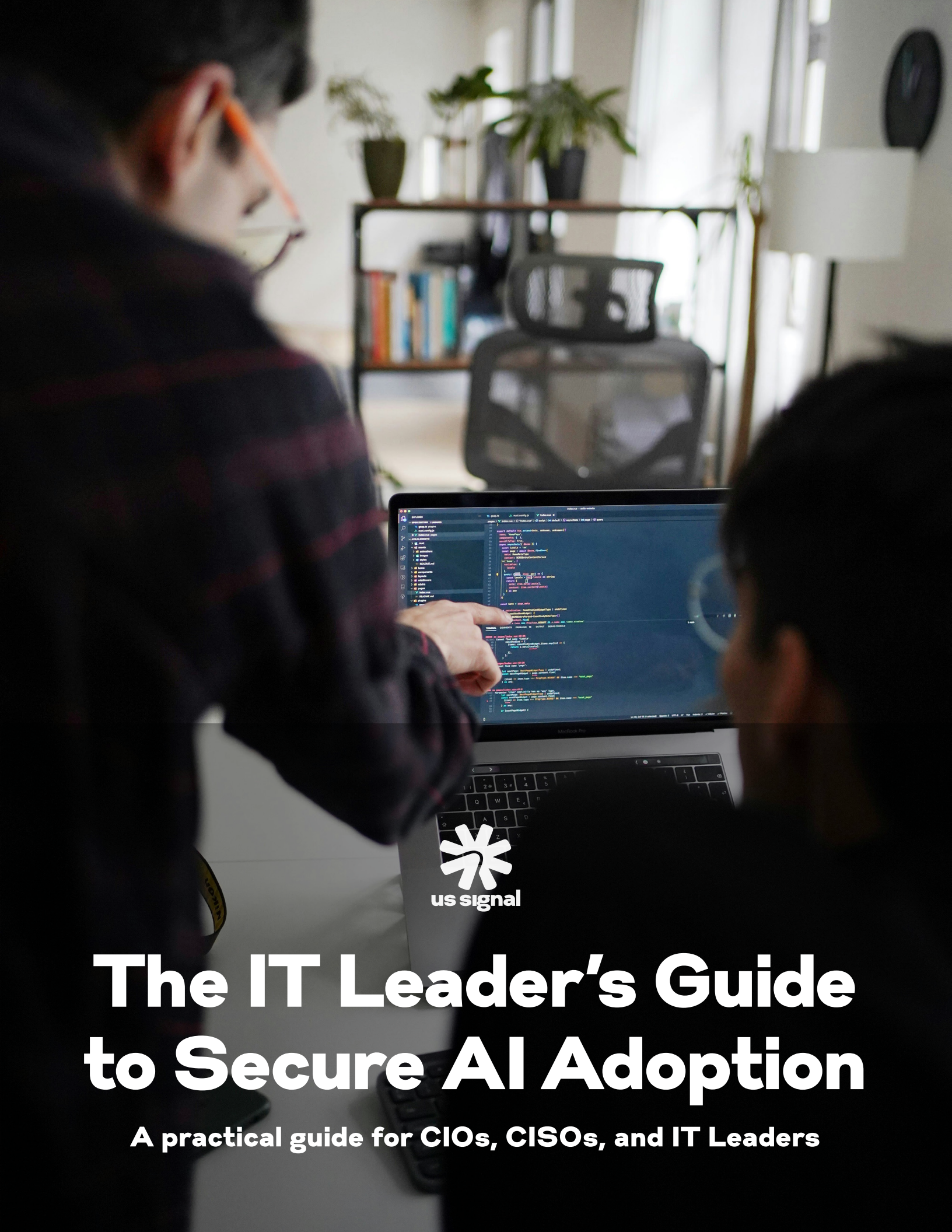


us signal

The IT Leader's Guide to Secure AI Adoption

A practical guide for CIOs, CISOs, and IT Leaders

Artificial intelligence is quickly becoming part of everyday business. Employees are using generative AI assistants to improve productivity, developers are embedding AI into applications, and organizations are beginning to explore AI agents capable of automating increasingly complex tasks.

The opportunity is significant. AI can accelerate decision-making, improve customer experiences, reduce repetitive work, and help organizations innovate faster. The challenge is that AI introduces new security and governance considerations that many organizations have never had to address before.

This guide is designed to help IT leaders understand those challenges and build a practical roadmap for secure AI adoption.

Executive Questions:

- Do we know where AI is already being used?
- What information is employees sharing with AI tools?
- Do we have an AI acceptable use policy?
- Are developers building AI applications securely?
- Could we explain our AI governance strategy to our executive team today?

Chapter 1: AI is Already Part of Your Business

For many organizations, AI adoption didn't begin with an executive initiative. It started with curiosity. Someone used ChatGPT to summarize meeting notes. A developer installed an AI coding assistant. Marketing generated the first draft of a campaign. Finance experimented with analyzing spreadsheets.

That pattern is important because it means AI adoption often happens organically before governance catches up.

The goal shouldn't be to stop employees from using AI. In most organizations, AI is already creating measurable productivity gains. The objective is to understand where it is being used, what data it can access, and how those activities align with business policies.

Reality Check

Many organizations don't have an AI problem—they have a visibility problem.

- They don't know which AI tools employees use.
- They don't know what data is being shared.
- They don't know where AI is being built into applications.
- They don't know which departments are leading AI adoption.

32% of organizations experienced attacks on AI applications leveraging prompts.

Source: Gartner



Chapter 2: Why AI Changes the Security Conversation

Traditional cybersecurity remains essential. Firewalls, endpoint protection, identity management, cloud security, and data loss prevention continue to provide the foundation for protecting modern organizations.

AI doesn't replace those investments. Instead, AI changes the way users, applications, and data interact.

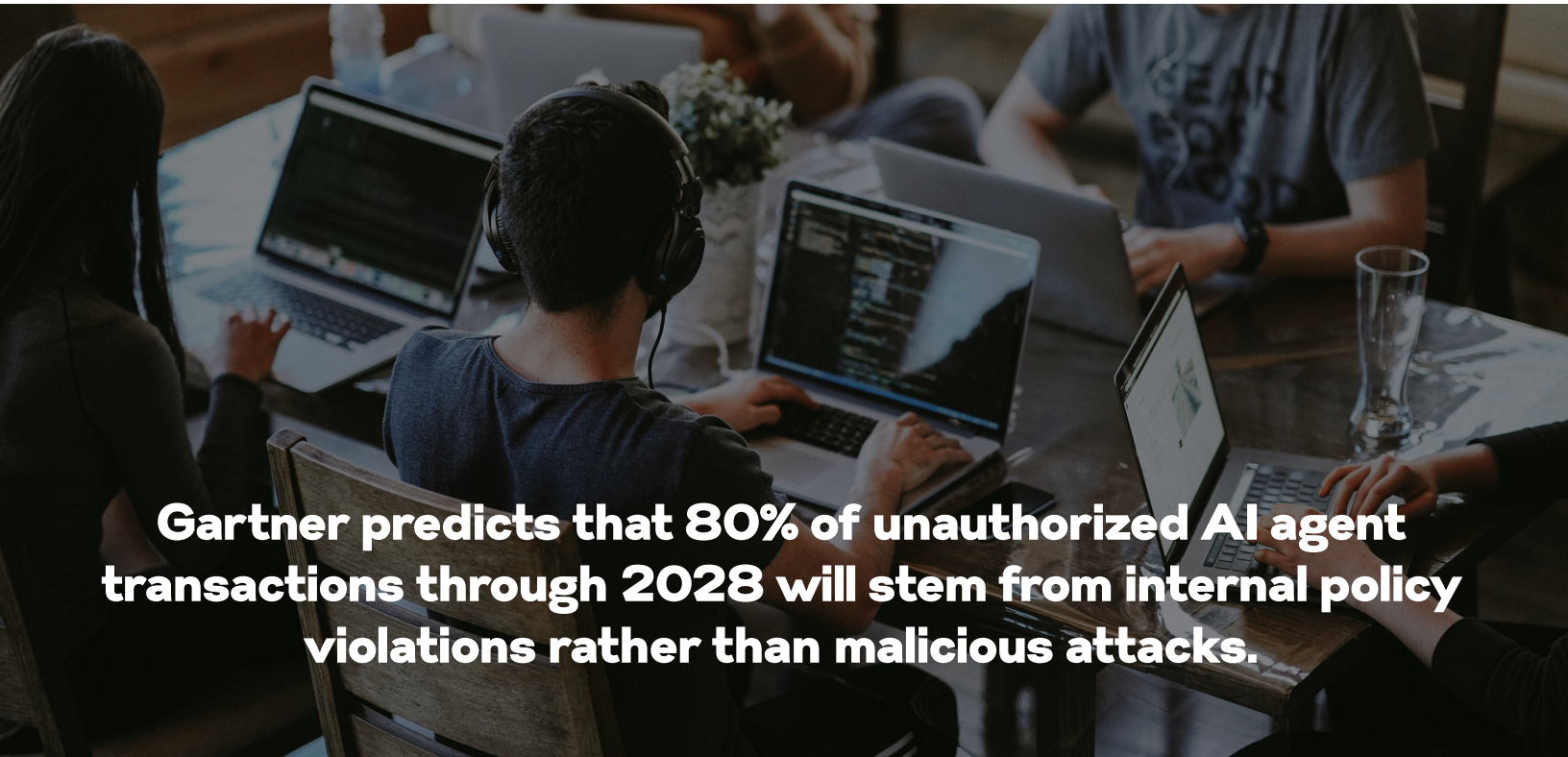
Employees now communicate with AI through prompts and conversations. Developers connect applications to large language models through APIs. AI agents are beginning to perform tasks with increasing levels of autonomy. Those interactions create new risks that require additional visibility and governance.

Myth vs. Reality

Myth: We can simply block AI.
Reality: Employees will continue looking for ways to improve productivity. Governance is more effective than blanket restrictions.

Myth: AI security replaces cybersecurity.
Reality: AI security extends existing cybersecurity investments.

Myth: AI is just another SaaS application.
Reality: AI introduces conversations, prompts, autonomous actions, and new attack surfaces.



Gartner predicts that 80% of unauthorized AI agent transactions through 2028 will stem from internal policy violations rather than malicious attacks.

Chapter 3: Four AI Security Challenges

1. Shadow AI

Employees frequently adopt AI tools before formal approval. This creates blind spots for IT and security teams. The first step toward governance is understanding what is already being used.

2. Sensitive Data Exposure

Prompts often contain customer information, financial data, intellectual property, source code, or internal documents. Organizations need policies that help prevent sensitive information from being unintentionally shared.

3. AI Applications

As development teams build AI-powered applications, security must evolve as well. AI introduces concerns such as prompt injection, model manipulation, and runtime protection that traditional application security programs were not designed to address.

4. AI Agents

AI agents can access systems, retrieve information, call APIs, and trigger workflows. Organizations need governance around what agents are permitted to do and how those activities are monitored.

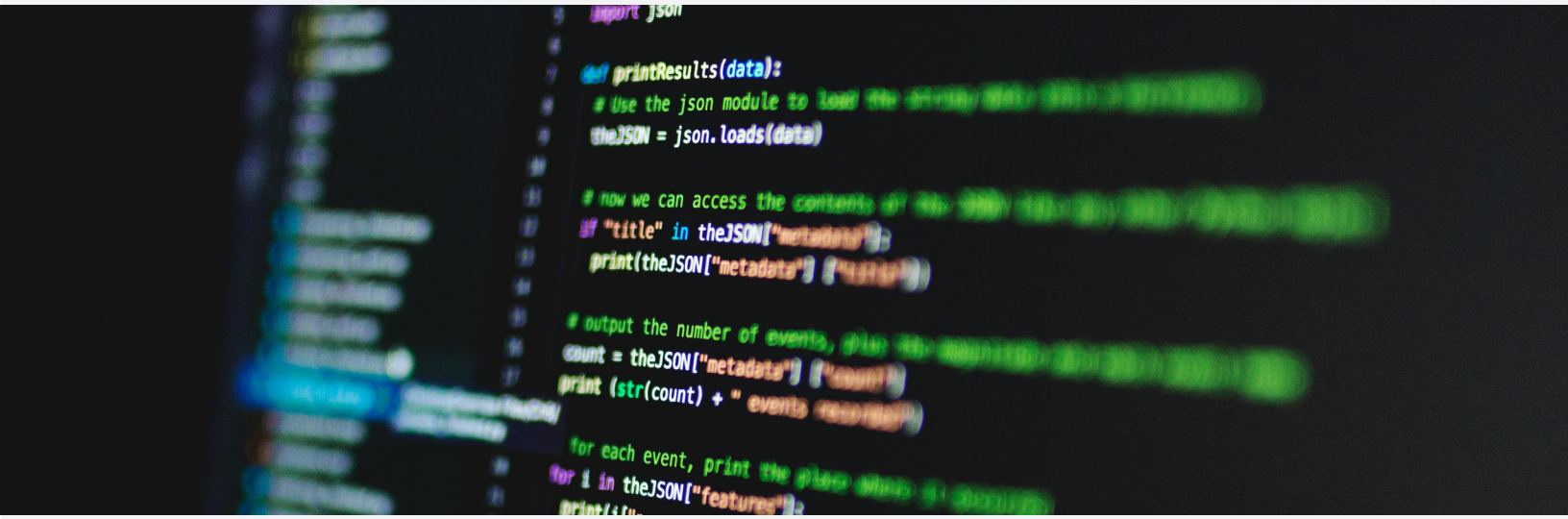
These four challenges aren’t obstacles to avoid. They’re the reasons AI governance exists. Organizations that recognize these risks early can design policies and controls that prevent problems before they happen—rather than responding to incidents after the fact. The good news is that understanding these challenges is the first step toward building a governance framework that allows your organization to move forward confidently.

Chapter 4: What Good AI Governance Looks Like

Successful organizations don't approach AI with fear. They create clear governance that allows innovation while reducing unnecessary risk.

Good governance typically includes:

- An AI acceptable use policy
- Visibility into approved and unapproved AI tools
- Policies for handling sensitive information
- Executive ownership
- Employee education
- Regular reviews of AI usage
- Monitoring and audit capabilities



Chapter 5: What to Look for in an AI Security Solution

As AI adoption grows, look for solutions that can:

- Discover AI applications across the organization
- Identify unsanctioned AI usage
- Protect sensitive information shared through prompts
- Provide visibility into AI-powered applications
- Monitor AI agents and their activities
- Apply consistent governance policies
- Produce audit-ready reporting

Chapter 6: Your First 90 Days

Organizations don’t need to solve every AI challenge immediately. Focus on building a strong foundation.

- Inventory AI usage across the organization.
- Meet with business leaders to understand AI initiatives.
- Develop an AI acceptable use policy.
- Identify high-risk data that should not be shared with AI.
- Evaluate AI governance and monitoring capabilities.
- Create an AI security roadmap aligned with business objectives

AI is not another passing technology trend. It is changing how organizations work, build software, and serve customers.

The organizations that succeed won’t necessarily be those that adopt AI first. They’ll be the ones that adopt it thoughtfully—with the right balance of innovation, governance, and security.

Secure AI adoption starts with visibility. From there, organizations can build the policies, governance, and protections that allow employees to innovate confidently.



How US Signal Can Help

Successfully adopting AI requires more than a security product. It starts with understanding how AI is being used across your organization, identifying potential risks, and establishing governance that enables innovation without compromising security. To support those efforts, US Signal delivers an AI Security solution powered by Cato Networks, extending security across the entire AI lifecycle.

Our solution helps organizations:

- Discover AI usage by identifying approved and unapproved AI applications across the organization, providing visibility into where AI is already being used.
- Protect sensitive information with inline controls that help prevent confidential data, intellectual property, source code, and regulated information from being exposed through AI prompts and interactions.
- Secure AI-powered applications by helping defend against emerging threats such as prompt injection, model manipulation, and other AI-specific attacks.
- Monitor AI agents with visibility into agent activity, API interactions, and automated workflows, helping ensure AI operates within defined policies.
- Strengthen AI governance with centralized policy enforcement, monitoring, and audit-ready reporting that supports compliance and executive oversight.

Because AI security is integrated into the broader security ecosystem, organizations gain a consistent approach to protecting users, applications, and data without adding unnecessary complexity.

Whether your organization is just beginning its AI journey or expanding AI initiatives across the business, US Signal provides the expertise and technology to help you adopt AI securely, confidently, and at your own pace.

get started now!