



E-book

Comprehensive Security in the Era of AI

Build a secure foundation for
AI-powered productivity



03

Introduction:

Security challenges in the era of AI

05

Chapter 1:

Pivot to a proactive AI security strategy

08

Chapter 2:

Three key requirements for security and compliance controls

11

Chapter 3:

Get AI-ready with Microsoft 365

15

Chapter 4:

Secure AI-powered productivity with Copilot for Microsoft 365

Your guide to securing AI-powered productivity

Read this comprehensive guide to explore best practices for mitigating security risks in the era of AI. You'll learn how to pivot toward a proactive AI security strategy and gain insights into security and requirements controls. You'll also learn three steps to get your organization AI-ready now and how to secure AI-powered productivity with Microsoft 365 E3.



Security in the era of AI

AI is ushering in a new era of work, and for many companies, the transformation has already begun. The adoption of AI into business operations is rapidly gaining traction, with organizations across industries exploring or implementing AI in various capacities.

Embracing AI empowers companies to significantly increase productivity and foster innovation among their workforce, laying the groundwork to grow the business and achieve organizational goals. However, while the transformative potential of AI creates opportunities, it can also bring new challenges in security and regulatory compliance.

Get AI-ready now

A robust security posture is business-critical for AI readiness. Safeguarding data integrity and privacy is essential to making AI a secure asset for your company, employees, and customers. As the availability of AI services grows, the need to secure the data exchanged between applications

and users becomes more urgent. In addition, the lack of visibility into the unauthorized use of AI tools and apps amplifies security risks.

Given the data-centric nature of AI systems, the potential for breaches exists. Secure AI platforms play a vital role in maintaining the integrity of AI operations and defending against malicious interference. Additionally, stringent regulations govern data and AI usage across various industries. These factors highlight the importance of enhanced security to facilitate compliance.

AI is just one of the significant workplace changes that require increased security measures. Hybrid work, including the implementation of bring your own (BYO) device policies, also introduces greater complexity and heightened security challenges.

Address growing security challenges

Advancements in AI and the growth of hybrid work have significantly intensified the need for enhanced identity, security, and information protection as part of an organization's tech stack. Consider the following:

- **Cybercriminals are getting the credentials they need to succeed in their attacks.**

With more than 4,000 password attacks occurring every second, totaling 30 billion per month,¹ the urgency to secure and manage user identities is more critical than ever before. Today's attackers are already taking advantage of AI to automate identity theft, perpetuate fraud, and orchestrate sophisticated attacks that mimic legitimate user behavior. As AI capabilities expand, robust identity management and security becomes increasingly vital to prevent unauthorized access and defend against AI-driven cyberthreats.

- **Securing endpoints is more difficult.** The widespread adoption of BYO devices has significantly expanded and exposed endpoint vulnerabilities. On average, an enterprise hosts about 3,500 connected devices lacking detection from an endpoint detection and response agent.² These unmanaged devices, often part of the "shadow IT" landscape, are particularly attractive to threat actors due to their limited security. In fact, Microsoft research indicates that devices are 71% more likely to be infected when they're unmanaged.³ When unmanaged devices connect to company networks, they create opportunities for cyberattackers to launch broader assaults on servers and other critical infrastructure.

Secure platforms play a critical role in preserving the integrity of AI operations and safeguarding against interference from malicious actors. To bolster defenses and facilitate a secure transition into an AI-powered future, security and IT teams must implement two business-critical strategies in their tech stacks: Zero Trust and simplified endpoint management.

\$4.45M



The average cost of a data breach reached a record high of \$4.45 million in 2023, **an increase of 15% over three years.**⁴

The background features several overlapping, semi-transparent geometric shapes in shades of purple and blue. These include a large circle in the bottom right, a rectangular plate in the center, and various other plates and a curved surface in the upper left. A large, light purple number '1' is positioned on the left side of the slide.

1

Pivot to a
proactive AI
security strategy

A disjointed tech stack limits the power and promise of AI. To implement AI successfully and securely in your organization, a solid IT foundation is essential. As IT and security teams pivot to support AI, questions consistently emerge around these three themes:

1

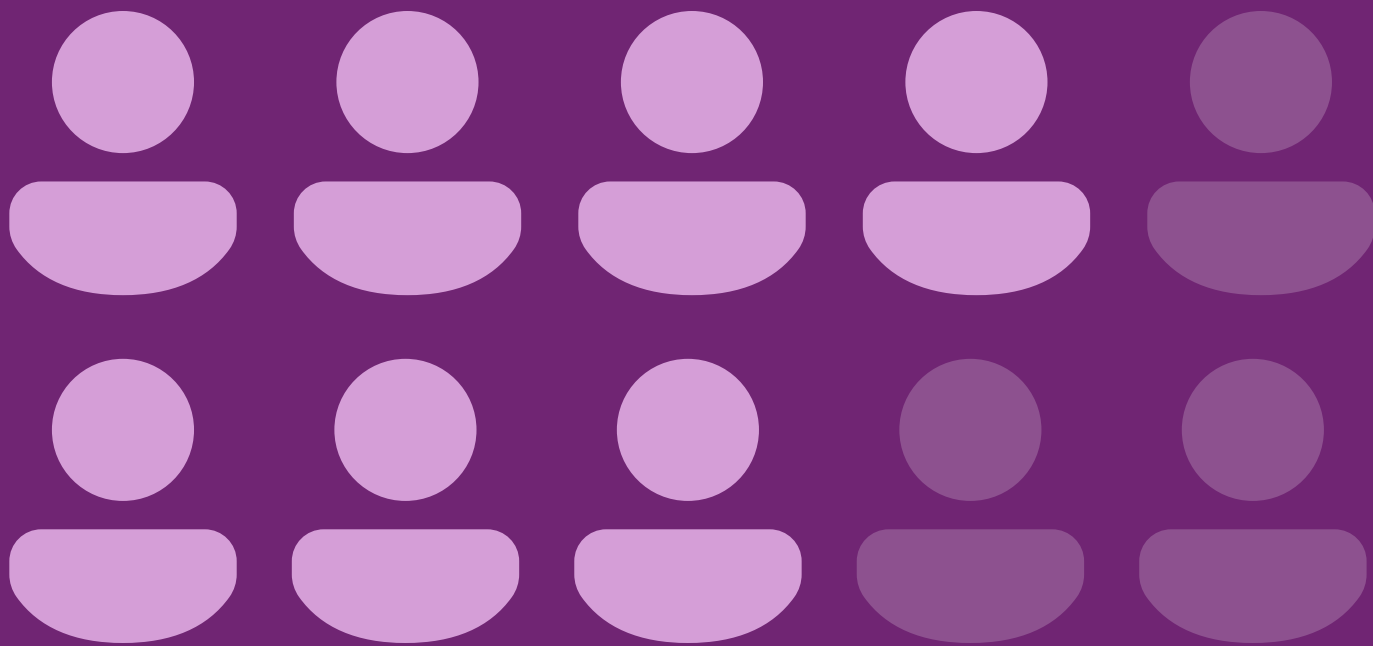
How is your organization doing with a Zero Trust security strategy? How can you tighten access controls and minimize security breaches?

2

How well are you protecting your data and enforcing data governance policies?

3

How do you make sure that your employees have secure access to the latest best-in-class productivity applications?



70%

of workers said they would delegate as much work as possible to AI to lessen their workloads.⁵

Key strategies for securing modern work

Implement Zero Trust—the foundation of robust security

AI introduces new vectors for security risk with repercussions like data breaches, financial losses, and damage to an organization's reputation. To mitigate these risks, a Zero Trust foundation with anomaly detection is essential. This involves securing all identities, devices, and applications.

Unlike traditional security models that assume trust behind corporate firewalls, Zero Trust operates on the principle of breach assumption. This approach verifies each request as if it came from an open network. It also minimizes security incidents by continuously verifying identity and access, both internally and externally.

Protect data with streamlined endpoint and app management

To defend against cyberthreats on multiple platforms, effective endpoint management is crucial. Endpoint management technology

enhances data loss protection controls, applies robust data governance, and enforces policies for data retention and access rights. It also reduces complexity by streamlining and applying consistent policies. These policies are implemented across the processes and tools used to authenticate, monitor, and secure your organization's devices.

Fuel productivity with the right solution

The transition to AI-driven productivity is currently underway, reshaping how people work. Across industries, business leaders face mounting pressure to adopt AI-powered tools to drive productivity forward. Simultaneously, many employees are already using AI, finding it beneficial as they cope with increased workloads, data overload, and the demands of constant communication.

To meet the requirements of both business leaders and employees, the optimal solution is essential. This solution should boost productivity, foster innovation, enhance collaboration, and help employees take advantage of the full potential of AI—all in a secure environment.



2

Three key requirements
for security and
compliance controls

Implementing comprehensive security and compliance controls is a crucial component of a proactive AI security strategy. These controls empower organizations to realize the full potential of AI while upholding trust, ethical standards, and effective risk management practices.

1. Manage risky sign-ins

Identifying and thwarting unauthorized or potentially harmful sign-in attempts is a significant security challenge. Risky sign-ins stem from cybercriminals exploiting compromised devices, using stolen credentials, or masking their identity via anonymized IP addresses. Alternatively, they could originate from legitimate employees working in atypical locations or on unfamiliar devices. Regardless of the source, it's imperative to have mechanisms in place to detect risky sign-ins and implement measures to protect your organization.

2. Mitigate device risk

The concept of device risk involves the likelihood of a security breach occurring through mobile devices, including tablets, smartphones, and laptops. With each new device added to your organization's network, the potential for cyberthreats—such as data breaches, phishing attempts, and ransomware—increases incrementally. Attackers might exploit stolen data to impersonate system administrators or high-ranking officials to gain access to sensitive information and cause significant damage. With the proliferation of mobile devices in the new era of work, managing device risk has emerged as a paramount concern for businesses worldwide.



3. Prevent data overexposure

Organizations store content with varying access levels, ranging from publicly accessible to restricted areas. Data overexposure, a critical cybersecurity issue, occurs when sensitive content is granted excessive access levels. This often happens when employees share personal information stored on secure platforms

too liberally. For example, employees might share publicly accessible links or grant access permissions to everyone in the organization. Implementing data overexposure policies is essential to identifying and assessing these risks and promptly alerting your security team to potential issues.



Understanding the difference between data exposure and data breach

Although they're often used interchangeably, data exposure and data breach are two distinct concepts.


Data breach: A data breach occurs when unauthorized parties access and potentially expose, steal, or sell sensitive data. Malicious actors use various methods to infiltrate protected systems, including malware attacks, insider threats, brute-force attacks, phishing schemes, and password cracking. From an organizational standpoint, human error and security system vulnerabilities are the most common causes of data breaches.

Data exposure: Unlike a data breach, where private data is intentionally stolen, data exposure occurs when sensitive information is accidentally exposed. The root cause often lies in coding errors or an organization's failure to properly secure and encrypt online data. While unintentional, a data exposure incident still has the potential to damage the organization's reputation and compromise data integrity.

The background features a light beige gradient with several translucent, 3D-style geometric shapes in shades of blue and purple. These shapes, including flat plates and curved segments, are arranged in a dynamic, overlapping composition. A large, dark blue square on the left side contains a large, light blue number '3'.

3

Get AI-ready with
Microsoft 365



The best way to get AI-ready is to deploy Microsoft 365 E3. This essential foundation for modern work brings all the capabilities for AI readiness together—identity, applications, management, security, and your enterprise data.

With Microsoft 365 E3, you can fortify your security posture and get your organization ready for AI adoption in three steps.

Step

1

Set up a strong Zero Trust foundation

The Zero Trust foundation and endpoint management within Microsoft 365 E3 provide a comprehensive security solution. Microsoft 365 E3 secures and manages identities, defends against cyberthreats across multiple platforms, and safeguards sensitive information throughout your data estate.

At its core, this solution implements proactive security controls across your entire environment, guided by three fundamental principles:

- **Verify explicitly.** Use all available data points—including user identity, location, device health, resource, data classification, and anomalies—to make informed security decisions. To ensure that only authorized users gain access, Microsoft 365 E3 uses

Microsoft Entra ID for identity verification with robust authentication methods.

- **Least privilege access.** Limit access through just-in-time and conditional access policies, granting no standing privileges. Microsoft 365 E3 uses access controls and policies to minimize the potential impact of breaches. Employees receive only the access they need to perform their tasks.
- **Assume breach.** Minimize the impact of potential security incidents by implementing micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response. Operating under the assumption that breaches can occur at any time, Microsoft 365 E3 uses automated threat detection and response mechanisms to quickly identify and mitigate cyberthreats.

Step

2

Streamline endpoint management

Empower your workforce to work securely and efficiently from any location and device with a modern, flexible endpoint management solution. You'll enhance your ability to safeguard, manage, and support all endpoints and applications by using Microsoft 365 E3 to:

- **Enhance security.** Security begins with default controls that safeguard devices from the moment of activation. As part of your Microsoft 365 E3 subscription, you get access to Windows 11 Enterprise, which protects against threats during startup using hardware-based root of trust. The solution also delivers robust application security and prevents access to unverified apps. Additionally, employees will have enhanced security features such as Windows Hello for Business, offering passwordless security to protect their identities.
- **Manage and protect any endpoint, from the cloud.** Effectively manage both company-owned and BYO devices through a unified solution that provides visibility, recommendations, and data insights. You'll get on-by-default security settings that comply with Zero Trust principles and automatic updates to Windows and Microsoft 365 E3. You'll also gain the flexibility to customize compliance policies and address noncompliant endpoints.
- **Simplify and optimize your endpoint estate to boost IT efficiency.** Empower your IT team to improve the support experience and minimize endpoint-related incidents. With proactive remediation capabilities, your IT staff can identify and resolve issues before your employees are even aware of them. By using one central command center in Microsoft 365 E3 to manage and protect all your organization's endpoints, you'll reduce the IT time and costs needed to manage siloed and redundant products and platforms.



Step 3

Step 3: Drive productivity and collaboration

Connect and empower your entire workforce, anytime and anywhere, on any device with Microsoft 365 E3 and Microsoft Teams, to:

- **Get everyone connected and working together.** By transitioning to a single cloud-based platform, you consolidate communication, collaboration, and information access all in one place. This eliminates the need to deploy multiple solutions, reducing IT costs and complexity.
- **Empower your employees with best-in-class communications tools.** Consider adding Teams to your Microsoft 365 license. Teams supports hybrid work and facilitates seamless communication through

meetings, chat, calling, file sharing, and brainstorming—all within a single interface. Teams also streamlines workflows and boosts productivity with features like automatic meeting summaries, transcripts, and real-time translation in 40 languages.

- **Safely introduce the power of AI to your employees.** To help your employees get started with AI, enable them to take advantage of Copilot AI-powered chat. With commercial data protection turned on, employees can ask Copilot to perform tasks like generating content for new products and safely include sensitive internal information in the prompt, such as the product specs and pricing. With each interaction, they're reminded that personal and company data is protected throughout the chat session, with no data stored or used for training AI models.

Securely try Copilot

Employees can securely access Copilot assistance in the Microsoft Windows sidebar, Bing search, Bing mobile app, Microsoft Edge web browser sidebar, and at **copilot.microsoft.com**.



4

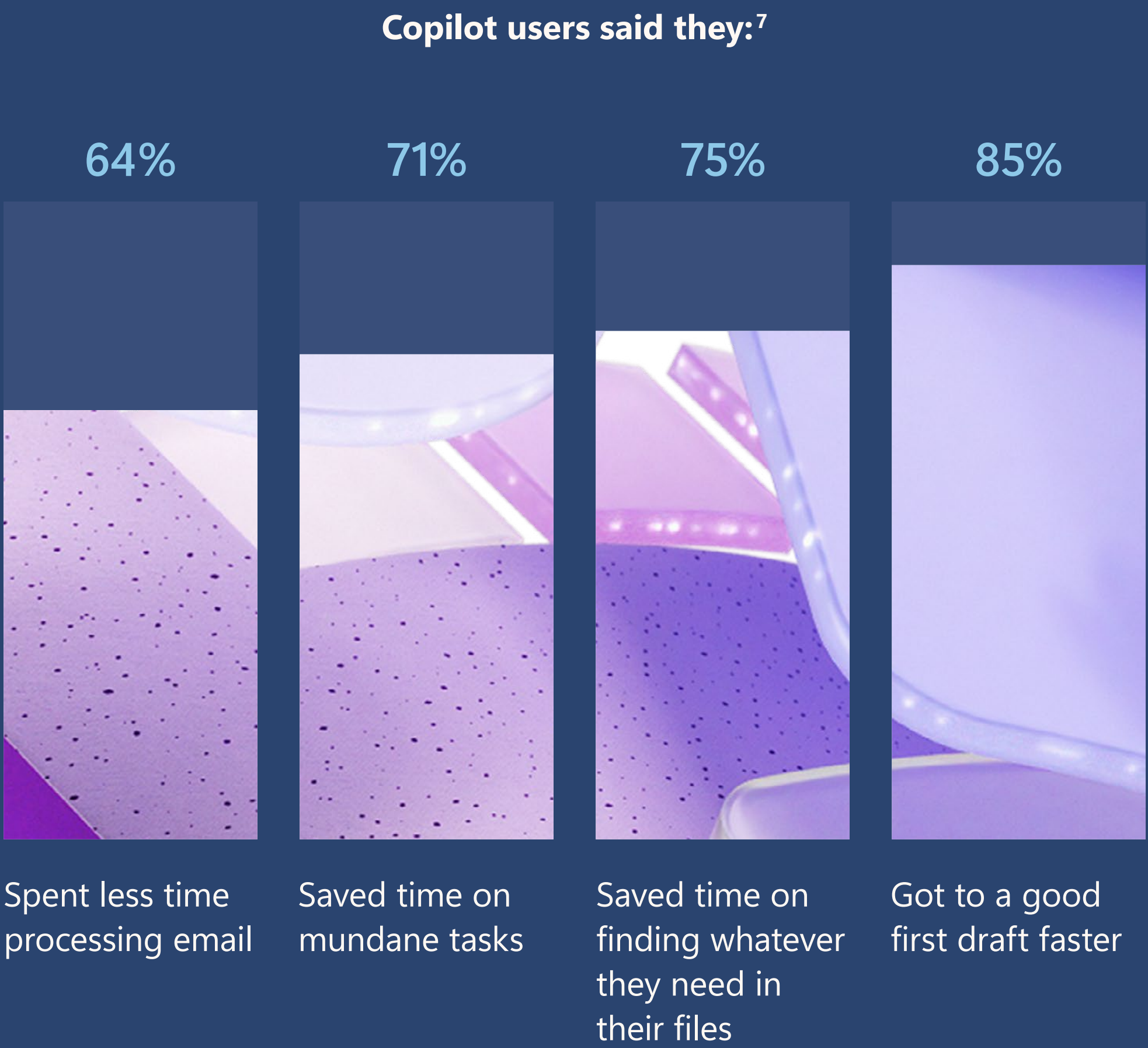
Secure AI-powered productivity with Copilot for Microsoft 365

Copilot helps employees jumpstart their creativity, convert documents into presentations, clear their inboxes in minutes, and get real-time summaries of meetings and action items.

Once your team has implemented Microsoft 365 E3, you're ready to securely deploy Copilot for Microsoft 365. As their AI assistant at work, Copilot works in the apps your employees use, including Word, Excel, PowerPoint, and Microsoft Teams.

Copilot users are more productive

In short, Copilot helps people improve productivity, creativity, and efficiency according to a Microsoft study of 297 participants in the Copilot for Microsoft 365 Early Access Program.⁶ The study showed that the productivity gains from Copilot are significant, according to Copilot users who participated in the program.



Core security controls for a secure user journey with Copilot

For all the value that Copilot for Microsoft 365 brings to employees and organizations, the architecture itself is fundamentally simple. It's an orchestrator and large language model that builds on your Microsoft 365 E3 security controls and operates within your organization's compliance boundaries.*

This means that Copilot combines the power of innovative large language models with your organization's specific content in Microsoft Graph—your documents, emails, calendar,

chats, meetings, contacts, and other business data—to deliver accurate, relevant, and contextual responses.

Copilot builds on and adheres to your existing privacy, security, and compliance commitments, only accessing content that's already available to your employees. Your organization manages Copilot with the same tools and standards that you use today.

*Compliance boundaries create logical boundaries within an organization that control the user content locations (such as SharePoint sites, OneDrive accounts, and mailboxes), which e-discovery managers can search. Compliance boundaries also control the access permissions for e-discovery cases utilized in managing human resources, legal, or other investigations within your organization.

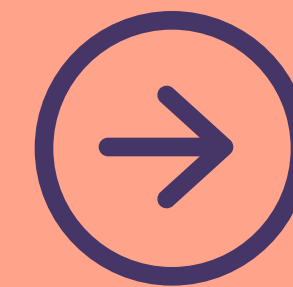
Compliance boundaries are frequently required by multinational corporations that must respect geographical borders and regulations, and by governments that are typically divided into various agencies. Microsoft 365 E3 helps organizations meet compliance boundaries when performing content searches and managing investigations with e-discovery cases.



Conclusion

As organizations embrace an era fueled by AI-powered productivity, business leaders are exploring new ways of working due to advancements in generative AI. Today, the best way to become AI-ready, and specifically Copilot-ready, is to implement Microsoft 365 E3.

Microsoft 365 E3 brings together essential capabilities to safeguard your enterprise data in a single solution, spanning identity, applications, management, and security. This comprehensive solution empowers your team to fortify your security posture and successfully transition to the new era of work with confidence.



Learn more about securing AI-powered productivity with Microsoft 365 E3.

Citations

¹["Microsoft Digital Defense Report,"](#) October 2023.

²["Anatomy of a modern attack surface,"](#) Microsoft Security Insider, May 2023.

³["Secure unmanaged devices with Microsoft Defender for Endpoint now – Microsoft Security Blog,"](#) April 2021.

⁴["Cost of a Data Breach Report 2023,"](#) IBM, 2023.

⁵["Work trend Index Annual Report: Will AI Fix Work?,"](#) Microsoft Work Trend Index. May 2023.

⁶["What Can Copilot's Earliest Users Teach Us About Generative AI at Work?,"](#) Microsoft Work Trend Index Special Report, November 15, 2023.

⁷["What Can Copilot's Earliest Users Teach Us About Generative AI at Work?,"](#) Microsoft Work Trend Index Special Report, November 15, 2023.

©2024 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.