboard that tracks every prompt and enforces real-time data anonymization.

Result: Reduced unauthorized AI tool usage by 48% within six months.
Enterprises today cannot afford to let Shadow AI grow unchecked. Discover how AI Firewalls and Private AI can help you regain control.



See a Guided Demo of AGAT's Secure AI Platform

Final Thought

Shadow AI is not simply a "user problem." It is a visibility problem, a governance challenge, and a strategic risk rolled into one. Across enterprises today, AI adoption is exploding, teams are experimenting, deploying, and interacting with AI in ways IT and security teams may not even know about. Employees may be using public AI tools for drafting documents, analyzing data, or automating workflows without realizing the potential for sensitive information to leave the organization. This is the essence of Shadow AI: AI activity that exists outside the purview of formal IT, security, or compliance oversight, creating blind spots in even the most mature enterprises.

Shadow AI is also a strategic opportunity. Enterprises that fail to address it risk not only regulatory penalties and compliance failures but also the leakage of intellectual property, reputational damage, and missed opportunities to optimize AI safely. Conversely, organizations that govern AI like they govern finance, security, and people will turn Shadow AI from a risk into a competitive advantage. They will be able to innovate confidently, deploy AI rapidly, and scale AI-driven initiatives without compromising control or trust.

Addressing Shadow AI requires a holistic approach:

- Governance: Define clear AI policies, compliance guardrails, and risk thresholds aligned with regulatory requirements.
- Visibility: Implement monitoring, audit trails, and AI-native detection systems to track all AI usage.
- Control: Use private AI environments, AI firewalls, and access-based rules to ensure sensitive data stays within approved boundaries.
- Culture & Training: Educate employees on responsible AI usage, while empowering them with safe tools that enhance productivity rather than restrict it.

The enterprises that succeed will not merely react to incidents of Shadow AI. They will anticipate, manage, and optimize every AI interaction, ensuring that innovation and compliance coexist. Shadow AI is not something to be feared, it is a call to action for enterprise leaders to treat AI governance as a first-class strategic function. By seeing the invisible, understanding the flow of data, and enforcing intelligent control, companies can take back control of their AI environments and lead in a future defined by secure, responsible, and innovative AI.

PRAGATIX PERSPECTIVE

What Enterprises Are Asking

How can I identify Shadow AI in my organization?
Start by mapping unauthorized AI API calls, reviewing tool usage reports, and deploying monitoring tools that flag non-sanctioned apps.

What policies should I enforce for responsible AI use?
Adopt frameworks from NIST and ISO, mandate employee AI training, and enforce a "no external LLM use for sensitive data" policy.

How do I integrate AI governance into existing compliance workflows?
Leverage your DLP, SIEM, and IAM tools to feed into a central AI monitoring dashboard. Use adaptive policy enforcement and automated alerts.

What's the best first step for containment?
Deploy an AI firewall to detect, classify, and control data flow between internal users and AI endpoints.

How can I build trust with leadership?
Quantify AI risk exposure and benchmark improvements post-containment. Present metrics tied to compliance and data loss prevention.

See a Guided Demo of AGAT's Secure AI Platform

PRAGATIX PERSPECTIVE

PRAGATIX

Contact Us

Phone: +972-2-579-9123
Email: info@agatsoftware.com
Website: agatsoftware.com

Security First AI • November 2025 Edition