Microsoft 365 Copilot

Ensuring Data Security in the AI Era

A Guide for IT Leaders

E-book

This guide is written for IT leaders who need to drive AI adoption while keeping their organizations' data secure. It will help you understand the risks AI presents to data security and privacy while giving you the insights needed to lead your company's AI transformation with confidence.

Table of contents

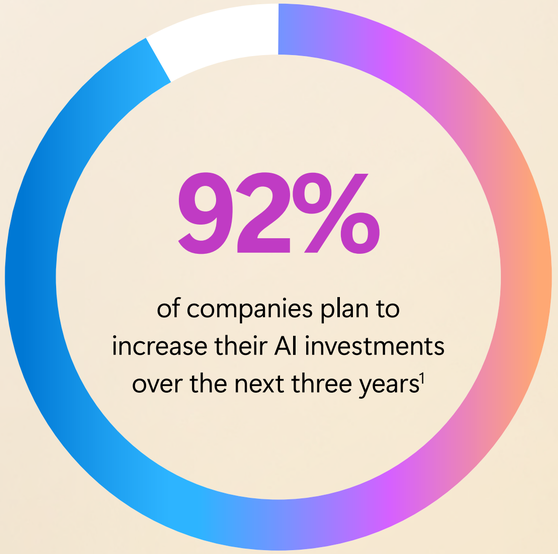
01

The new rules of AI-powered work

Generative AI is opening new doors for innovation and helping teams work faster and smarter than ever before. For forward-thinking organizations, AI isn't just another technology trend—it's a business imperative, essential to how they operate, deliver value, and sustain a competitive edge.

But this rapid adoption brings new and amplified challenges that IT leaders must proactively address and control. AI systems can actively search for and combine information across the entire data ecosystem, increasing security risks beyond traditional tools. Despite the rapid expansion of AI, only **1%** of organizations report having fully integrated AI into their workflows with proper security protocols.[1] By implementing robust security and governance measures from the start of your AI journey, your team can effectively protect sensitive data, maintain compliance requirements, and safeguard your organization's information—all while enabling innovation to flourish.

The AI adoption wave is already here



02

Understanding AI's impact on data security

Before diving into specific challenges, it's important to understand how AI fundamentally changes the data security landscape. Unlike traditional software that only accesses data when specifically instructed, generative AI actively processes, analyzes, and creates content based on all the information it receives.

This difference is significant for several reasons:

- AI tools can discover connections between data that humans might miss
- They can synthesize information across multiple sources automatically
- They can generate new content that contains elements from sensitive inputs

Your traditional security tools likely weren't designed with these capabilities in mind. While conventional software follows predictable paths when accessing data, AI can take unexpected routes through your information ecosystem, potentially exposing sensitive data in ways you haven't anticipated.

This fundamental shift requires new approaches to security and data governance that specifically address how AI interacts with your organization's information assets.

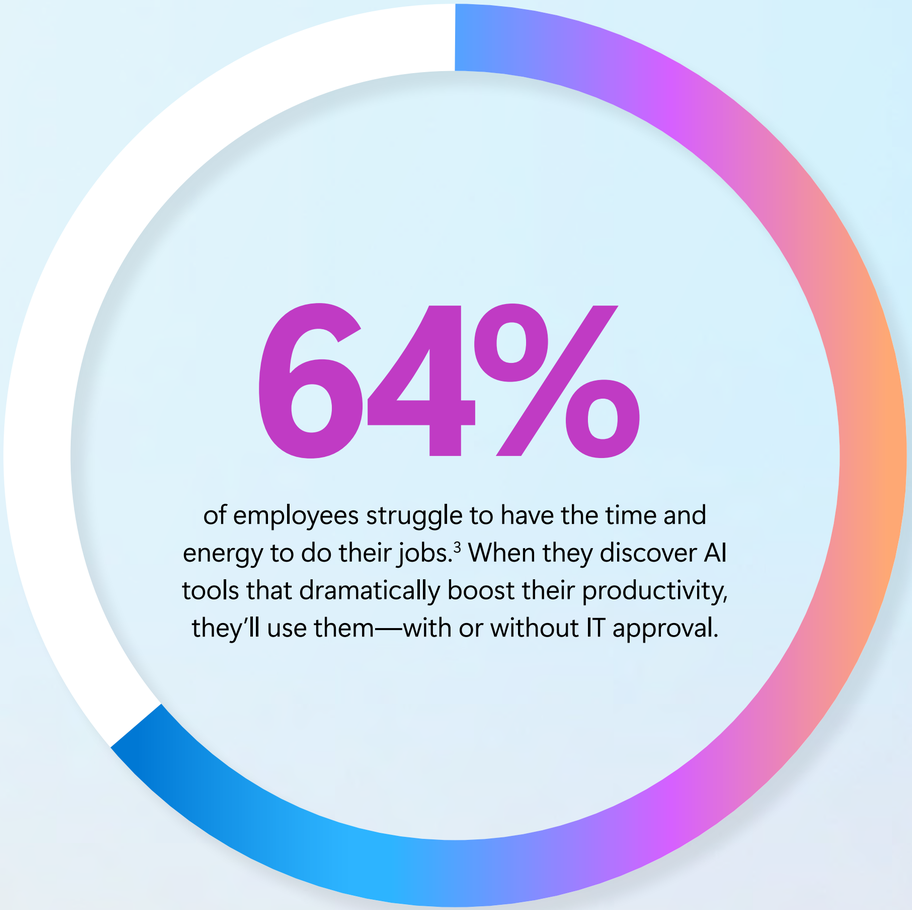
03

The shadow AI challenge

Wherever you are on your AI adoption journey, your employees are already finding their own solutions, creating what's known as "shadow AI."

This unauthorized use creates significant blind spots in your security posture. When employees share company data with external AI systems, they bypass existing security controls and create vulnerabilities that most organizations aren't prepared to address.

Shadow AI isn't just a security issue—it could be a symptom of unmet productivity needs in your organization. When employees turn to unsanctioned tools, they're signaling where your official systems aren't meeting their requirements. Addressing shadow AI requires both stronger governance and enhanced productivity solutions.



of employees struggle to have the time and energy to do their jobs.[3] When they discover AI tools that dramatically boost their productivity, they'll use them—with or without IT approval.

Why shadow AI emerges:

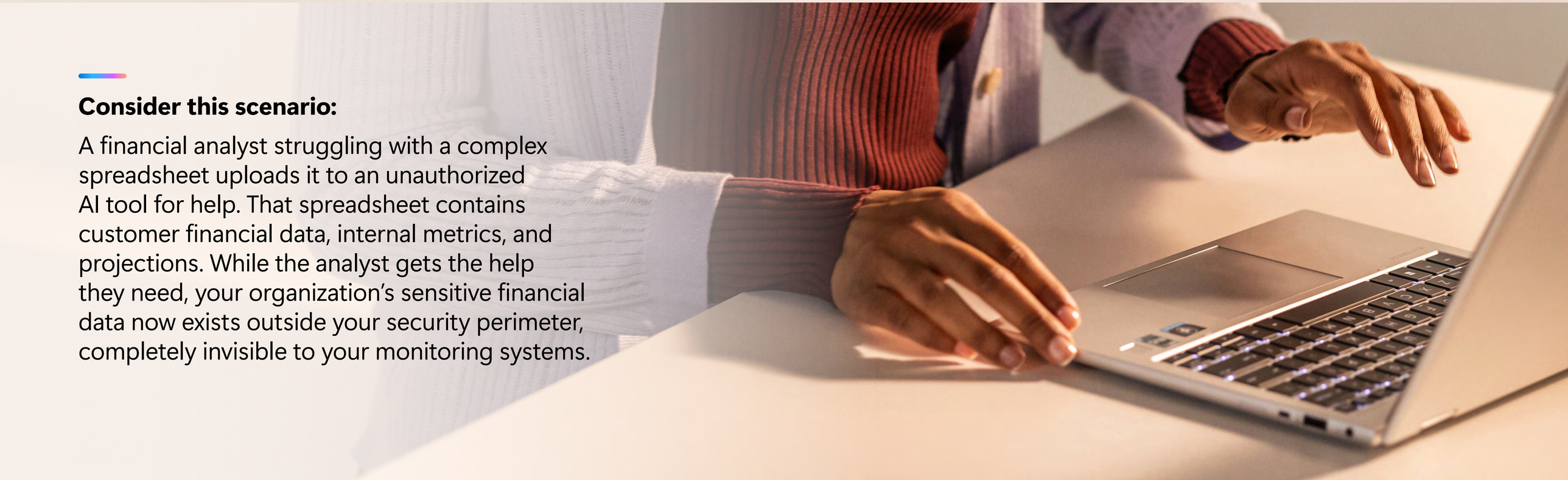
- Employees are eager to boost productivity through AI's impressive capabilities
- Daily workloads increasingly exceed available time and energy
- Teams face mounting pressure to deliver more with the same resources
- Consumer AI tools offer immediate solutions without approval barriers
- Official IT procurement processes can't match the pace of innovation

The risks of shadow AI:

- No visibility into what company data is being processed by external AI systems
- No guarantee that confidential information isn't being retained
- No consistent security standards across different AI platforms
- No auditability for compliance purposes
- No integration with your existing security infrastructure

Consider this scenario:

A financial analyst struggling with a complex spreadsheet uploads it to an unauthorized AI tool for help. That spreadsheet contains customer financial data, internal metrics, and projections. While the analyst gets the help they need, your organization's sensitive financial data now exists outside your security perimeter, completely invisible to your monitoring systems.



04

The BYOAI reality

Without clear guidance from leadership, employees are increasingly taking AI adoption into their own hands—**78%** of AI users are taking a "bring your own AI" (BYOAI) approach to work.[2] This trend is even more pronounced at small- and medium-sized companies, where **80%** of employees engage in BYOAI practices.[2]

This unsanctioned approach comes with significant downsides. Employees often keep their AI use under wraps—**52%** are reluctant to admit using AI for important tasks, and **53%** worry that using AI makes them look replaceable.[2] This secrecy not only prevents organizations from realizing the full benefits of strategic AI implementation but also creates serious security vulnerabilities in an environment where leaders cite cybersecurity and data privacy as their **#1** concern.[2]

Given the widespread usage and inevitable growth of AI, the question isn't whether to allow AI at your organization—it's how to provide a secure solution that meets your employees' needs while keeping your organization's data protected.

05

The regulatory maze

Frameworks and laws around data privacy and security create another layer of complexity when adopting AI. While some frameworks are specifically designed for AI governance, others have broader applications that still impact how you handle information—and the penalties for violations remain severe.

When your employees use AI tools without proper oversight, they could unintentionally create compliance violations. AI makes this risk greater because it can access, combine, and expose regulated information in ways traditional technologies cannot.

Key regulations affecting your AI use:

GDPR

The European Union's General Data Protection Regulation gives people control over their personal data and requires clear consent for processing it

EU AI Act

The European Union's comprehensive framework specifically designed to regulate artificial intelligence systems based on their risk levels

HIPAA

This U.S. federal law for healthcare sets strict standards for handling protected health information

NIST AI Risk Management Framework

This voluntary U.S. guidance helps organizations address risks in the design, development, and deployment of AI systems

The compliance risks with AI:

- Customer data being processed on servers outside approved regions
- Personal information being used without proper consent
- Sensitive data persisting in systems without appropriate retention controls
- No audit trail of how protected information is being accessed and used
- AI-generated content that violates sector-specific compliance requirements

These violations can lead to serious consequences:

- Large financial penalties (GDPR fines can reach **4%** of your global revenue)[4]
- Requirements to notify affected parties about data breaches
- Legal action from those affected
- Damage to your company's reputation and customer trust

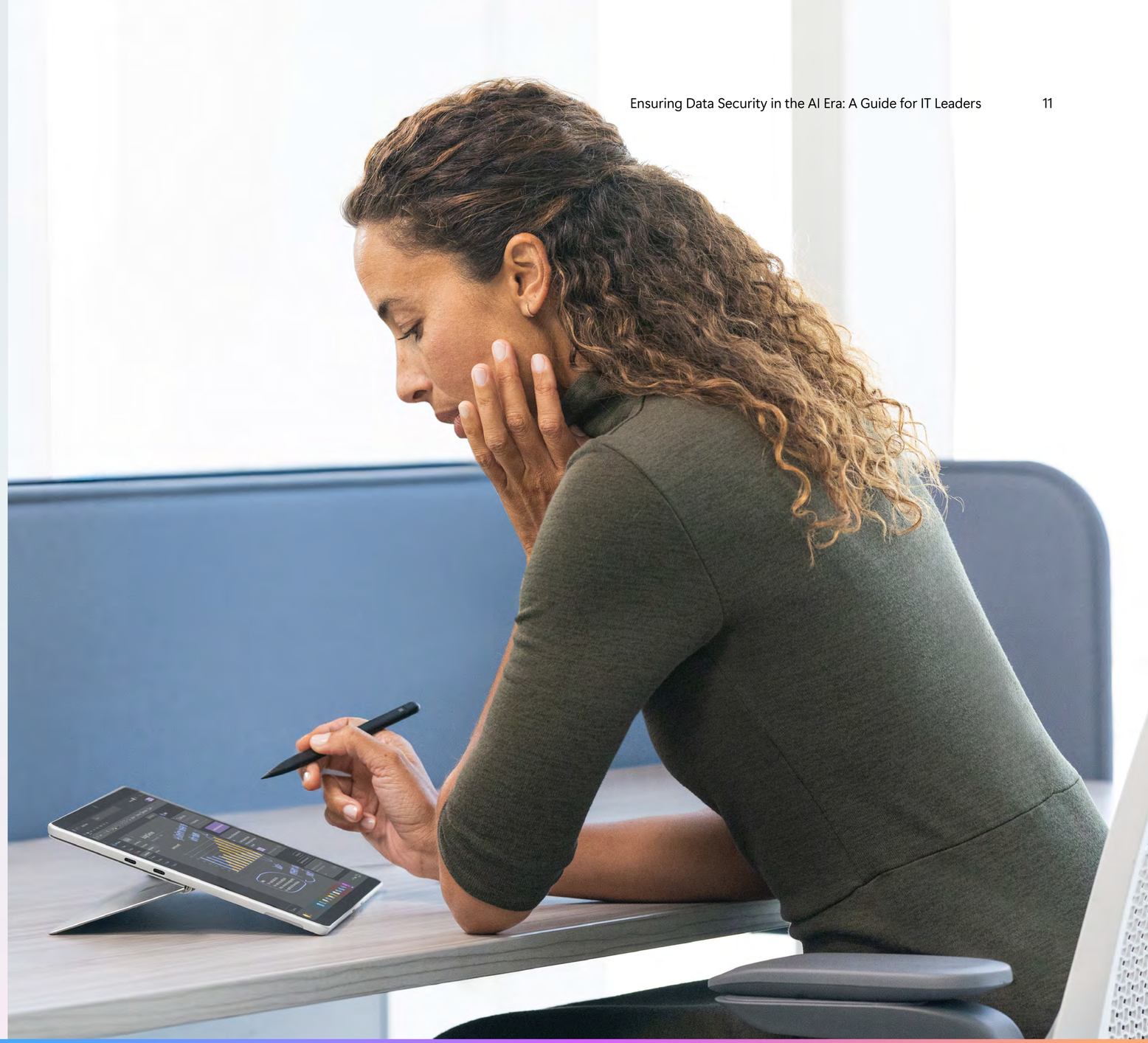
As AI use grows across your organization, you need governance that helps people work efficiently while keeping your organization compliant with the regulations that affect your business and your customers.

06

A security-first framework for evaluating AI solutions

With shadow AI, BYOAI, and regulations creating significant risks, you need a structured approach to evaluating AI solutions that ensures they can help your organization drive innovation—while also protecting sensitive data and ensuring compliance with evolving regulatory requirements.

The following framework provides six simple questions to assess whether an AI platform delivers on both fronts.



Question 1

Does it offer enterprise-grade security from the ground up?

With the right solution, your security shifts from just reacting to problems after they happen, to proactively seeking out vulnerabilities in your organization's data—before they become bigger issues.

Look for solutions that:

- Provide real-time visibility across your entire data ecosystem
- Automatically identify potential data risks before they become incidents
- Protect sensitive information at every level

Question 2

Can it easily adopt and enhance existing security controls?

Your organization's security policies should work seamlessly with AI. Your AI solution provider should respect and integrate into your existing security frameworks—not require you to create entirely new ones.

Look for solutions that:

- Seamlessly adopt your existing security policies, sensitivity labels, and information protection settings
- Apply granular access controls at the individual level, so no user has access to data they shouldn't
- Actively flag attempts to subvert access controls

Question 3

Does it include built-in governance and privacy controls?

Since AI tools work more proactively, your security measures must be proactive too. Implementing strong data governance creates clear boundaries where your employees can innovate safely without putting sensitive information at risk.

Look for solutions that:

- Centralize AI governance with automated policy enforcement across all activities
- Include early detection of potential data oversharing
- Align with regulatory frameworks to ensure compliant AI use

Question 4

Can it be deployed consistently across the entire organization?

Your employees have their own styles of working, their own schedules, and may be located all over the world. AI should benefit everyone.

Look for solutions that:

- Offer seamless setup and easy AI adoption in daily workflows
- Provide flexible access, from free AI chat to scalable agent solutions
- Help employees build AI fluency and integrate it into their work

Question 5

Does it seamlessly integrate across existing frameworks?

Your business currently operates with its own digital infrastructure of software programs, apps, and more.

Look for solutions that:

- Mesh seamlessly with your tools and programs to minimize disruption
- Provide a continuous AI experience across all apps so work can flow seamlessly between tools
- Automate and optimize tasks within existing workflows

Question 6

Are users empowered to innovate?

At its core, AI should transform how work gets done. This isn't just about automation—it's about enhancing productivity and driving innovation.

Look for solutions that:

- Turn time drains into streamlined processes
- Automate repetitive tasks
- Empower workers to reclaim time and focus on priorities

07

Microsoft 365 Copilot: AI you can trust

Microsoft 365 Copilot is the generative AI solution built to deliver robust security, governance, and access controls—ensuring secure deployment and sustained innovation. It enhances productivity with intuitive tools like Copilot Chat, which works where you do, and Copilot Studio, where your team can build custom AI agents without coding skills.

Copilot integrates seamlessly within your Microsoft 365 environment, inheriting user permissions, sensitivity labels, data loss prevention policies, and geographic data residency requirements—without extra configuration. By embedding AI in the tools your employees already use, Copilot mitigates security risks while keeping data within your trusted Microsoft 365 environment.

Microsoft's commitments ensure your organization remains in control:

- Your data is secure at rest and in transit
- Your data isn't used to train AI models
- You choose what information goes into the cloud
- You're protected against AI security and copyright risks

Purpose-built governance tools like the Copilot Control System and SharePoint Advanced Management give IT teams the visibility, controls, and audit logs needed to maintain compliance.

With Microsoft 365 Copilot, you don't have to choose between innovation and security—you can have both.

08

The secure path to AI transformation

The AI revolution presents a unique opportunity for IT leaders to deliver strategic value by balancing innovation and security.

In implementing secure AI tools like Microsoft 365 Copilot, you'll empower employees with tools for greater productivity, all while eliminating the risks of shadow AI. The path forward is about securely enabling innovation. Your leadership in secure AI adoption will position IT as an enabler of transformation, helping your organization thrive in this new era while keeping data secure and compliant.

Get started with Microsoft 365 Copilot

Sources:

[1] "Superagency in the workplace: Empowering people to unlock AI's full potential," McKinsey & Company, January 28, 2025. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2] "AI at Work is Here. Now comes the Hard Part," Microsoft Work Trend Index, May 8, 2024. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[3] "Will AI Fix Work?" Microsoft Work Trend Index, May 9, 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," European Parliament and Council of the European Union, April 27, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.