Microsoft Security

Securing Copilot for Microsoft 365 in Microsoft 365 for Business

Copilot for Microsoft 365

Unlock productivity and unleash creativity

Natural language

Large language models + Microsoft Graph your data + Microsoft 365 apps + The web

Built on Microsoft's comprehensive approach

Copilot for Microsoft 365 is transforming work

60%

of leaders say a lack of innovation or breakthrough ideas is a concern

64%

of people have struggled with finding time and energy to get their work done

70%

of people indicated they would delegate as much as possible to AI to lessen their workloads

68%

said Copilot improved the quality of their work

70%

said Copilot made them more productive

77%

said they didn't want to give Copilot up

Work trend Index Annual Report: Will AI Fix Work? Microsoft. 9 May 2023 | Microsoft Work Trend Index: What can Copilot's Earliest Users Teach Us About Generative AI at Work?: Microsoft. 15 November 2023

HR

Store, access, and prioritize notes in a fraction of the time

Marketing

Jumpstart the creative process and generate ideas while writing

Data and IT Pros

Effectively manage shared projects and track progress

Copilot for M365 empowers

every end user

Sales

Stay focused on closing deals with an AI assistant for email

Finance

Simplify financial reporting and validating data quality

Customer Service

Stay coordinated as a team to resolve more customer issues

Concerns we've heard from you...

Lack of visibility

58%

of organizations are concerned about the lack of visibility into the use of GenAI[1]

Lack of protection

97%

of organizations have concerns about implementing AI due to the lack of controls to mitigate risks of data leakage[2]

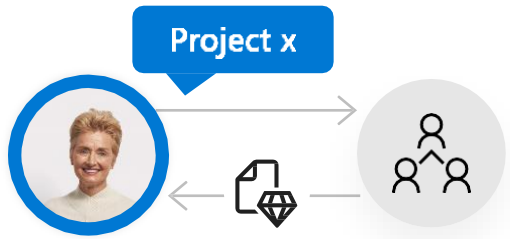
Source:
1. First Annual Generative AI study: Business Rewards vs. Security Risks, , Q3 2023, ISMG, N=400
2. Survey of 658 data security professions, Mar 2023, commissioned by Microsoft

Security and compliance challenges

1

Data oversharing:

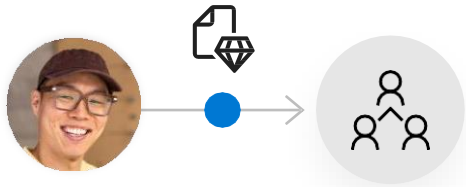
Users may access sensitive data via AI apps they're not authorized to view or edit



2

Data leak:

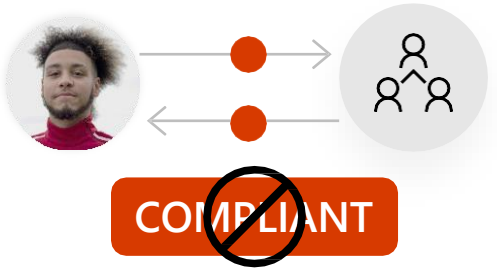
Users may inadvertently leak sensitive data to AI apps



3

Non compliance usage:

Users use AI apps to generate unethical or other high-risk content



Secure and govern Copilot with Microsoft Security

Security + Compliance + Privacy + Responsible AI

Secure access

Manage organization wide search with **Restricted SharePoint Search controls**

Restrict or block risky access with **conditional access**

Control the use of Copilot on devices with **device and application management**

Protect sensitive data

Protect access to sensitive data in Copilot interactions with **sensitivity labeling**

Keep confidential information within your business with **DLP policies**

Understand user activities and detect risky access to Copilot with **audit logging**

Govern Copilot usage

Retain and log Copilot interactions **with retention and deletion policies**

Find information on Copilot interactions with **search and export capabilities**

Manage cases and apply legal hold to **investigate security and compliance incidents**

Security and compliance controls for Copilot for Microsoft 365

Foundational security controls

Microsoft 365 Business Basic or Business Standard

+ Copilot for M365

- **Multi factor authentication (MFA)** to securely access M365 applications to use Copilot
- **Search for and export results** for Copilot prompts and interactions
- **Audit logs** for Copilot interactions
- **Retention or deletion policies** for Copilot interactions on any generated content

Comprehensive security controls

Microsoft 365 Business Premium

+ Copilot for Microsoft 365

- **MFA with Conditional Access** based on identity, device, location, and network
- **Search, export, eDiscovery case management, and legal hold** for Copilot prompts and interactions
- **Audit logs** for Copilot interactions
- **Retention or deletion policies** for Copilot interactions on any generated content
- **Manual sensitivity and retention labels** for content that can be processed by Copilot in files and emails
- **Data loss prevention policies** to help protect sensitive data generated by Copilot in files and emails

Security and compliance add ons available for Business Premium

Microsoft 365 Business Premium provides security and compliance controls that are sufficient for most small and medium sized businesses (SMBs) when using Copilot for Microsoft 365. For those SMBs that require additional security, the following add ons are available to purchase with your Business Premium license.

Information Protection and Governance ($7pupm)

Adds the additional features below to Microsoft 365 Business Premium:

- ***Microsoft Defender for Cloud Apps** helps you discover SaaS apps and protect users from accessing risky apps
- **Communications DLP (Teams chat)** blocks sensitive content when shared with Teams users
- **Endpoint DLP** prevents data leak of sensitive items physical stored on Windows 10/11 and MacOS devices
- **Automatic sensitivity labels (client side)** automatically discover, classify, label and protect sensitive data
- **Machine Learning Based sensitivity Labels** use trainable classifiers to identify items and apply labels
- **Records management** helps manages businesses lega obligations
- **Advanced Message Encryption** helps control sensitive emails shared outside the organization

Insider Risk Management ($6pupm)

Adds the additional features below to Microsoft 365 Business Premium:

- **Insider risk management** helps minimize internal risks by responding to malicious activities
- **Communication compliance** helps detect business code of conduct violations

eDiscovery and Audit ($6pupm)

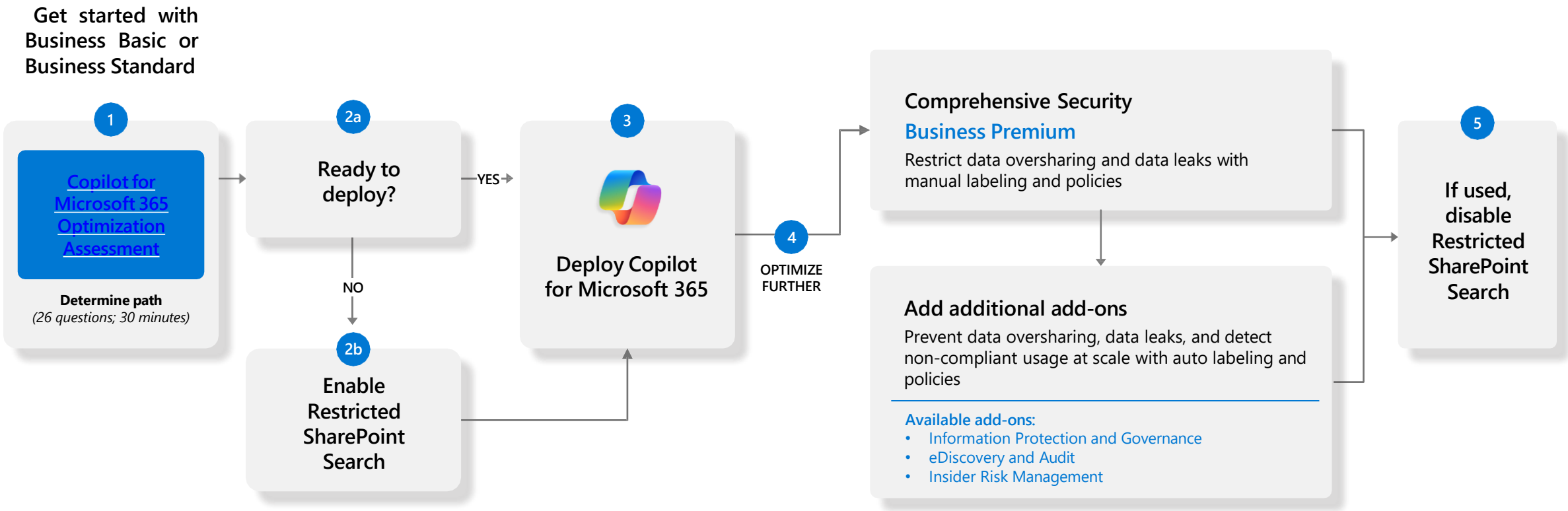
Adds the additional features below to Microsoft 365 Business Premium:

- **eDiscovery (Premium)** with end to end workflow for managing eDiscovery cases and investigations
- **Audit (Premium)** with longer record retention and intelligent insights policies

**Can be purchased as a standalone product*
Note: This may not reflect the full set of features available in these packages. The features identified above are highly relevant when using Copilot for M365.

Take the time to apply appropriate data security solutions with confidence

Copilot for Microsoft 365 includes *Restricted SharePoint Search (RSS)*. It is intended as a solution that can be enabled or disabled while implementing data security solutions. This limits Copilot experiences and organization-wide search to a select set of SharePoint sites. To get the best Copilot experience, we recommend using Business Premium to leverage additional data security features.



Learn more about Restricted SharePoint Search here.

Security and compliance scenarios for Copilot for Microsoft 365

		Foundational		Comprehensive
	Scenario	Business Basic	Business Standard	Business Premium
Identity and access management	Login to Copilot for Microsoft 365 with a single identity	✓	✓	✓
	Enforce MFA when accessing Microsoft 365 to use Copilot	✓	✓	✓
	Enable end user password reset, change, and unlock when accessing Microsoft 365	Cloud users	Cloud users	✓
	Implement Conditional Access policies based on identity, device, and location when accessing Microsoft 365 to use Copilot			✓
	Enable near real time access policies enforcement, evaluate critical events, and immediately revoke access to Microsoft 365			✓
Endpoint management	Push/deploy the Microsoft 365 apps to devices and grant access to Copilot in these apps			✓
	Manage updates for Microsoft 365 apps that use Copilot			✓
	Restrict the use of the Microsoft 365 apps and Teams, as well as Copilot in these apps, on personal devices			✓
	Prevent saving files, including those generated by Copilot, to unprotected apps			✓
	Wipe all work content, including content generated by Copilot, if a device is lost	✓	✓	✓
	Revoke work access on noncompliant devices that have access to Copilot	iOS, Android	iOS, Android	✓
Data security and compliance	Search for Copilot generated data and interactions with eDiscovery capabilities	Search and export results	Search and export results	+ Case management and legal hold
	Audit logs for Copilot interactions	Audit (Standard)	Audit (Standard)	Audit (Standard)
	Apply a manual retention policy for Copilot interactions	✓	✓	✓
	Data Loss Prevention policies to protect sensitive data, generated by Copilot and saved in Microsoft 365 locations, from exfiltration			Files and email
	Inherit sensitivity labels and cite sensitivity label in output and references in Copilot			✓
	Prohibit Copilot from summarizing or including data that users have no extract permissions in its response messages for the saic users	✓	✓	✓
	Exclude sensitive files that users have no view permission from being processed by Copilot for the said users	✓	✓	✓
	Manually label and protect Microsoft 365 content used by Copilot			Files and Email

Scenarios for securing Copilot for Microsoft 365 in across Microsoft 365 for Business

No.	Scenario	Inciting description
1	Access to internal systems and securing the information those systems contain or generate	Companies can offer their employees a variety of tools to help them be productive from anywhere. Increasingly, companies like Northwind Traders are excited about the prospect of generative AI like Microsoft Copilot for Microsoft 365 boosting employee productivity and business outcomes. But access to such powerful tools creates concerns that proprietary and confidential data could get into the wrong hands. The company wants to ensure that only the right people can access internal systems and that their data original material and material generated by Copilot for Microsoft 365 stays within their organization.
2	Access to sensitive data or PII	Whether it's unreleased product information, personally identifiable employee data or confidential information about their clients, companies often store sensitive information within their systems. Generative AI tools like Copilot for Microsoft 365 can be used to access or generate many types of internal information. Northwind Traders is keen to make sure that only appropriate types of information are accessible by specific employees when using Copilot for Microsoft 365.
3	Audit, compliance, and eDiscovery	Documenting compliance with regulatory requirements and preparing for litigation are common business processes for many organizations. With the amount of data consumed or generated with Copilot for Microsoft 365 or other generative AI tools, it is important to make this process straight forward. Northwind Traders' technology and leadership teams want to have the ability to review Copilot for Microsoft 365 interactions for audit, investigation and compliance purposes.

⚠ Challenge

Positioning:
Enable new levels of employee productivity while safeguarding company data and resources

Companies can offer their employees a variety of tools to help them be productive from anywhere. Increasingly, companies like Northwind Traders are excited about the prospect of generative AI like Microsoft Copilot for Microsoft 365 boosting employee productivity and business outcomes. But access to such powerful tools creates concerns that proprietary and confidential data could get into the wrong hands.

The company wants to ensure that only the right people can access internal systems and that their data original material and material generated by Copilot for Microsoft 365 stays within their organization.

The flexibility to access organizational resources on company owned and personal devices can increase employee productivity but can result in vulnerabilities to company data and opportunities for bad actors to gain access or worse, extract data.

Question:
How can companies like Northwind Traders enable new levels of employee productivity with tools like Microsoft Copilot for Microsoft 365 while safeguarding company data and resources?

Solution

Positioning:
Enable new levels of employee productivity while safeguarding company data and resources

Foundational security controls

Microsoft 365 Business Basic or Business Standard
+ Copilot for M365

With Business Basic or Business Standard, companies can

Make sure that unauthorized employees can not use Copilot for Microsoft 365 to gain access to information or confidential data in files that they are not allowed to access.

With the help of relevant capabilities:

- **Login without a password** using multi factor authentication and help ensure only authorized users have access to data
- Ensure **only enrolled, compliant devices can access Microsoft 365 resources** with device based conditional access
- **Wipe all work content**, including content generated by Copilot if a device is lost, stolen or compromised
- **Revoke work access** on noncompliant devices except Windows devices

Comprehensive security controls

Microsoft 365 Business Premium
+ Copilot for Microsoft 365

With Business Premium, companies can *also*:

1. Further prevent external bad actors from getting access to Microsoft 365 resources and protect against employees' mis using Copilot for Microsoft 365 by creating conditions to grant internal access.
2. Reduce the ability for employees or external parties from inappropriately saving or leaking data outside the organization.

With the help of relevant capabilities:

- **Use biometrics to login to your Microsoft 365 account** using Windows Hello for Business (enabled through Windows 11 Pro which is available to BP licenses)
- **Only grant access to Microsoft 365 resources when specific conditions** (identity, device and location) are met using user based conditional access
- Require employees or guests to **accept terms of use** policy prior to getting access to resources
- **Restrict the use of the** Microsoft 365 apps and Teams as well as Copilot in these apps on personal devices
- **Prevent saving files** to unprotected apps
- **Restrict the ability to copy and forward confidential business information** with data loss prevention for emails and files

⚠ Challenge

Positioning:
Keep sensitive or personally identifiable information from being unnecessarily exposed

Whether it's unreleased product information, financial numbers, personally identifiable employee data or confidential information about their clients, companies often store sensitive information within their systems.

Generative AI tools like Copilot for Microsoft 365 can be used to access or generate many types of internal information. Northwind Traders is keen to make sure that only appropriate types of information are accessible by specific employees when using Copilot for Microsoft 365.

Enabling employees to access, analyze, and create data from various parts of an organization can enhance work productivity. However, it also introduces the potential risk of exposing or disclosing confidential or sensitive information.

Question:
How can Northwind Traders ensure that sensitive or personally identifiable information is not unnecessarily exposed when using Copilot for Microsoft 365?

Solution

Positioning:
Keep sensitive or personally identifiable information from being unnecessarily exposed

Foundational security controls

Microsoft 365 Business Basic or Business Standard
+ Copilot for M365

With Business Basic or Business Standard, companies can:

Make sure that unauthorized employees can not use Copilot for Microsoft 365 to gain access to information or confidential data in files that they are not allowed to access.

With the help of relevant capabilities:

- **Change default sharing** options in SharePoint and OneDrive
- **Prohibit Copilot for Microsoft 365 from including sensitive data** that users do not have permissions to view in generated responses
- **Exclude sensitive files** that users do not have permissions to view from being processed by Copilot

Comprehensive security controls

Microsoft 365 Business Premium
+ Copilot for Microsoft 365

With Business Premium, companies can *also*:

Further protect sensitive data by requiring sensitivity labels for Microsoft 365 content. These labels help ensure that only employees with specific permissions can use Copilot for Microsoft 365 to access, generate or share sensitive data. Matching sensitivity labels are automatically applied to any content generated by Copilot for Microsoft 365.

With the help of relevant capabilities:

- **Protect Microsoft 365 data from being accessed by unauthorized users** by implementing manual, default and mandatory content labeling
- **Copilot for Microsoft 365 automatically inherits and applies sensitivity labels** that match any queried material or references

⚠ Challenge

Positioning:
Support regulatory compliance and eDiscovery requests

Documenting compliance with regulatory requirements and preparing for litigation are common business processes for many organizations. With the amount of data consumed or generated with Copilot for Microsoft 365 or other generative AI tools, it is important to make this process straight forward.

Northwind Traders' technology and leadership teams want to have the ability to review Copilot for Microsoft 365 interactions for audit, investigation and compliance purposes.

Growth minded businesses demand a wide variety of tools to maintain their competitive advantage but without the proper systems, keeping a pulse on how these resources are used and the data they generate can be challenging.

Question:
How can Northwind Traders monitor interactions with Copilot for Microsoft 365 and support related regulatory compliance or eDiscovery requests?

Solution

Positioning:
Support regulatory compliance and eDiscovery requests

Foundational security controls

Microsoft 365 Business Basic or Business Standard
+ Copilot for M365

With Business Basic or Business Standard, companies can:

1. Monitor, search and export employee interactions with and any content generated by Copilot for Microsoft 365.
2. Define how long content generated by Copilot for Microsoft 365 should be retained within Microsoft 365.

With the help of relevant capabilities:

- **Search for Copilot interactions** by content and keyword search, and export
- **Maintain a log** of all Copilot for Microsoft 365 interactions within the organization
- **Apply retention or deletion policies** for Copilot interactions and any generated content

Comprehensive security controls

Microsoft 365 Business Premium
+ Copilot for Microsoft 365

With Business Premium, companies can *also*:

Support investigations or other legal processes by asserting a legal hold on material associated with Copilot for Microsoft 365.

With the help of relevant capabilities:

- **Use eDiscovery (standard)** to search for Copilot interactions, export results, manage cases, and apply legal hold to investigate incidents and respond to litigation

Thank you