



Unlock AI Potential with Security-Led Innovation

Explore Safe and
Scalable AI Adoption

<http://www.frontrow.technology>



Executive Summary

Artificial Intelligence (AI) is revolutionizing business operations, driving efficiency, innovation, and profitability. Tools like Microsoft 365 Copilot empower organizations by automating tasks, enhancing collaboration, and delivering deep insights. However, as AI adoption accelerates, businesses must establish a strong security foundation to fully harness its potential.

By integrating AI with Microsoft's security solutions, businesses can innovate with confidence—protecting sensitive data, maintaining compliance, and ensuring responsible AI usage. This guide explores how AI and security work together to unlock unprecedented opportunities while mitigating risks such as data leaks, regulatory challenges, and governance gaps.

The Rise of AI in Business

AI's Role in Digital Transformation

From automating repetitive tasks to uncovering valuable insights in business data, AI is becoming embedded in every aspect of work. It's transforming how companies operate, enhancing collaboration, streamlining workflows, and driving smarter decision-making. As AI continues to evolve, businesses that embrace it strategically will gain a competitive edge, improving efficiency and innovation across industries of all sizes.

The Productivity and Profitability Impact

According to Microsoft's FY25 Q1 Earnings Conference Call ¹, 70% of Fortune 500 companies have used Microsoft 365 Copilot to reimagine work. Additionally, the *First Annual Generative AI Study*, 51% of respondents reported productivity gains of over 10% from using generative AI.³ These early results highlight the growing impact AI is having on business performance.

AI Without Security is Risky Business— But the Rewards Are Limitless

AI is still in its early stages, and we have yet to see its full potential and impact on society. To achieve what it's truly capable of, AI needs access to data—lots of it. However, without a clear strategy, this can lead to unthinkable situations. In fact, **80% of business leaders cite data leakage as their primary fear when adopting AI.**² Ensuring a strong foundation allows businesses to harness AI's power safely and effectively, driving innovation and success.

By establishing a strong security foundation, organizations can confidently embrace AI—protecting sensitive data while maximizing its capabilities. Secure AI adoption not only mitigates risks but also creates new opportunities for growth, compliance, and long-term success. Businesses that prioritize security will lead the way in harnessing AI's full power responsibly and effectively.

1. Microsoft FY25 Q1 Earnings Report, October 2024.
2. Protect Copilot with Microsoft Purview, 2025
3. ISMG, First Annual Generative AI Study, 2023.

The Foundation for AI Success

Managing AI Risks With the Right Strategy

AI thrives on data, making security a top priority. While AI's benefits are immense, organizations must ensure they protect sensitive data, comply with industry regulations, and manage AI access effectively. A security-led AI strategy allows businesses to fully capitalize on AI's potential without exposing themselves to unnecessary risks.

As AI continues to evolve, implementing security best practices ensures organizations can move forward with confidence. By adopting Microsoft's security solutions, businesses can do the following.

Prevent Data oversharing – AI may unintentionally expose sensitive files or grant excessive access to employees beyond what is necessary to do their jobs.

Protect sensitive information – Unauthorized access or misuse of AI-generated insights can lead to data loss or intellectual property theft.

Govern AI interactions – AI use, now and into the future, will need to align with evolving business and industry regulations.

Data Oversharing

What is it:

AI thrives on data, but ensuring that employees access only the information necessary for their roles is essential for security. Proper data governance allows organizations to leverage AI effectively while preventing unintended data exposure.

How does it occur:

- Accidentally saving a file to a location with broad access permissions
- A user sharing content with someone who should not have access
- Files do not have access protections

How to optimize AI for security and efficiency:

- Restrict user and/or Copilot access to risky sites while remediating identified oversharing risks
- Act on policy suggestions to mitigate oversharing risks
- Prevent Copilot from processing certain sensitive files and from using them in responses if required
- Remove organization-wide site access as needed
- Get notifications when new oversharing occurs with options for remediation
- Further secure sensitive data through file level access controls and Data Loss Prevention policies
- Improve Copilot responses by archiving or deleting unneeded content



Data Protection

What is it:

AI-powered tools like Copilot enhance collaboration and productivity by making information more accessible. However, businesses must ensure that AI-driven insights are shared securely and used appropriately. Proactive security measures help protect against data loss and insider threats, ensuring AI remains a force for innovation.

How does it occur:

- Documents may be created without protection if the original content wasn't properly labeled or secured.
- Sensitive data can be exposed when users bypass or misunderstand data usage guidelines.
- If user credentials are compromised, bad actors may gain access to sensitive information.
- Departing employees may attempt to collect valuable company data before they leave.

How to keep AI-powered insights secure:

- Get alerts and reports of risky behavior and AI use in the organization
- Protect sensitive files and Copilot interactions by labeling data
- Train Microsoft 365 Copilot to apply security policies based on risky actions patterns that are being seen by users



35%

of respondents are concerned about lack of tools to protect data that goes into generative AI ⁴

4. Security-led Secure AI for SMC and Enterprises Infographic, 2024.

By 2027

At least one global company will see its AI deployment banned by a regulator for non-compliance ⁴

Govern AI Use to Meet Regulations & Policies

What is it:

Effective AI governance ensures that AI is used in alignment with organizational policies and regulatory requirements. By implementing compliance and management controls, businesses can enforce safe and responsible AI use, mitigating risks while maximizing its benefits. This includes integrating AI interactions into existing compliance, management, and legal processes.

How does it occur:

- Configures Copilot admin controls to support compliance with a specific AI regulatory framework (Ex: EU AI Act, NIST AI Risk Management Framework)
- Increase AI response quality by limiting its access to outdated information
- Limit exposure, identify issues early and mitigating them quickly
- Keep, delete or evaluate AI generated content according to your risk management preferences

How to govern AI effectively

- Monitor and audit AI interactions to ensure compliance and security
- Implement lifecycle policies and legal holds to safeguard AI-generated content
- Proactively investigate and address compliance concerns to maintain ethical AI use

Drive Security-Led Innovation

The potential of AI is limitless—but only when implemented with security at its core. Many organizations hesitate to adopt AI due to concerns about data exposure, compliance, and governance. However, businesses that integrate AI with Microsoft's security solutions can turn these challenges into opportunities, enabling seamless innovation while protecting their digital assets.

The future belongs to businesses that harness AI while ensuring security and compliance. If you're ready to get the most out of AI without the headaches, Myriad Services is here to support you. We'll work with you to pinpoint where AI can make the biggest impact in your business—while helping you stay secure, efficient, and compliant every step of the way.

Sources:

1. Microsoft FY25 Q1 Earnings Report, October 2024.
2. Protect Copilot with Microsoft Purview, 2025.
3. ISMG, First Annual Generative AI Study, 2023.
4. Security-led Secure AI for SMC and Enterprises Infographic, 2024.

Reference:

Secure and Govern Microsoft 365 Copilot, 2025
Microsoft Data Security Index, 2024.



Contact us



1300 989 314

<http://www.frontrow.technology>