Microsoft 365

Copilot voor Microsoft 365

Ben jij klaar voor de nieuwe manier van werken?

INDITO.

INHOUD

Waarschijnlijk het machtigste productiviteits-hulpmiddel op aarde

Zal het gebruik van kunstmatige intelligentie (AI) veel impact hebben op bedrijven? Of hebben we het over een trend die gehyped wordt en op een gegeven moment wel zal afvlakken? AI-oplossingen vinden momenteel steeds meer hun weg naar bedrijven, hun processen en bedrijfsactiviteiten. De laatste grote revolutie op het gebied van arbeid is nog niet zo lang geleden: de overstap naar het werken op afstand – hybride en flexibel werken – werd in belangrijke mate aangestuurd en ondersteund door Microsoft dankzij innovaties als Microsoft Teams. En zelfs nu nog is Microsoft een pionier als het gaat om de manier waarop AI-oplossingen ons werk fundamenteel veranderen.

Stel je eens voor: human resources die een combinatie vormen van onvervangbaar menselijk vernuft en de innovatieve mogelijkheden van een veilig en gebruiksvriendelijk AI-systeem.

Met de juiste tools én de juiste mentaliteit kan elke organisatie de overstap maken naar effectief werken met AI-ondersteuning. Dat is precies wat Microsoft Copilot is: niets minder dan 'misschien wel de krachtigste productiviteitstool ter wereld.'
Het komt regelmatig voor op de werkvloer: je werkt in PowerPoint om een overtuigend datagestuurd pitchdeck te creëren voor een potentiële nieuwe klant. Het vinden van de juiste achtergrondinformatie en cijfers kan veel tijd kosten. Copilot helpt je hierbij en haalt relevant onderzoek uit andere documenten die je al hebt gemaakt om de belangrijkste onderwerpen van uw pitch te benadrukken. Wat vroeger uren tijd kostte, is in een mum van tijd gedaan.

Of stel je voor dat je terugkomt van een week vakantie en je e-mails probeert te checken. Met Copilot in Outlook is opruimen van een 'rommelige' inbox een taak die maar een paar minuten duurt, zodat je weer snel productief kunt zijn.

Ga met ons mee op een spannende reis door de wereld van Microsoft Copilot, vanaf de eerste dagen van de voorbereiding tot het spannende moment van lancering. Laat je inspireren en ontdek hoe Microsoft Copilot de spelregels verandert en tegelijkertijd jouw databeveiligng in de gaten houdt.

DE ROL VAN COPILOT IN EEN MODERNE WERKOMGEVING

Copilot is veel meer dan alleen een hulpmiddel; het is een krachtige productiviteitstool die naadloos is geïntegreerd in het dagelijks leven en kan worden gebruikt in toepassingen zoals Word, Ecxel en PowerPoint. Het neemt werk van de contentproductie niet over, maar stimuleert het met productiviteitsverhogende ondersteuning, krachtige tools en intelligente inzichten. Een unieke functie is de mogelijkheid om met Copilot te communiceren via natuurlijke spraakopdrachten, mogelijk gemaakt door het innovatieve Microsoft 365 Chat in Teams. Deze functie maakt gebruik van gegevens uit agenda's, e-mails, chats, documenten, vergaderingen en contacten en kan daarmee taken uitvoeren die voorheen ondenkbaar waren.

Copilot kan bijvoorbeeld op verzoek een productstrategie-update genereren op basis van informatie uit vergaderingen, e-mails en chatgeschiedenis.

Hieronder zes casevoorbeelden van hoe Copilot kan helpen bij je dagelijkse werk.

1. Geautomatiseerde data-analyse in Excel

Copilot kan snel trends analyseren, geavanceerde berekeningen uitvoeren en uitgebreide rapporten maken en zo uren handmatig werk besparen. Dit is vooral ideaal voor medewerkers op financiële afdelingen.

2. Efficiënt e-mailmanagement in Outlook

Laat Copilot je e-mailbeheer optimaliseren door belangrijke e-mails prioriteit te geven en passende reacties te plannen. Je inboxen zij efficiënter georganiseerd, zodat je minder tijd kwijt bent aan het doorzoeken van e-mails. Dit kan met name voordelig zijn voor administratief personeel en medewerkers van de klantenservice.

3. Betere documenten maken in Word:

Creëer effectievere documenten met Copilot. Copilot stelt optimalisaties voor qua inhoud, opmaakopties en genereert zelfs teksten op basis van korte instructies, waardoor het proces voor het maken van documenten aanzienlijk wordt versneld. Vooral administratieve en marketing-medewerkers kunnen zo in minder tijd betere resultaten behalen.

4. Geautomatiseerde planning in Teams

Soms lijkt het bijna onmogelijk om voor iedereen die bij een project betrokken is een geschikt vergadermoment te vinden. Copilot helpt bij het plannen van vergaderingen in Microsoft Teams door agenda-informatie en beschikbaarheid van deelnemer te analyseren en automatisch vergaderingen te plannen om ervoor te zorgen dat alle deelnemers beschikbaar zijn. Vooral handig voor administratief personeel of grote teams met verschillende beschikbaarheid.

5. Beter presentaties maken in PowerPoint:

Gebruik eenvoudige aanwijzingen en maak professionele en creatieve presentaties met Copilot. Copilot voegt automatisch relevante content uit je bron-documenten toe.

6. Verbeterde data-visualisatie in Excel:

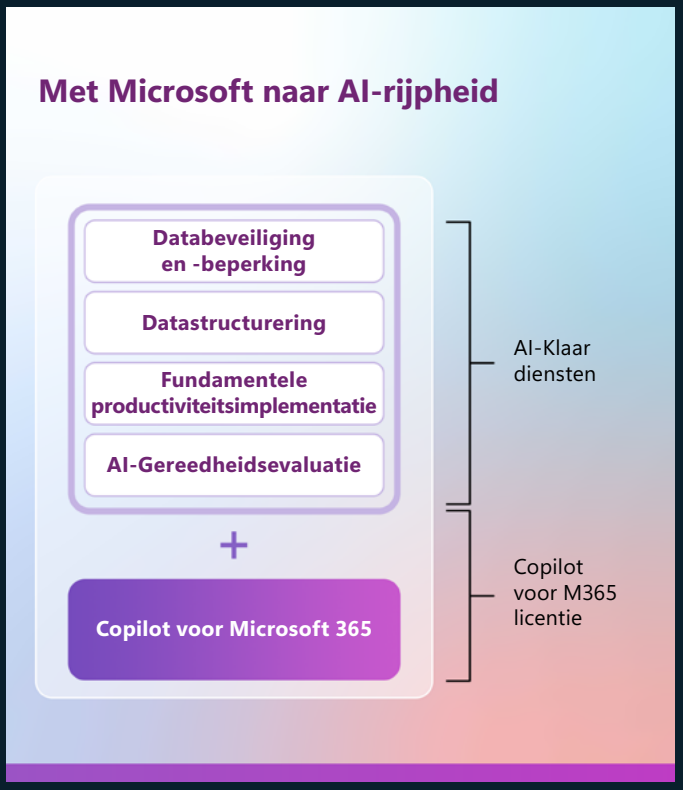
Copilot kan je helpen bij het maken van professionele datavisualisaties in Excel door automatisch diagrammen en grafieken te genereren en relevante gegevens uit bron-documenten toe te voegen. Medewerkers van financiële afdelingen kunnen zo in een mum van tijd aantrekkelijke en relevante grafieken en documenten produceren.

MAAK JE ORGANISATIE AI READY

Platformtransitie naar AI kan niet plaatsvinden zonder duidelijk leiderschap en gerichte aanpak. Het implementeren van AI-technologe kan complex zijn, vooral zonder een duidelijk omschreven plan vooraf. Het vereist een cultuur van productiviteit en samenwerking, een veilige basis voor end point management en de bereidheid om veranderingen te omarmen. Ben jij klaar om het AI-tijdperk te betreden? Stel jezelf de volgende vier vragen om erachter te komen:

- **Beschik je over een uitgebreide zero trust architectuur?**
- **Zijn je endpoints en apps makkelijk te managen?**
- **Zijn je data gestandaardiseerd en makkelijk toegankelijk?**
- **Is je organisatie klaar voor AI?**

Kun je al deze vragen met ‘ja’ beantwoorden? Mooi, dan is jouw organisatie klaar voor de inzet van kunstmatige intelligentie. Is dat niet het geval, geen probleem. Laten we er samen aan gaan werken.



Ons aanbod voor jouw AI-plan

Hoe ziet 'AI-klaar zijn' eruit?

Een bedrijf dat klaar is voor AI begrijpt zijn eigen potentieel als strategische bron, weet hoe dit in het voordeel van het bedrijf gebruikt kan worden en is in staat medewerkers en klanten goed te begeleiden in het verantwoord gebruiken van AI. Het beoordelen van wel of niet klaar zijn voor AI is de eerste stap in het transformeren naar een organisatie die de veranderingen en uitdagingen van deze nieuwe wereld van werken met next gen technologiën zoals AI omarmt. Het lijkt geen twijfel dat Copilot de potentie heeft om werkenden te inspireren tot een nieuw niveau op het gebied van creativiteit, productiviteit en samenwerking. Het helpt mensen om hun doelen te herontdekken en verhoogt de efficiency op een opwindende en transformatieve manier. Met de steun van betrokken personeel en hun eigen unieke menselijke kwaliteiten – intuïtie, empathie en kritisch denken – kan Copilot mensen in staat stellen beter en met een duidelijker doel voor ogen te werken.

Het optimaliseren van data

Ook de kwaliteit van je bedrijfsdata is cruciaal voor het succes van Microsoft Copilot. Een zorgvuldige organisatie en opschoning van data is essentieel om optimale resultaten te behalen. Onjuiste of ongepaste gegevens kunnen de prestatie van Copilot beïnvloeden of zelfs hinderen. Het is essentieel om uw gegevens efficiënt op te slaan, te beheren en te categoriseren om het maximale uit Copilot te halen en ongewenste toegang tot gevoelige informatie te voorkomen.

Belangrijke stappen bij de implementatie van Copliot zijn onder andere het intrekken van verouderde machtigingen, het identificeren en beschermen van gevoelige gegevens en het monitoren op afwijkingen en potentiële risico's. Door tijdig controles op gegevenstoegang uit te voeren en goed te letten op de naleving van gegevensbescherming kun je ervoor zorgen dat je gevoelige informatie én je organisatie beschermd worden. Indien nodig kun je dataspecialisten inschakelen om de voortgang veilig te versnellen. Deze stap is cruciaal om vanaf het begin alle voordelen van Copilot te benutten, de adoptie te stimuleren en de blijvende waarde ervan voor je organisatie te garanderen.

Zero Trust

Het Zero Trust-model vormt een onmisbare basis voor het gebruik van Copilot en AI in de bedrijfscontext.
In een tijdperk waarin data zowel een waardevolle hulpbron als een potenteel veiligheidsrisico zijn, garandeert de 'nooit vertrouwen, altijd verifiëren'-filosofie van Zero Trust de veiligheid en integriteit van gegevens. Dit is essentieel voor AI-toepassingen zoals Copilot. Door elke toegangspoging tot het netwerk voortdurend te controleren, zorgt Zero Trust ervoor dat alleen geauthenticeerde en geautoriseerde verzoeken worden verwerkt, waardoor de basis wordt gelegd voor veilig en effectief gebruik van AI technologiën in je bedrijf. Microsoft ondersteunt de implementatie van het Zero Trust-model met bewezen beveiligingsoplossingen – en diensten. Met tools zoals Entra ID en Microsoft Defender kunnen bedrijven krachtige identificatieverificatie, voortdurende monitoring van netwerkactiviteit en geavanceerde detectie van bedreigingen implementeren.

Centraliseren en bewaken van endpoints

Gecentraliseerd endpoint management is cruciaal voor het gebruik van Copilot en AI in bedrijven, vooral in een arbeidswereld die gekenmerkt wordt door flexibiliteit en hybride werkmodellen. Moderne manieren van werken brengen vaak het gebruik van verschillende apparatuur met zich mee zoals laptops en smartphones, zowel op kantoor als werken vanuit huis of onderweg. Gecentraliseerd beheer van deze endpoints zorgt ervoor dat alle apparaten veilig, up-to-date en efficiënt blijven.

Dit is met name belangrijk omdat de verwerking van gevoelige informatie en de bescherming tegen cyberaanvallen belangrijke uitdagingen zijn. Bovendien verbetert efficiënt apparaatbeheer de gebruikerservaring en ondersteunt het de naleving van compliancerichtlijnen. Al deze aspecten zijn essentieel om de voordelen van AI-technologieën zoals Copiot te maximaliseren in en veilige en efficiënte werkomgeving.

De reeks illustraties in de bijlage biedt een overzicht van nieuwe onderdelen van de logische architectuur. Het bevat aanbevelingen voor het voorbereiden van uw omgeving voor Copilot met beveiliging en gegevensbescherming tijdens het toewijzen van licenties.

IS JOUW ORGANISATIE KLAAR VOOR COPILOT?

Laten we een korte test doen om te bepalen hoe goed jouw bedrijf is voorbereid op het gebruik van Copilot. Elke vraag heeft mogelijke antwoorden. Kies degene die het beste aansluit bij de huidige situatie van je bedrijf en noteer de antwoorden.

Aan het eind van deze AI-check kun je beoordelen of je bedrijf er helemaal klaar voor is, bijna klaar of dat er verdere ondersteuning nodig is.

Open mind ten opzichte van verandering en innovatie:

A ■ Ons bedrijf is zeer innovatief en staat open voor verandering.

B ☐ We staan er in principe op in, maar op sommige gebieden aarzelen we nog.

C ☐ We zijn traditioneel en twijfelen als het om innovaties gaat.

Vertrouwen in productiviteit met de huidige technologie:

A ☐ We hebben er alle vertrouwen in dat onze medewerkers effectief kunnen werken met de huidige technologie.

B ☐ Er zijn wat onzekerheden, maar over het algemeen hebben we er vertrouwen in.

C ☐ We hebben twijfel over de technologische vaardigheden van onze medewerkers.

Het belang van AI voor zakelijk succes:

A ☐ AI is een beslissende factor voor ons succes.

B ☐ AI heeft bij ons zeker betekenis, maar is niet doorslaggevend.

C ☐ AI speelt momenteel geen rol van betekenis bij ons.

Medewerkers open-minded ten opzichte van AI:

A ☐ Onze medewerkers staan absoluut open voor AI.

B ☐ Sommigen zijn ruimdenkend, andere staan er sceptisch tegenover.

C ☐ Er bestaat onder onze medewerkers veel scepsis tegenover AI.

Hoe modern is de IT-infrastructuur:

A ☐ Onze IT-infrastructuur is volledig up-to-date. We vertrouwen op Cloud-identities en hebben Zero Trust al geïnstalleerd.

B ☐ Wij hebben deels over Cloud-based systemen, maar ook on-premise componenten.

C ☐ Onze IT-infrastructuur is grotendeels een lokale structuur.

Databeveiliging and veiligheidsmaatregelen:

A ☐ Er zijn bij ons uitgebreide richtlijnen en harde beveiligingsmaatregelen van kracht.

B ☐ Er zijn basisrichtlijnen en -maatregelen, maar er is behoefte aan verbetering.

C ☐ Er is een duidelijk gebrek aan richtlijnen en maatregelen op dit gebied.

Gebruik van Microsoft 365 producten:

A ☐ In ons dagelijks werk maken we intensief gebruik van Microsoft 365 producten. Onze gegevens worden opgeslagen in de Cloud en Teams is een an onze belangrijkste communicatiemiddelen.

B ☐ Microsoft 365 producten worden bij ons deels gebruikt.

C ☐ Wij maken geen gebruik van Microsoft 365 producten of de Cloud.

Implementatie van een evergreen IT-strategie:

A ☐ Onze IT-strategie wordt voortdurend bijgewerkt en aangepast om gelijke tred te houden met de technologische veranderingen.

B ☐ We streven ernaar om up-to-date te zijn, maar er zijn gebieden die nog gemoderniseerd moeten worden.

C ☐ Traditioneel vertrouwen we op patchdagen en vaste uitrolcycli en wachten graag met het implementere van nieuwe productversies.

Investeren in verandermanagement:

A ☐ We investeren actief in verandermanagement en beschikken bijvoorbeeld over change agents die ervoor zorgen dat onze teams effectief met veranderingen kunnen omgaan en zich verder kunnen ontwikkelen.

B ☐ Er zijn enkele inspanningen op het gebied van verandermanagement, maar deze zijn niet alomvattend of systematisch.

C ☐ We hebben nog niet geïnvesteerd in verandermanagement en het ontbreekt aan structuren om veranderingsprocessen te ondersteunen.

Resultaat:

Tel hier je antwoorden bij elkaar op:

A _____ maal

B _____ maal

C _____ maal

Evaluatie van de quiz:

Meest antwoorden zijn a):
Je organisatie is goed voorbereid om Copilot effectief te gebruiken. Jullie beschikken over een geavanceerde IT-infrastructuur, een ruimdenkend team en de nodige middelen om Copilot succesvol te integreren. Het is raadzaam om deze sterke punten te gebruiken om de implementatie vooruit te helpen en optimaal te profiteren van Copilot.

Mix van a) en b) antwoorden:
Je bedrijf is goed op weg, maar heeft nog wel enkele aanpassingen nodig om het maximale uit Copilot te halen. Het is goed om specfieke gebieden in kaart te brengen waar verbeteringen nodig zijn, zoals verdere opleiding van medewerkers of het updaten van de IT-infrastructuur. Een gericht plan om deze punten aan te pakken zal het gebruik van Copilot vergemakkelijken.

Vooral b) of c) antwoorden:
Je organisatie heeft verdere ondersteuning nodig om Copilot effectief te gebruiken. Dit kan een fundamentele herziening van de IT-infrastructuur, een intensievere opleiding van medewerkers of een strategische herschikking ten op zichte van nieuwe technologieën omvatten. Belangrijk is om te beseffen dat de introductie van Copiloet een uitgebreide voorbereiding en maatwerk vraagt. Tip: overweeg om deskundigen te raadplegen of externe bronnen aan te boren om dit proces te ondersteunen.

ZES TIPS OM COPILOT SUCCES VOL TE GEBRUIKEN.

Copilot heeft de potentie om de manier waarop je werkt radicaal te veranderen, maar een succesvolle implementatie hangt af van strategische planning en uitvoering. Hier zijn zes waardevolle tips om je op weg te helpen:

1. Bereid je data voor:

Copilot heeft een grote hoeveelheid gegevens nodig om effecief te kunnen werken. Zorg ervoor dat de databases en datasets up-to-date zijn en dat ze een format hebben dat Copilot kan verwerken.

2. Train je medewerkers:

Copilot is een krachtig hulpmiddel, maar vereist ook enige training om het effectief te kunnen gebruiken. Zorg ervoor dat je medewerkers over de nodige vaardigheden en kennis beschikken om Copilot te gebruiken.

3. Creëer een duidelijke autorisatiestructuur:

Copilot heeft toegang tot verschillende databronnen en het is belangrijk dat je medewerkers alleen toegang hebben tot de gegevens die zij nodig hebben. Creëer een duidelijke autorisatiestructuur om ervoor te zorgen dat alle gegevens veilig zijn.

4. Creëer een heldere strategie:

Voordat je Copilot introduceert, moet er een duidelijke strategie liggen over hoe je de tool wilt gebruiken. Stel doelen en definieer hoe je het succes van Copilot gaat meten.

5. Laat medewerkers Copilot gebruiken:

Copilot is zo goed als de data waartoe het toegang heeft. Zorg er dus voor je medewerkers Copilot gebruiken, zodat de gebruikte gegevens actueel zijn.

6. Creëer een heldere communicatiestrategie:

Zorg ervoor dat je medewerkers op de hoogte zijn van de introductie van Copilot en hoe dit hen kan helpen. Creëer een heldere communicatiestrategie om ervoor te zorgen dat je medewerkers zich bewust zijn van de voordelen die Copilot hen biedt.

Ons aanbod voor jouw AI-plan

Wil je meer weten over Copilot voor Microsoft 365 of wil je persoonlijk benaderd worden over dit onderwerp? Neem contact met ons op!

INDITO.

ZERO TRUST: ARCHITECTURE & DEPLOYMENT

Microsoft Copilot for Microsoft 365 architecture & deployment

Copilot combines the power of large language models (LLMs) with your data in the Microsoft Graph — your calendar, emails, chats, documents, meetings, and more — and the Microsoft 365 apps to provide a powerful productivity tool.

Microsoft Copilot for Microsoft 365 logical architecture

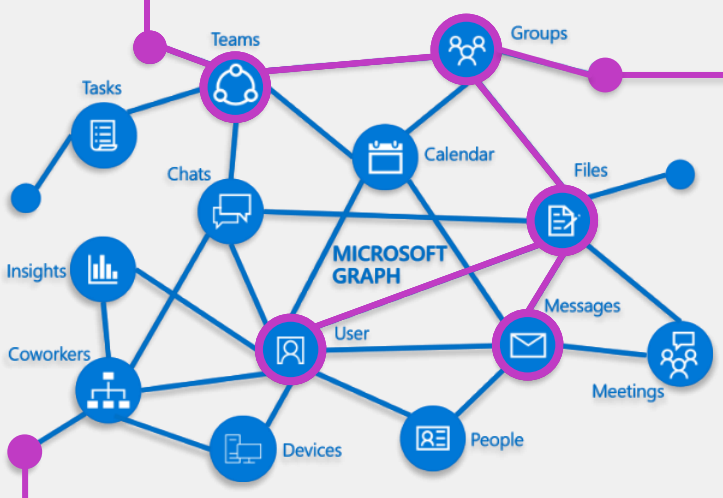
Microsoft Copilot for Microsoft 365 or Copilot introduces several components to help users make use of content and data they already have access to. Note that only data a user has access to is returned in query responses (as illustrated).

Users and devices

Microsoft 365 apps

Copilot and related components

Copilot for Microsoft 365



Microsoft Graph

Semantic Index for Copilot

Maps your data and relationships

Provides personalized, relevant, and actionable information

Organization data (Example data)

OneDrive

User folders and files

Recordings

Exchange Online

Group mailboxes

User mailboxes

SharePoint

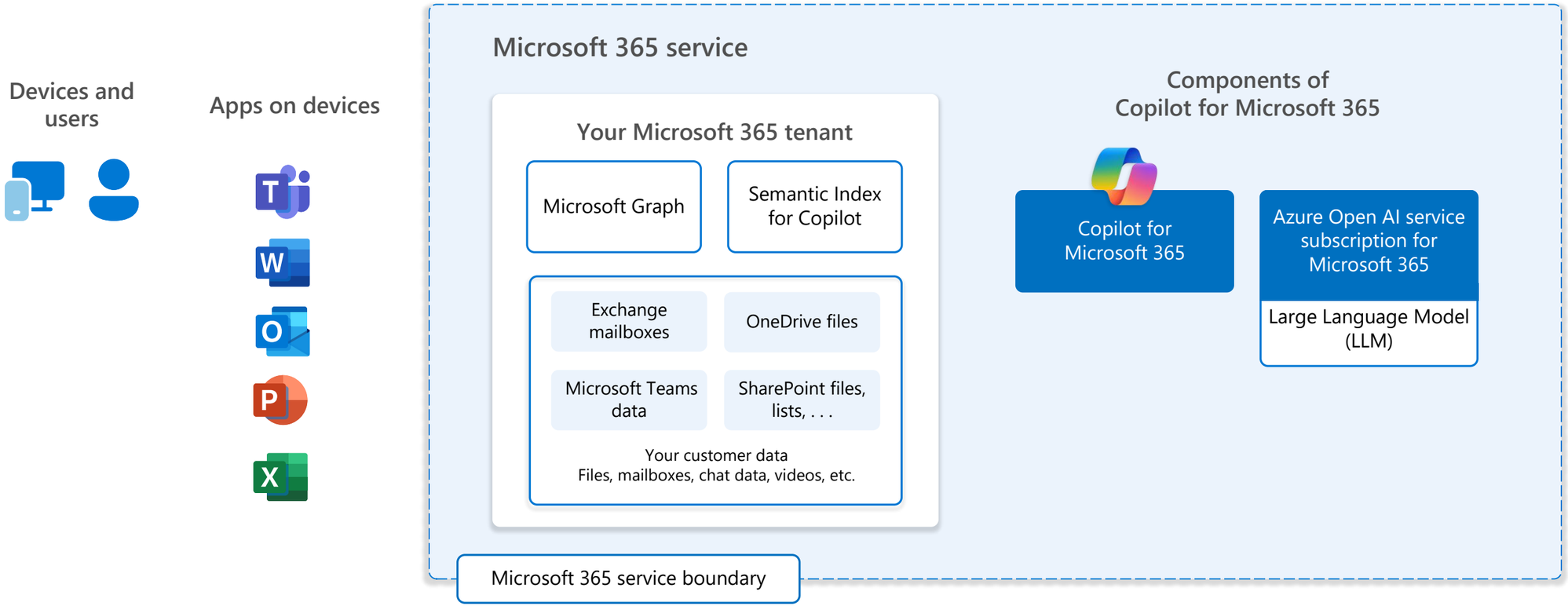
Communication sites

Team sites

Teams Chat

Viva Engage groups

Microsoft Copilot for Microsoft 365 service and tenant logical architecture



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

Your tenant sits inside the Microsoft 365 service boundary, where Microsoft's commitment to security, compliance, data location, and privacy are upheld.

Copilot is a shared service just like many other services in Microsoft 365. **Communication between your tenant and Copilot components is encrypted.**

For more information, see Data, Privacy, and Security for Copilot for Microsoft 365.

Semantic Index for Microsoft Copilot for Microsoft 365

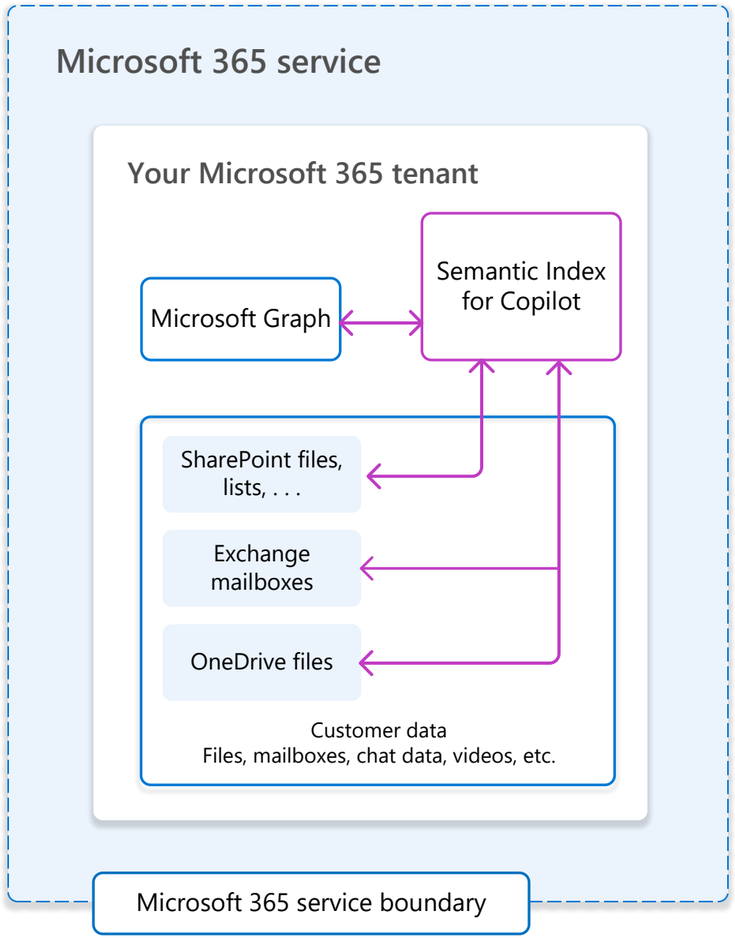
The Semantic Index for Copilot is a separate index or map of your user and company data — identifying relationships and connections. It works with Copilot and the Microsoft Graph to create a sophisticated map of all data and content in your organization to enable Copilot to deliver personalized, relevant, and actionable responses. The Semantic Index is part of the Microsoft 365 service and is created automatically.

Semantic indexing vs keyword indexing

Semantic Index builds upon keyword matching, personalization, and social matching capabilities within Microsoft 365 by creating vectorized indices to enable conceptual understanding, which helps determine your intent and helps you find what organizational content you need.

Unlike a standard keyword index, vectors are stored multi-dimensional spaces where semantically similar data points are clustered together in the vector space, enabling Microsoft 365 to handle a much broader set of search queries beyond "exact match."

Each dimension of a vector captures an aspect of semantic meaning of the data point being represented. This provides for fast and accurate search and retrieval of data based on vector distance or similarity. This means that instead of using traditional methods for querying based on exact matches or predefined criteria, the Semantic Index finds the most similar or relevant data based on the semantic or contextual meaning.



What is currently indexed

- Semantic Index indexes text-based files in SharePoint that are shared with two or more people.
- At the user level, Semantic Index indexes 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)
- Semantic Index leverages the Microsoft Graph to better correlate relationships and understand permissions.

Excluding SharePoint Online sites

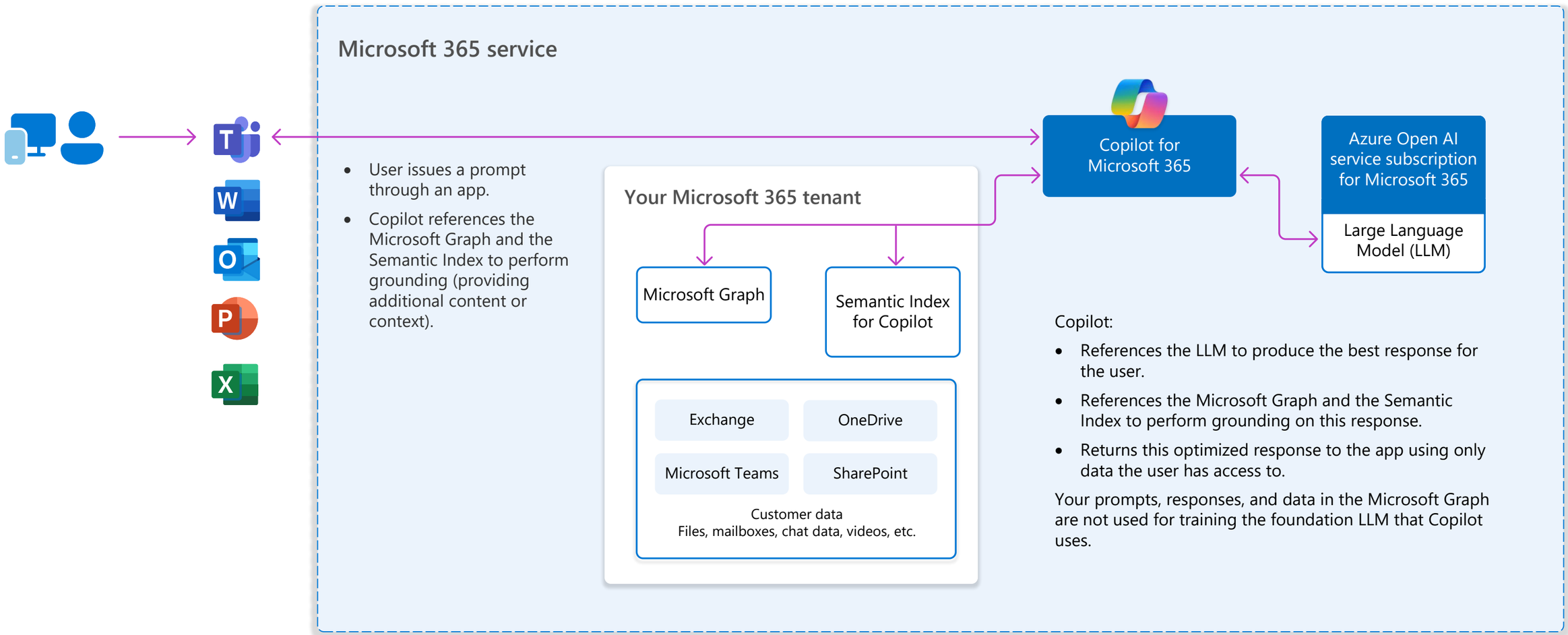
You can exclude a SharePoint Online site from being indexed by both Microsoft Search and the Semantic Index (such as payroll data or financial information). Site administrators select this option within the Site Settings page.

Additional resources

Video — Semantic Index for Copilot: Explained by Microsoft

Training article — Examine how Copilot uses the Semantic Index (MS-012 Prepare your organization for Copilot for Microsoft 365)

Microsoft Copilot for Microsoft 365 query flow



Prepare your environment for Microsoft Copilot for Microsoft 365

Security and information protection recommendations

Microsoft recommends building a foundation of secure productivity to get AI-ready, including Microsoft Copilot for Microsoft 365 or Copilot.

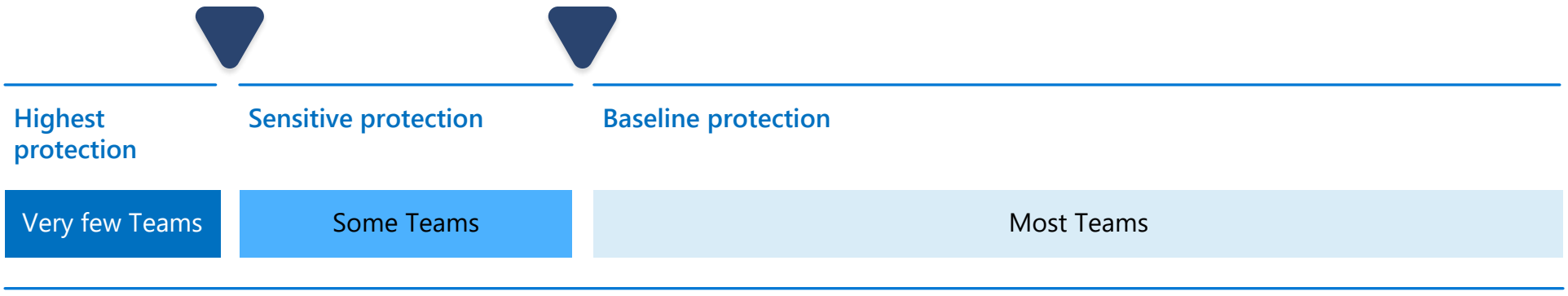
Area to protect	Getting started with E3	Next steps with E5
Identity and access	**Configure common conditional access policies** With Microsoft Entra ID P1, configure the following policies to use multi-factor authentication (MFA): • Require MFA for administrators • Require MFA for all users • Block legacy authentication See Common Conditional Access policies. Be sure Microsoft 365 Services and your other SaaS apps are included in the scope of these policies. If your environment includes hybrid identities, also enforce on-premises Microsoft Entra Password Protection for Active Directory Domain Services.	**Configure recommended policies for Zero Trust** With Microsoft Entra ID P1, configure the following policies to use multi-factor authentication (MFA): • Require MFA when sign-in risk is medium or high • Block legacy authentication • Require high risk users to change their password See Common security policies for Microsoft 365 organizations. Also configure Privileged Identity Management.
Microsoft 365 Apps	**Implement Intune App Protection policies (APP)** 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. See Implement App Protection policies.	
Devices	**Manage devices** After devices are enrolled, set up compliance policies and then require healthy and compliant devices. Finally, deploy device profiles to manage settings and features on 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. See Monitor device risk and compliance to security baselines.
Threat protection	**Configure Exchange Online Protection and endpoint protection** Exchange Online Protection (EOP) helps protect your email and collaboration tools from phishing, impersonation, and other threats. You can rapidly apply these protections by configuring preset security policies. Microsoft Defender for Endpoint P1 includes Attack surface reduction and Next generation protection for antimalware and antivirus protection. See Overview of Microsoft Defender for Endpoint Plan 1.	**Pilot and deploy Microsoft 365 Defender** For more comprehensive threat protection, pilot and deploy Microsoft 365 Defender, including: • Defender for Identity • Defender for Office 365 • Defender for Endpoint • Defender for Cloud Apps See Evaluate and pilot Microsoft 365 Defender.
Organization data	**Develop your classification schema and get started with sensitivity labels and other policies** Sensitivity labels form the cornerstone of protecting your data. Before you create the labels to denote the sensitivity of items and the protection actions to be applied, understand your organization's existing classification taxonomy and how it will map to labels that users will see and apply in apps. Create data loss prevention policies Create retention policies Use content explorer (to review results)	**Extend policies to more data and begin using automation with data protection policies** Sensitivity labeling expands to protecting more content and more labeling methods. For example, labeling SharePoint sites and Teams by using container labels, and automatically labeling items in Microsoft 365 and beyond. For more information, see a list of common labeling scenarios and how they align to business goals.

Set up secure file sharing and collaboration with Microsoft Teams

Configure Microsoft Teams with appropriate protection

Microsoft provides guidance for protecting your Teams at three different levels – baseline, sensitive, and highly sensitive. Guidance includes sensitivity labels and site sharing settings.

Introducing Copilot is a good time to review your environment and ensure that appropriate protection is configured.



1. 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.
2. Next, identify Teams or projects that warrant sensitive protection and apply this protection.
3. Finally, ensure all Teams and projects are configured for baseline protection, at a minimum.

Resources

- Set up secure file sharing and collaboration with Microsoft Teams
- Compare levels of protection
- Configure Teams with three tiers of protection

Configure external sharing with appropriate security

Introducing Copilot is a good time to review your policies for sharing files with people outside your organization and for allowing external contributors. Note that guest accounts are not licensed to use Copilot.

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

Pilot and deploy Microsoft Copilot for Microsoft 365

Onboard users to Microsoft Copilot for Microsoft 365

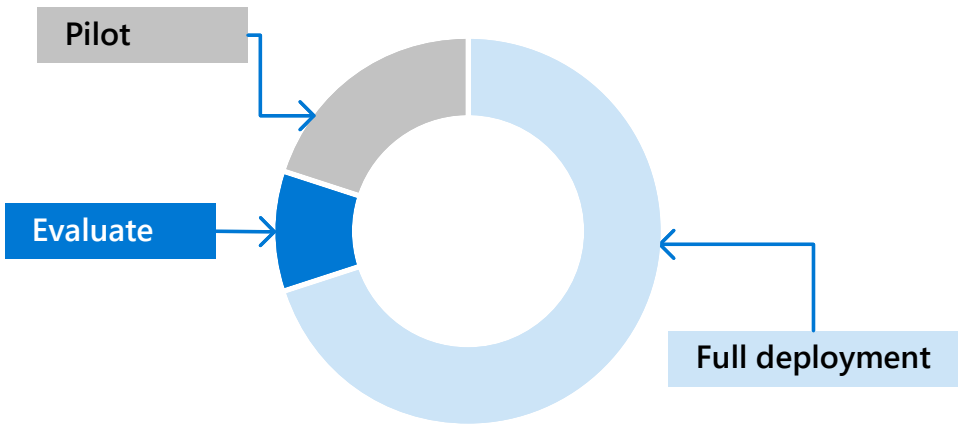
Microsoft recommends deploying Copilot as you phase in protections for access, devices, and data. Whether you're starting with Microsoft 365 E3 or you're taking next steps with Microsoft 365 E5, use the following sequence:

1. Apply identity and access protection.
2. Apply device protection.
3. Assign Copilot licenses to users with these protections.

Ongoing — Continue your deployment of information protection capabilities.

Begin by building a plan and then testing the plan. Then roll out new configurations and capabilities incrementally. This provides the opportunity to improve on the plan while lessons are learned.

The following diagram illustrates the recommendation to start a project with a small group to evaluate the changes. This small group can be members of your IT team or a partner team. Then, pilot the changes with a larger group. Full deployment is accomplished by gradually increasing the scope of the deployment until your whole organization is covered.



Applying protections and deploying Copilot in parallel

	Evaluate	Pilot	Full deployment
Identity and access	Identify 50 users for testing	Identify the next 50-100 users in the production environment	Apply protections to the rest of the users in larger increments
Devices	Test device protections with the same 50 users	Apply device protections to the same users	Enroll the rest of the endpoints in larger increments
Copilot	Assign Copilot licenses to users AFTER their account and devices are protected		

Technical adoption of information protection