Reducing Risk of Shadow AI in the Agentic Era

A practical guide for discovering, governing, and reducing risk from unsanctioned AI and IT without slowing down the innovation your teams rely on.

pax8.com

The New Reality: AI Is Moving Faster Than Your Policies

Shadow IT has been around for years, but the rise of generative AI has changed the stakes. Employees aren't intentionally trying to bypass security—they're trying to work faster and smarter.

However, this causes potentially serious organizational risks, including:

- Employees using personal AI accounts that scrape data
- Unapproved SaaS apps tied to corporate emails
- Automations built on personal devices
- Files shared through restricted storage tools

The result is a growing attack surface that's invisible to most security teams.

Shadow AI and IT: The Insights Behind Impact

Here are a few numbers that paint the Shadow AI/IT picture:

63%

63% of organizations in 2025 lacked AI governance policies.[1]

20%

Shadow AI incidents affected 20% of businesses in 2025, increasing costs by USD $670K.[1]

97%

In 2025, 97% of organizations hit by an AI-related security incident lacked proper AI access controls.[1]

59%

59% of all employees used AI outside their company's view in 2025.[2]

The AI genie is out of the bottle, and completely shutting down its use isn't really a viable option. Instead, your goal should be to channel it so that employees stay productive and organizations stay protected.

Your Framework to Reduce Shadow AI and IT Risks

This framework provides practical guidance and steps designed for the pace of the modern workplace that any organization can adopt.

Step 1: Discover What's in Use

You can't govern what you can't see. Start by identifying:

- AI tools accessed through browsers
- Personal accounts used for work-related tasks
- Unapproved SaaS logins tied to corporate email
- File sharing tools outside of sanctioned platforms
- Personal devices accessing corporate data

Take action:

- Implement cloud app discovery systems
- Audit browser extensions across managed devices

Step 2: Assess the Risk Before You React

Not every shadow tool is an imminent threat. While some are harmless, others can leak sensitive data in seconds. The key is to evaluate each tool through a consistent lens:

- Data exposure: What could be copied, pasted, or uploaded?
- Model training: Does the tool retain prompts or files?
- Identity: What OAuth permissions does it request?
- Compliance: Does it conflict with HIPAA, SOC 2, GDPR, or client requirements?
- Operational impact: Could an automation modify or delete data?

Take action:

- Sort tools into Allow, Allow with Guardrails, or Block categories.
- Map AI usage to data sensitivity levels.
- Require SSO for AI tools and remote devices touching business data.

Step 3: Govern with Guardrails, Not Roadblocks

It's a given that employees will use AI regardless, so let's ensure they use it safely. Heavy bans only push people further into the shadows. Instead, build guardrails that are easy to understand and even easier to follow.

Create AI policies that include:

- A short, plain-language AI Acceptable Use Policy
- Clear "Do/Don't" examples for everyday tasks
- Blocking high-risk browser extensions
- Enforcing SSO for AI tools
- Logging and monitoring for AI interactions
- Data loss prevention rules for sensitive content

Take action:

- Publish a one-page AI usage guide
- Enable data loss prevention rules for AI data movement
- Block high-risk apps automatically

Step 4: Reduce Risk by Offering Better, Safer Tools

The fastest way to eliminate shadow AI is to give employees tools that are just as powerful, but secure. When people have access to AI that's fast, capable, and easy to use, there's less temptation to go rogue.

Take action:

- Replace risky tools with sanctioned equivalents
- Offer short training sessions so employees feel confident using approved AI

A Role-Driven Approach to AI Governance

Company-driven AI governance means that each group plays a different role in reducing Shadow AI and IT risk. The chart below outlines each role's focus areas and recommended actions, from executives to IT to everyday employees. Some responsibilities naturally overlap, so use this as a general framework that you can adapt to any organization's structure.

Role-Based AI Governance

Role	Focus	Actions
Executives	Business risk, regulatory exposure, and strategic alignment	Approve an AI governance charter document, provide secure AI tools, and report on AI usage patterns.
IT and Security	Identifying, access permissions, and data protection	Enable SaaS discovery, enforce SSO, deploy DLP, block high-risk extensions, and approve safe AI tools.
Managers	Productivity, team clarity, and reducing friction	Share approved AI tools, reinforce usage guidelines, and encourage safe AI experimentation.
Employees	Understanding security risks and how to use AI safely	Use approved tools, avoid sharing sensitive data, and report or request permission to use new AI tools before adoption.

Reduce Shadow AI and IT Risks with Pax8

Pax8 gives MSPs and their SMB clients a practical path to govern AI without slowing innovation. We've built an entire ecosystem of services, programs, and offerings, such as our MIP (Managed Intelligence Provider) Program and the Agentic Marketplace, to provide organizations with a repeatable framework for safely launching, scaling, and using AI.

Schedule a call

pax8.com

1. Cost of a data breach, IBM, 2025
2. 2025: The rise of the invisible colleague: Shadow AI