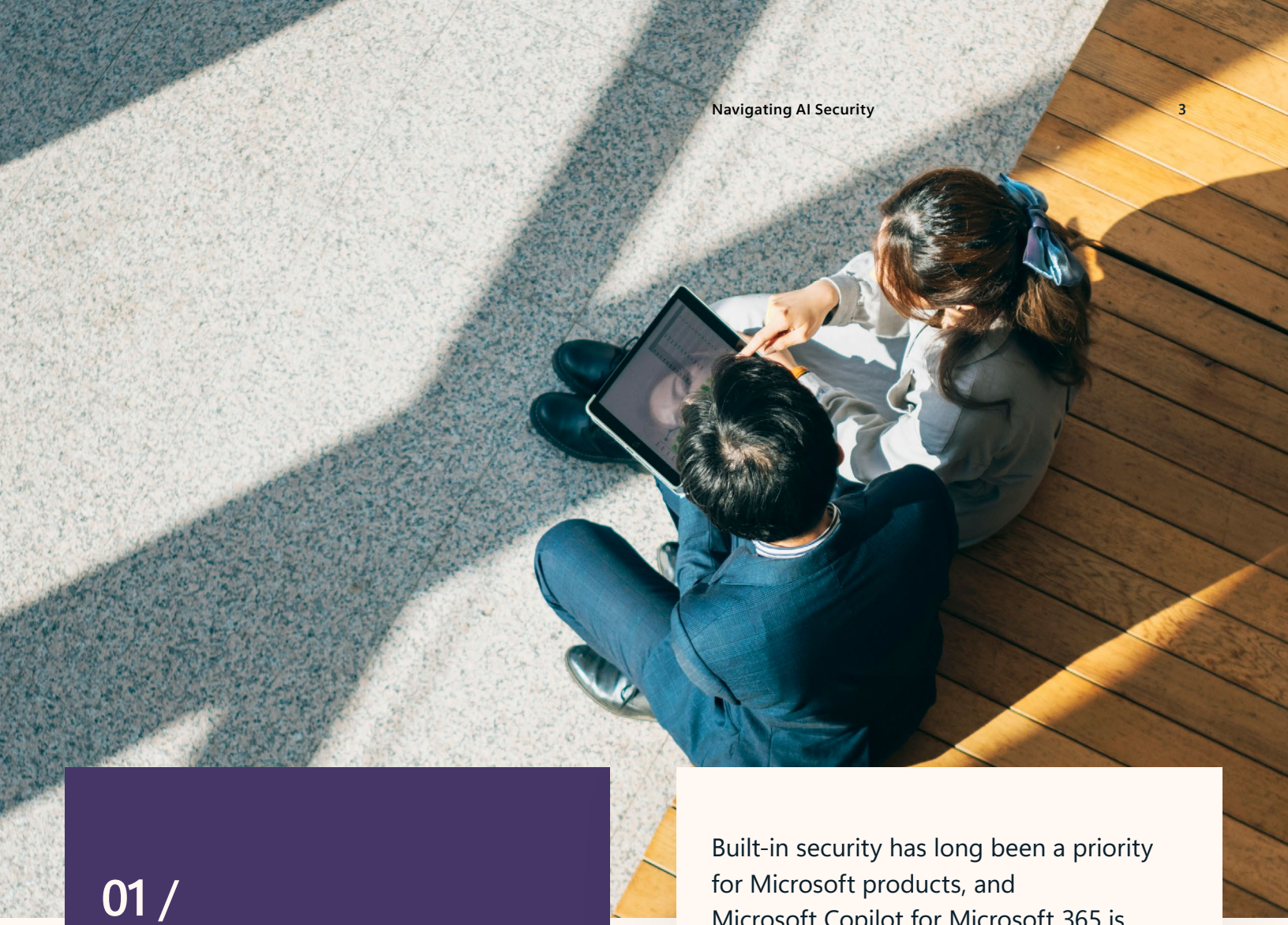
E-book Series

Microsoft 365

Navigating AI Security

A Guide for Microsoft Copilot for Microsoft 365

Contents



01 / Security comes first

Built-in security has long been a priority for Microsoft products, and Microsoft Copilot for Microsoft 365 is no exception. From its ability to rely on existing Microsoft 365 security features to the way Copilot itself operates, Copilot is designed to integrate with your existing systems while helping keep your data, infrastructure, and privacy protected.

Specifically, the strength of Copilot security is rooted in how it handles data, built-in privacy controls, and how the AI model itself is trained. Let's take a closer look at those and other related topics as we explore how Copilot helps keep your data secure and private.

02 /

A personal experience that works for you

Microsoft Copilot helps make you more productive and creative, but it's also designed to do that in a personalized way. The instance of Copilot that you interact with is not a centralized resource that everyone in your company plugs into. It is uniquely your own.

Copilot gains insights from the projects you're working on, what your priorities are, your writing style, and who you collaborate with most frequently. In short, it delivers a personal experience by summarizing your emails and meetings, identifying action items, and helping to create content for documents. The more you engage with Copilot, the more useful and accurate it's able to be in responding to queries and performing tasks.

But keep in mind, no one else can access your Copilot data, including Microsoft. That's because Copilot inherits your organization's existing Microsoft 365 security, identity, and compliance policies. This means that, by design, it can only access the same data that users can access.

This in effect extends your existing security architecture around Copilot, which is another advantage of its integration with Microsoft 365. It also makes it easier to configure and manage the security capabilities while making Copilot itself more secure.

03 /

Security that works for your business

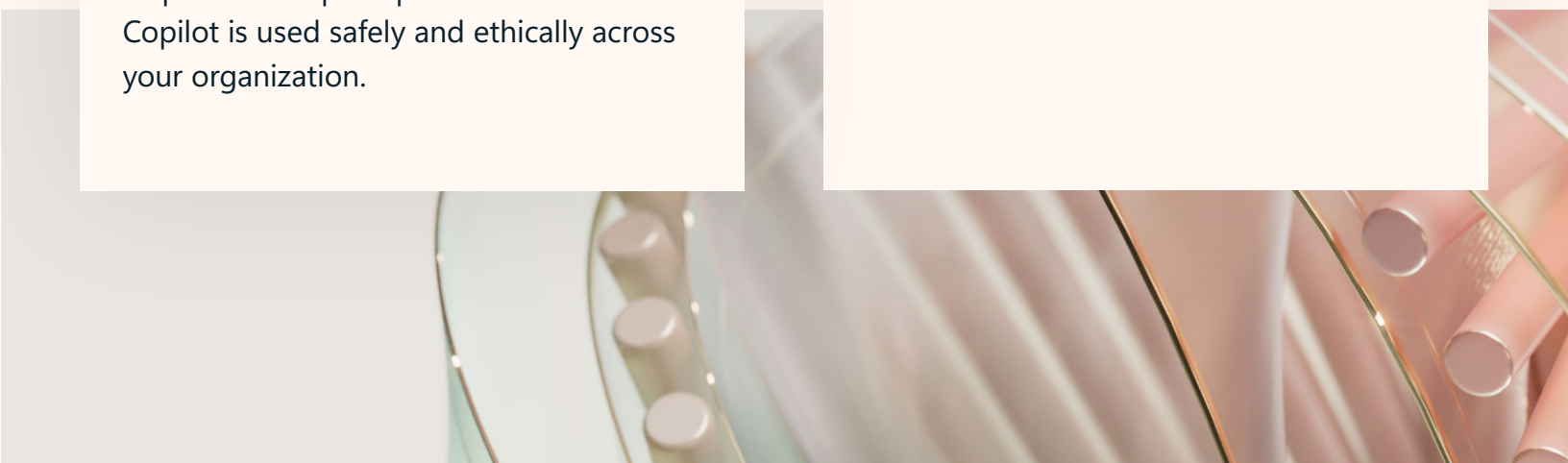
Backed by Microsoft security

Microsoft's comprehensive approach to security, privacy, and identity combines advanced encryption features, robust tools, advocacy and support for the Zero Trust framework, compliance capabilities, a commitment to transparency, and responsible AI principles to ensure that Copilot is used safely and ethically across your organization.

Encryption

Because Copilot is contained within Microsoft 365, it benefits from built-in encryption capabilities to protect data while it is being stored or used. Your data "at rest" is encrypted, and TLS encryption guards your data when it is in transit between Copilot components and services.

As noted earlier, only users within your Microsoft 365 tenant can access data, according to your organization's permissions and access policies. Therefore, your IT organization needs to use the permission models available in Microsoft 365 services to ensure that the right users or groups, including users outside your organization, have access to the appropriate data.



You control your data

Controlling which apps and technologies can access and share your data to help you be productive is an important part of keeping data secure.

Microsoft does not share your data with third parties unless you explicitly grant permission. Copilot does not use any of the data it has access to for training its LLM or improving other products unless you provide consent. The prompts you enter and the corresponding responses are not accessible to other users either. You can also exclude certain files or folders from Copilot access so that it does not use them as context for responses.

Microsoft's approach to data control helps keep your information secure, but by giving users control, it helps build the trust that is essential to successful adoption. When users know they have control over their Copilot data and that it will be handled responsibly, they are more likely to trust it and get the most out of it.

Data storage

Copilot runs completely within the Microsoft Azure cloud and is built to align with the latest Microsoft commitments to data security and privacy for the enterprise.

Microsoft has been committed to ensuring all of its products and services comply with GDPR ever since that regulation took effect. Thus, the way that Copilot operates is also in compliance with GDPR, as well as EU and other data boundary standards.

Other important security and privacy points to note are:

- Copilot uses Microsoft Entra ID for authentication and only allows users to access it with commercial data protection using their work account.
- Entra ID user's tenant and user information is removed from chat data at the start of a chat session. This information is only used to determine if the user is eligible for commercial data protection.

Applying Zero Trust

Part of maximizing the security capabilities of Copilot is to ensure that it is integrated into your Zero Trust framework. Zero Trust is an enterprise security strategy built on the principles of explicit verification for each user session, least-privileged access that provides users access to the minimum amount of network and data access they need at that moment, and an assume breach posture to minimize the impact in the event of a security incident. Thus, it is important to make sure Copilot is aligned with these principles and how your enterprise implements them.

Principles of Zero Trust

Verify explicitly: Always authenticate and authorize based on all available data points.

- Use least-privileged access: Limit user access with just-in-time and just-enough access, risk-based adaptive polices, and data protection.
- Assume breach: Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

The following steps provide high-level guidance for how to apply Zero Trust principles while ensuring your Microsoft 365 environment is ready for Copilot:

1. Deploy or validate your data protection.
2. Deploy or validate your identity and access policies.
3. Deploy or validate your App protection policies.
4. Deploy or validate device management and protection.
5. Deploy or validate your threat protection services.
6. Deploy or validate secure collaboration with Teams.
7. Deploy or validate user permissions to data.

Compliance

Just like other enterprise activities and data, AI-powered technology such as Copilot requires security and compliance management. Because Copilot is integrated with Microsoft 365, you can use Microsoft Purview compliance capabilities to support your risk and compliance requirements, including:

- Sensitivity labels
- Data classification
- Customer key
- Communication compliance
- Auditing
- Content search
- eDiscovery
- Retention and deletion
- Customer Lockbox

04 /

Your gateway to data and intelligence

One of the most valuable benefits of Copilot is its access to Microsoft Graph. Thus, it's vital to understand the relationship between the two, as well as how that relationship addresses security, privacy, and compliance.

What is Microsoft Graph?

Microsoft Graph is a secure and unified API developer platform that connects multiple services, devices, and their data within the Microsoft ecosystem. In terms of Copilot for Microsoft 365, this includes calendar data, email files, and organizational structure.

Most relevant to Copilot, Microsoft Graph offers several options for enhancing identity and access management, productivity and collaboration, and people and workspace intelligence.

Identity and access management

Microsoft Entra ID Governance helps you ensure that the right people have the right access to the right resources and at the right time. This may include users, groups, and applications, and users can refer to your employees, business partners, vendors, or contractors.

You manage Microsoft Entra ID Governance capabilities programmatically by using identity governance APIs in Microsoft Graph, such as Access Reviews, Entitlement Management, Lifecycle Workflows, Privileged identity management, and Terms of use.

Microsoft Entra ID Protection APIs and Workload ID APIs help detect and mitigate identity-based risks before they cause damage. Additionally, you can configure multifactor authentication, including phishing-resistant methods, to reduce risks associated with compromised credentials.

Productivity and collaboration

Microsoft Graph enables integration with Microsoft 365 and provides REST APIs and client libraries to access valuable, people-centric data and insights. By using Microsoft Graph, you can build secure applications that enhance user productivity, creativity, and team collaboration while protecting business resources and user data.

Microsoft Graph Security Connector helps connect different Microsoft and partner security products and services using a unified schema. It streamlines security operations and improves threat protection, detection, and response capabilities.

People and workspace intelligence

Microsoft Graph connectors allow you to ingest unstructured, line-of-business data into Microsoft Graph. This data becomes part of Microsoft Graph, enabling Copilot for Microsoft 365 to reason over your enterprise content.

Your developers can build custom connectors using the following Microsoft Graph connector APIs to build specialized Copilot apps and functionality:

- People API: Allows you to build smarter apps for accessing user data related to people.
- Insights API: Provides insights into user activities and interactions.
- Profile API: Accesses user profiles and related information.
- Profile Card API: Retrieves profile card data for users.

05 /

Principles of responsible AI

Another important part of building trust when deploying an AI solution like Copilot is knowing that it supports your organization's values in terms of ethical AI decision-making and responsible use cases. Microsoft developed the Responsible AI Standard to help address this need, as well as many other potential concerns.

As an AI product, Copilot has therefore been developed to align with the following principles of responsible AI developed by Microsoft research, policy, and engineering teams, so that you have a better idea of how it aligns with how you want to incorporate AI into your own organization.

Accountability

Ensure that AI systems can be assessed to identify when they may have a significant adverse impact on people, organizations, and society, and whether additional oversight and requirements should be applied to those systems.

Transparency

Microsoft provides information about what its AI systems can and can't do in order to support stakeholders in making informed choices about those systems. The systems themselves are designed to inform users that they are interacting with an AI system or are using a system that generates or manipulates image, audio, or video content that could falsely appear to be authentic.

Fairness

Microsoft AI systems are designed not to discriminate or perpetuate biases, and to provide a similar quality of service for and to minimize the potential for stereotyping, demeaning, or erasing of identified demographic groups, including marginalized groups.

Reliability and safety

Microsoft evaluates operational performance in terms of reliability and safety, remediates issues, and provides related information to customers.

Privacy and security

Microsoft AI systems are designed to protect privacy in accordance with the Microsoft Privacy Standard, and to be secure in accordance with the Microsoft Security Policy.

Inclusiveness

Microsoft AI systems are designed to be inclusive in accordance with the Microsoft Accessibility Standards.

06 / Security at the forefront

While AI solutions have the potential to improve productivity and creativity, many of those same capabilities are also built into Copilot to make it more secure. Backed by Microsoft, Copilot offers peace of mind in helping you realize the promise of AI in an environment that won't compromise your data and device security, privacy, or compliance.

Learn more about how Copilot can help empower your people while helping keep your data secure.

Explore Copilot for Microsoft 365