Whitepaper

Prepare Your Environment for Microsoft 365 Copilot

Applying Zero Trust Principles to Your Adoption Strategy

In today's world of increasing cyberattacks and data breaches, traditional perimeter defense security models are no longer sufficient. Organizations need a new approach that assumes no trust and verifies every request — regardless of where it comes from or where it goes. This is the essence of the Zero Trust model — a critical piece of a secure deployment of Microsoft 365 Copilot.

In this whitepaper, you'll learn how to prepare your environment for using Microsoft 365 Copilot, and how to apply Zero Trust principles and leverage the full value for M365 E5 licensing.

Microsoft 365 Copilot gives your end users the ability to ask any question of your data and get an answer, but it also allows bad actors to do the same. This makes a Zero Trust approach critical to your Copilot adoption strategy.

Zero Trust principles

The Zero Trust principle of **verifying explicitly** means that every request for access or resources should be authenticated and authorized based on all available data points, including:

- Identity
- Location
- Application context
- Device
- Network

This also means that trust should not be inferred from past interactions or assumed based on predefined boundaries. Instead, trust should be continually evaluated and validated throughout the entire session or transaction.

To apply this principle to Microsoft 365 Copilot, ensure that modern authentication with Multi-Factor Authentication (MFA) methods are combined with conditional access policies. This will **verify the claims of identity of users** and the current security posture of the device. By leveraging the power of Microsoft Entra™ ID Protection, you're able to assess the risk level of each user and sign-in attempt with enforcement of granular conditional access policies based on the user's role, location, device state and app sensitivity — helping you stop unauthorized access.

Another important principle for securing Microsoft 365 Copilot is to always use the **least privileged access** model. This means that users and applications should only have the minimum level of permissions and access rights required to perform their tasks. By limiting the exposure of sensitive data and resources, the risk of compromise or misuse is reduced. Additionally, in the event of a breach, the impact and damage can be contained and mitigated.

To apply this principle to Microsoft 365 Copilot, ensure that Role-Based Access Control (RBAC) is implemented to assign roles and permissions to users and applications based on their responsibilities and needs. By using RBAC, you can enforce the principle of separation of duties — which prevents conflicts of interest and unauthorized actions. You can also use Microsoft Entra Privileged Identity Management (PIM) to manage, monitor and audit the use of privileged accounts and roles. PIM provides features such as just-in-time access, time-bound access, approval workflows and access reviews to ensure that privileged access is granted only when needed (and revoked when not in use).

A third important principle for securing Microsoft 365 Copilot is to **assume breach**. This means that you should not rely on perimeter-based security measures alone — but rather adopt a defense-in-depth strategy that assumes that attackers may have already compromised your network or devices. By assuming breach, you can design your security policies and controls to protect your data and resources at every layer, from the identity and device level to the application and data level. You can also implement proactive monitoring and threat detection capabilities to identify and respond to any malicious activity or anomalies in your environment.

Verify explicitly.

Always validate all available data points, including:

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access.

To help secure both data and productivity, limit user access with:

- Just-in-Time (JIT) access
- Just-Enough Access (JEA)
- Risk-based adaptive policies
- Data protection against out of band vectors

Assume breach.

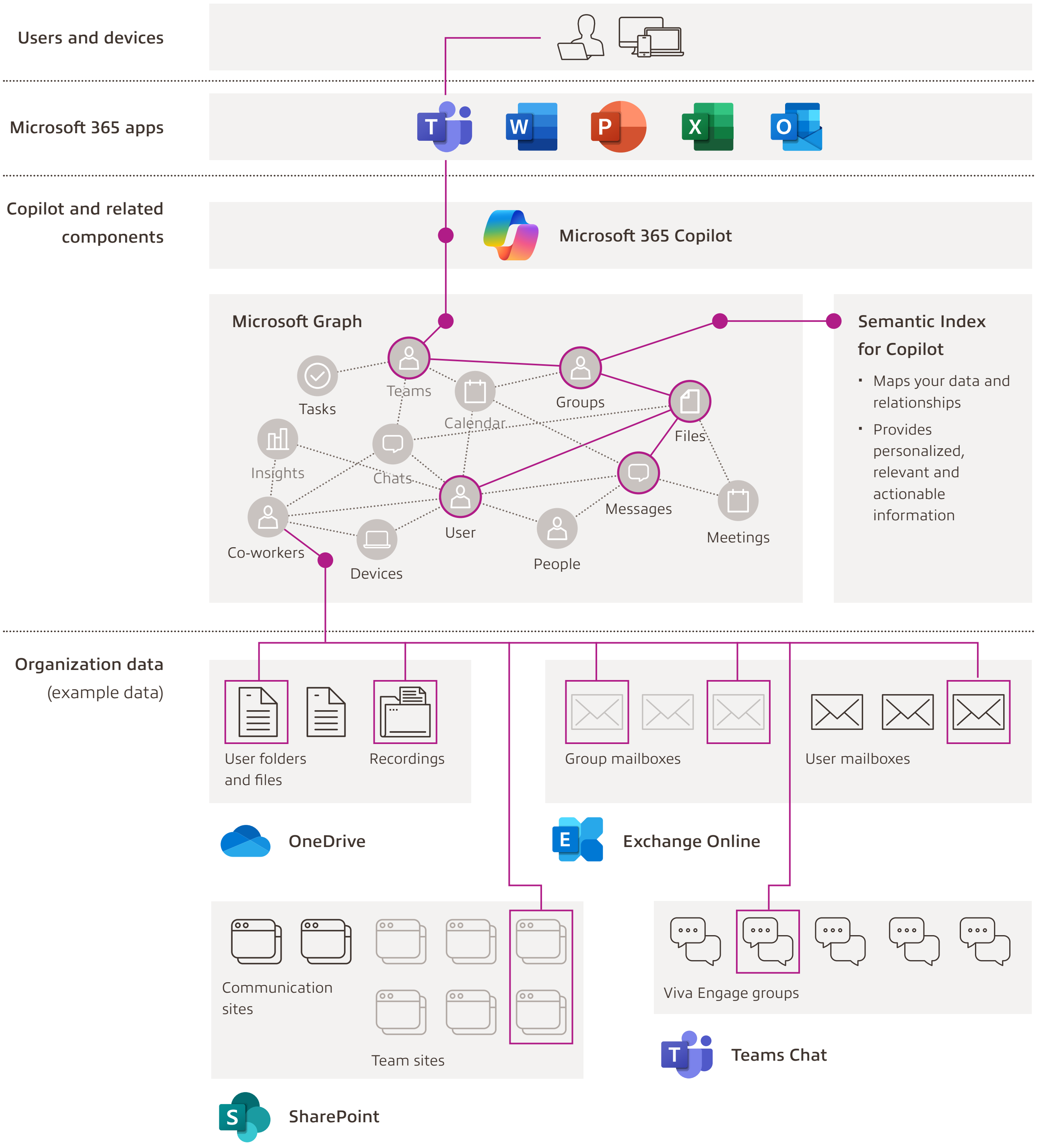
Minimize blast radius for breaches and prevent lateral movement by:

- Segmenting access by network, user, devices and app awareness
- Encrypting all sessions end-to-end
- Using analytics for threat detection, posture visibility and improving defenses

Microsoft 365 Copilot: Logical architecture

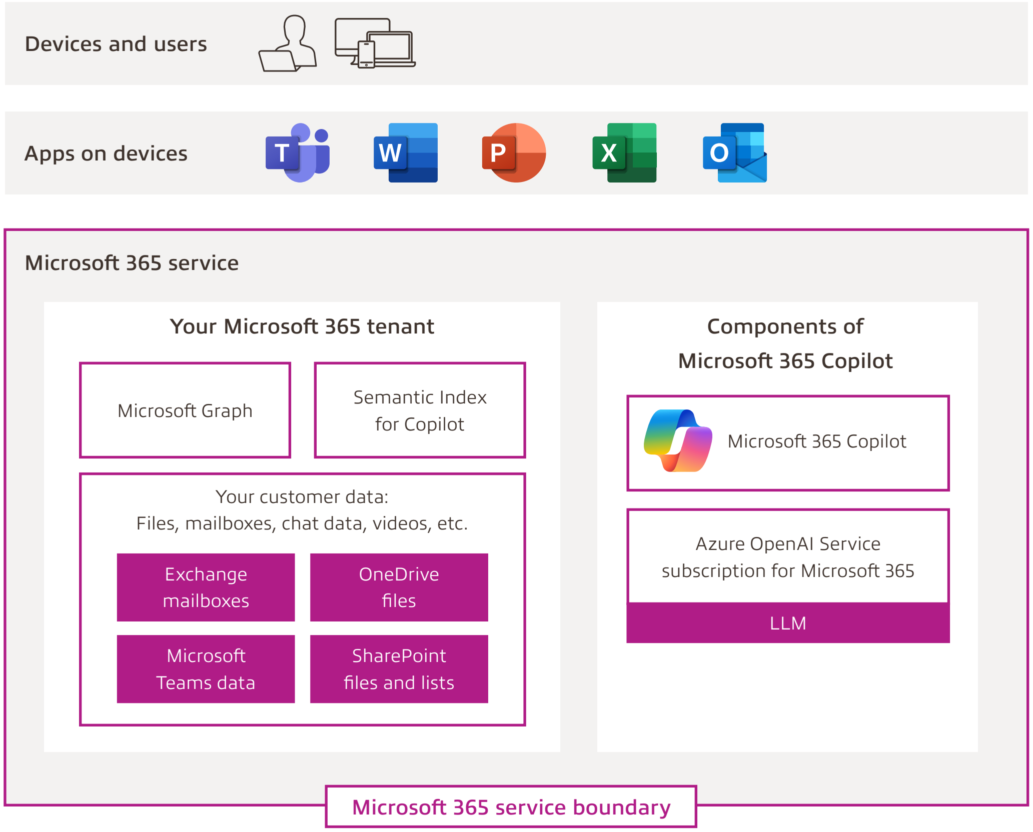
In describing the logical architecture of Microsoft 365 Copilot, we can examine its core components and how they interact. The Copilot service is the component that processes natural language queries from users and returns relevant answers. The Copilot service relies on Microsoft® Graph, a comprehensive API that exposes data and functionality from various Microsoft cloud services. Microsoft Graph connects to your Microsoft 365® tenant. This is the container of your organization's data and resources, including entities such as users and devices, files and folders, team sites and communication sites, mailboxes and chats, recordings and apps.

Your customer data stays within the Microsoft 365 service boundary. Your prompts, responses and data in Microsoft Graph are not used to train foundation Large Language Models (LLMs) that Copilot leverages. Your data is secured based on existing security, compliance and privacy policies already deployed by your organization.



Microsoft 365 Copilot: Service and tenant logical architecture

Your tenant sits inside the Microsoft 365 service boundary, where Microsoft's commitment to security, compliance, data location and privacy is upheld. Copilot is a shared service just like many other services in Microsoft 365. Communication between your tenant and the Copilot components is encrypted.


Devices and users
Apps on devices
Microsoft 365 service
Your Microsoft 365 tenant
Microsoft Graph
Semantic Index for Copilot
Your customer data: Files, mailboxes, chat data, videos, etc.
Exchange mailboxes
OneDrive files
Microsoft Teams data
SharePoint files and lists
Components of Microsoft 365 Copilot
Microsoft 365 Copilot
Azure OpenAI Service subscription for Microsoft 365
LLM
Microsoft 365 service boundary

Semantic Index for Microsoft 365 Copilot

The Semantic Index for Copilot identifies relationships and connections of your user and company data. Together with Copilot and Microsoft Graph, it creates a sophisticated map of all data and content in your organization to enable Copilot to deliver personalized, relevant and actionable responses. The Semantic Index is part of the Microsoft 365 service and is created automatically.

What is currently indexed:

- Semantic Index catalogs text-based files in SharePoint® that are shared with two or more people.
- At the user level, Semantic Index catalogs all email. It also indexes all text-based files in a user's OneDrive® that have been shared, interacted with (even just by the user) or commented on.

Current supported file types include:

- Word documents (.doc/.docx)
- PowerPoint® (.pptx)
- PDF
- Web pages (.html/.aspx)
- OneNote® (.one)

Correlates relationships and understands permissions with Microsoft Graph

Security and information protection recommendations

M365 E5 is the most comprehensive and secure cloud solution for enterprises that want to empower their employees, customers and partners with the best of Microsoft. E5 offers several advantages over E3 in terms of identity and access, Microsoft apps, devices, threat protection, organizational data, teams and external guests.

Identity and access

M365 E5 includes Azure® Active Directory® Premium P2, which provides advanced identity and access management features such as identity protection, privileged identity management, conditional access and access reviews. These features help organizations prevent identity compromise, manage privileged accounts, enforce granular access policies and audit access decisions.

Configure common conditional access policies:

- Require MFA for administrators.
- Require MFA for all users.
- Block legacy authentication.

For hybrid identities, enforce on-premises Microsoft Entra Password Protection for Active Directory Domain Services.

Configure recommended policies for Zero Trust:

- Require MFA when sign-in risk is medium or high.
- Require high-risk users to change their password.
- Configure PIM.

Microsoft apps:

E5 includes Office 365® E5, which provides premium productivity and collaboration apps such as Word, Excel®, PowerPoint, Outlook®, OneNote, Teams®, SharePoint, OneDrive, Yammer® and Stream. In addition, M365 E5 includes advanced capabilities such as Power BI® Pro, Power Apps, Power Automate®, Forms, Planner, To Do and Sway®. These features enable users to create, analyze, automate, and share data and insights across the organization.

Implement Intune App Protection Policies (APPs):

With APP, Intune® creates a wall between your organization data and personal data. Policies ensure corporate data in the apps you specify cannot be copied and pasted to other apps on the device, even if the device is not managed.

Devices

M365 E5 includes Windows® 10 Enterprise E5, which provides the most secure and flexible operating system for enterprise devices. Windows 10 Enterprise E5 includes features such as Windows Defender Advanced Threat Protection, Windows Defender Application Guard, Windows Defender Credential Guard, Windows Defender Device Guard and Windows Defender Exploit Guard. These features protect devices from malware, ransomware, phishing, zero-day attacks and other advanced threats.

Manage devices:

- Enroll devices into management.
- Set up compliance policies.
- Require healthy and compliant devices.
- Deploy device profiles.

Monitor device risk and compliance to security baselines:

- Integrate Intune with Defender for Endpoint to monitor device risk as a condition for access.
- For Windows devices, monitor compliance of these devices to security baselines.

Threat protection

M365 E5 includes Microsoft 365 Defender, which is an integrated security platform that leverages AI and machine learning to detect, investigate and respond to threats across endpoints, email, identity and cloud apps. Microsoft 365 Defender includes Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity and Microsoft Defender for Cloud Apps. These features provide visibility, prevention, detection, response and hunting capabilities for the entire attack surface.

Configure Exchange Online Protection and endpoint protection.

Deploy Microsoft 365 Defender.
For more comprehensive threat protection, deploy Microsoft 365 Defender, including:

- Defender for Identity
- Defender for Office 365
- Defender for Endpoint
- Defender for Cloud Apps

Organizational data

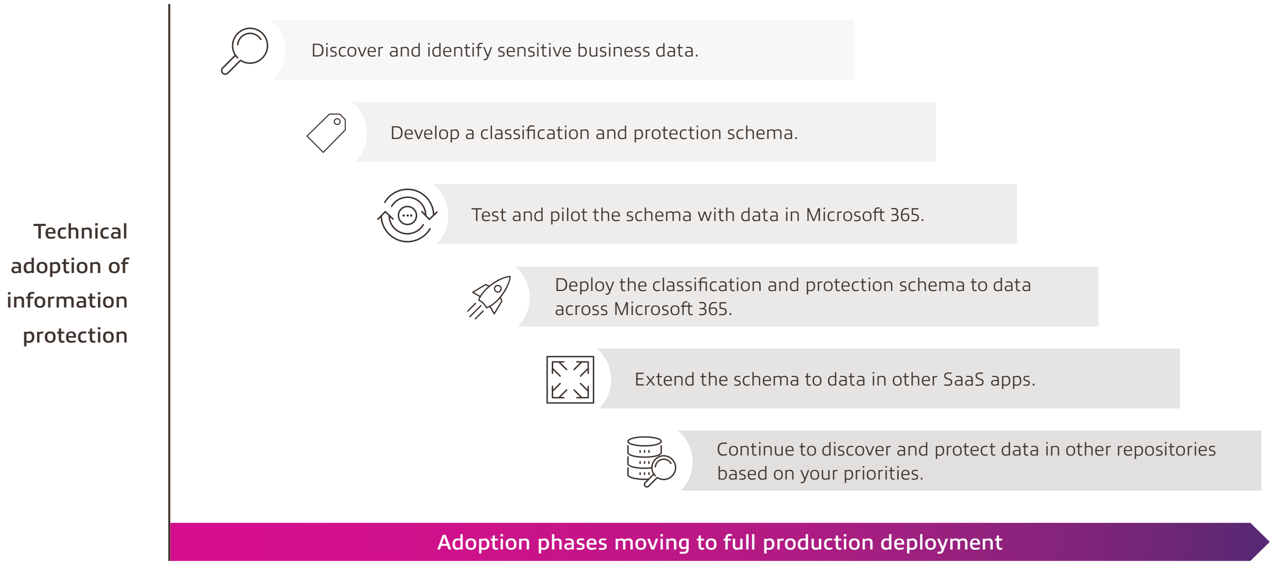
M365 E5 includes Microsoft 365 Compliance, which is a comprehensive solution that helps organizations comply with various regulations and standards such as GDPR, HIPAA, PCI DSS, ISO 27001 and NIST. Microsoft 365 Compliance includes features such as Data Loss Prevention, Information Protection, Records Management, eDiscovery, Audit and Compliance Manager. These features help organizations discover, classify, protect, retain and govern their sensitive data across devices, apps and cloud services.

Develop your classification schema and get started with sensitivity labels and other policies:

- Create data loss prevention policies.
- Create retention policies.
- Use context explorer (to review results).

Extend policies to more data and begin using automation with data protection policies:

- Sensitivity labeling expands to protect more content and more labeling methods.
- Label SharePoint sites and Teams by using container labels and automatically labeling items.



Technical adoption of information protection

Discover and identify sensitive business data.

Develop a classification and protection schema.

Test and pilot the schema with data in Microsoft 365.

Deploy the classification and protection schema to data across Microsoft 365.

Extend the schema to data in other SaaS apps.

Continue to discover and protect data in other repositories based on your priorities.

Adoption phases moving to full production deployment

Teams and external guests

M365 E5 includes Microsoft Teams, which is the hub for teamwork and communication in Microsoft 365. Teams enables users to chat, call, meet, and collaborate with their colleagues and external guests in a secure and compliant way. Teams also integrates with other Microsoft and third-party apps and services to provide a seamless user experience. In addition, M365 E5 includes features such as Teams Phone System, Teams Calling Plan, Teams Audio Conferencing and Teams Live Events. These features enable users to make and receive phone calls, host and join audio conferences, and stream and record live events from Teams.

Highest protection	Sensitive protection	Baseline protection
Very few Teams	Some Teams	Most Teams
First, **identify Teams or projects that warrant highly sensitive protection**. Configure protections for this level. Many organizations don't have data that requires this level of protection.	Next, **identify Teams or projects that warrant sensitive protection** and apply this protection.	Finally, **ensure all Teams and projects are configured for baseline protection**, at minimum.

Set up secure file sharing and collaboration with Microsoft Teams by configuring it with appropriate protection — baseline, sensitive and highly sensitive.

Sharing with people outside your organization

You may need to share information of any sensitivity with people outside your organization. Use these resources:

- **Apply best practices** for sharing files and folders with unauthenticated users.
- **Limit accidental exposure** to files when sharing with people outside your organization.
- **Create** a secure guest sharing environment.

Collaborating with people outside your organization

Use these resources for setting up your environment for collaborating with people outside your organization:

- **Collaborate on documents** — share individual files or folders.
- **Collaborate on a site** — collaborate with guests in a SharePoint site.
- **Collaborate as a team** — collaborate with guests in a team.
- **Collaborate with external participants in a channel** — collaborate with people outside the organization in a shared channel.

Conclusion

Microsoft 365 E5 is the most comprehensive and secure cloud solution for enterprise clients. It offers advanced capabilities for identity and access management, teamwork and communication, data protection and governance, threat protection and response, and business intelligence and analytics. Compared to Microsoft 365 E3, which provides core productivity and security features, Microsoft 365 E5 delivers additional value and protection for your organization.

Highlights

- **Sensitivity labeling** for SharePoint sites and Teams, which allows you to classify and protect your content based on its sensitivity and apply policies such as encryption, access control and retention
- **Automatic labeling of items**, which uses machine learning to detect sensitive information in your documents and emails and apply the appropriate labels and protection policies
- **Teams Phone System, Calling Plan, Audio Conferencing and Live Events**, which enable you to make and receive phone calls, host and join audio conferences, and stream and record live events from Teams, with enterprise-grade security and compliance
- **Defender for Office 365**, which protects your email, collaboration and cloud storage from advanced threats such as phishing, ransomware and Business Email Compromise (BEC)
- **Defender for Endpoint**, which provides Endpoint Detection and Response (EDR), threat and vulnerability management, attack surface reduction, and automated investigation and remediation for your devices
- **Defender for Identity**, which monitors and protects your identity infrastructure from identity-based attacks such as credential theft, privilege escalation and lateral movement
- **Microsoft Entra ID P2**, which enhances your identity and access management with features such as identity protection, privileged identity management, access reviews and entitlement management
- **Power BI Pro**, which enables you to create and share interactive dashboards and reports with rich data visualization and analysis

By upgrading to or exploiting Microsoft 365 E5 licensing, you can leverage these features and more to support and secure your Entra identities, Teams and all of Defender for 365. Microsoft 365 E5 will help you achieve your business goals and digital transformation while keeping your data and users safe and compliant.

Driving innovation with digital transformation

At Insight, we help clients enable innovation with an approach that spans people, processes and technologies. We believe the best path to digital transformation is integrative, responsive and proactively aligned to industry demands. Our client-focused approach delivers best-fit solutions across a scope of services, including the modern workplace, modern applications, modern infrastructures, the intelligent edge, cybersecurity, and data and AI.

Learn more at insight.com.

About the author

Norm Andersch is a senior cybersecurity architect with Insight's modern workplace team. His focus is on creating professional and managed services specifically for security and compliance to help clients strengthen their security programs. Norm holds numerous Microsoft certifications for Azure security, Azure AD and the entire suite of Microsoft Defender solutions.

CPM365-WP-1.0.03.24