

MICROSOFT NEWSLETTER, OCTOBER 2026

What to try, what to review, and what to **plan for.**



Microsoft Newsletter

OCTOBER EDITION

Inside this edition

	Welcome to the October edition	3
0 1	Microsoft 365 and Copilot	4
	More capable analysis in Excel	5
	Reusable skills in SharePoint	5
	More model choice within Copilot	5
	Who can bring a meeting bot into the conversation	7
0 2	Microsoft Purview and data protection	9
	DLP alerts are changing in Defender XDR	10
	Network data protection reaches general availability	10
	Labels on sites and protection on files	10
	Endpoint DLP, stored files and device coverage	12
0 3	Microsoft Entra ID and security	13
	Check where you use memberOf	14
	Device synchronisation comes to Cloud Sync	14
	Checking Conditional Access licence coverage	16
	Finding the applications that still rely on NTLM	17
	Project Perception	17
0 4	Azure	19
	Checking the resilience of an Azure environment	20
	Private connectivity between Azure and AWS	20
	Windows App endpoints for Azure Virtual Desktop	20
	Agentless migration of SMB file shares	21
0 5	Fabric, data agents and Power BI	23
	Assessing SQL databases for a Fabric migration	24
	Data agents gain more ways to answer questions	24
	Improvements for report readers and authors	24
0 6	Platform lifecycle and planning ahead	26
	October and November checks	27
	Into 2027	28
	From insight to impact	29
	About the author	31

Section start pages listed right.

Welcome to the October edition

Our regular look at the Microsoft updates most likely to affect your organisation.

There is quite a mix to cover this time. Copilot is gaining some useful capabilities for people working with spreadsheets and documents, Microsoft is expanding its data protection controls, and several identity and platform changes need attention over the next few weeks.

For anyone planning projects or budgets for the new year, there are also developments across Azure, Fabric and Power Platform to consider.

We have included a few public preview announcements where the direction is worth knowing about, with their status made clear alongside the detail.

August's edition covered Fabric and agents in depth. This month we are picking up the specific changes that give you something new to try, review or plan for. You will also find the approaching support deadlines together towards the end, including a few reminders from previous editions where time is now running short.

IN THIS EDITION

- Copilot model choice, Excel analysis and official content in SharePoint.
- Changes to DLP alerts, Entra device synchronisation and the retirement of the memberOf operator.
- Remote Help, Windows 365 and controls for external meeting bots in Teams.
- Azure resilience, Service Bus and the new AWS connectivity preview.
- Fabric, Power BI and Power Apps updates.
- The October and November deadlines, alongside changes to plan for in early 2027.



SECTION 01 — PRODUCTIVITY AND ADOPTION

Microsoft 365 and Copilot

More capable analysis in Excel

If you spend part of each month cleaning up exports, checking figures and preparing reports, the latest Excel update is worth a look. Edit with Copilot can now use Python to carry out analysis and put the results back into your workbook.

That opens up tasks such as statistical analysis, simulations and more advanced visualisations. A sensible first exercise would be a report you already understand well. Ask Copilot to analyse it, inspect the approach it takes and compare the result with your existing

work. You will quickly get a feel for where it saves time and where your own knowledge is still doing the work.

June's edition covered Copilot's editing capabilities in Excel. Python assisted analysis adds another option for working with the data itself. Anyone using the output for a management or financial decision should be able to explain the assumptions behind it.

Read more: [Release notes for Microsoft 365 Copilot, Microsoft Learn](#)

Reusable skills in SharePoint (preview)

Writing a good prompt takes some thought. If several people carry out the same document review, asking each person to build their own instructions introduces another source of inconsistency.

Copilot skills in SharePoint let you save instructions for a recurring task and reuse them. A team could create a skill to review a project document against an agreed checklist, identify missing information or produce a standard summary. The documented capability

works within the content and permissions available to the user.

We would start with one task that already has a clear process. Give someone responsibility for maintaining the skill, try it against a few representative documents and review the results with the people who normally do the work. A well defined review is a useful place to begin.

Read more: [Extend Copilot in SharePoint with skills, Microsoft Learn](#)

More model choice within Copilot

Microsoft is widening the choice of AI models available through Copilot. The options depend on which product you are using, with some releases still rolling out or limited to the Frontier programme.

THE LATEST FRONTIER AND IN-HOUSE MODELS

Microsoft AI	Anthropic	OpenAI
– MAI-Image-2.5 Flash and Pro (PowerPoint, OneDrive, Bing) – MAI-Code-1.1-Flash (GitHub Copilot)	– Opus 5 (M365 Copilot Chat, Word, Excel, PowerPoint, Cowork, Copilot Studio, Scout) – Sonnet 5 (M365 Copilot Chat, Word, Excel, PowerPoint, Cowork, Copilot Studio, Scout) – Fable 5.1 (Cowork)	– GPT-6 Astra (Cowork, Scout) – GPT-5.6 Quick and Think Deeper (M365 Copilot Chat, Word, Excel, PowerPoint, Copilot Studio) – GPT-5.6 Sol and Terra (Cowork)

Plus Mistral Medium 3.5 in Copilot Studio, and Grok 4.6 through the Frontier programme in Word, Excel and PowerPoint. The announced Grok rollout excludes the UK, EU and EFTA.

For customers, this creates more room to test which model suits a task. Compare the available options on work your team knows well, looking at accuracy, sources, speed and cost. Check the provider’s data processing terms and the controls available to your administrators before enabling it. A model’s

European origin alone does not establish where your organisation’s data will be processed.

Read more: [Claude Opus 5](#) | [Claude Sonnet 5](#) | [Claude Fable 5.1](#) | [GPT-5.6](#) | [GPT-6 Astra](#) | [Microsoft AI models](#) | [Microsoft and Mistral](#) | [Grok rollout](#)

Helping people find official content in SharePoint

An old policy saved in a project folder can look convincing when it appears in a search result. SharePoint Authoritative Sites give administrators a way to identify the organisation’s official sources within Copilot Search.

Designated sites receive an organisation label in the search experience. This could help staff recognise the approved HR policy library, finance guidance or central IT support content. Access continues to depend on the user’s permissions.

Choose sites with an owner who keeps the content current. The designation identifies an official source. The people responsible for it still need to remove obsolete documents and resolve conflicting guidance. Configuration

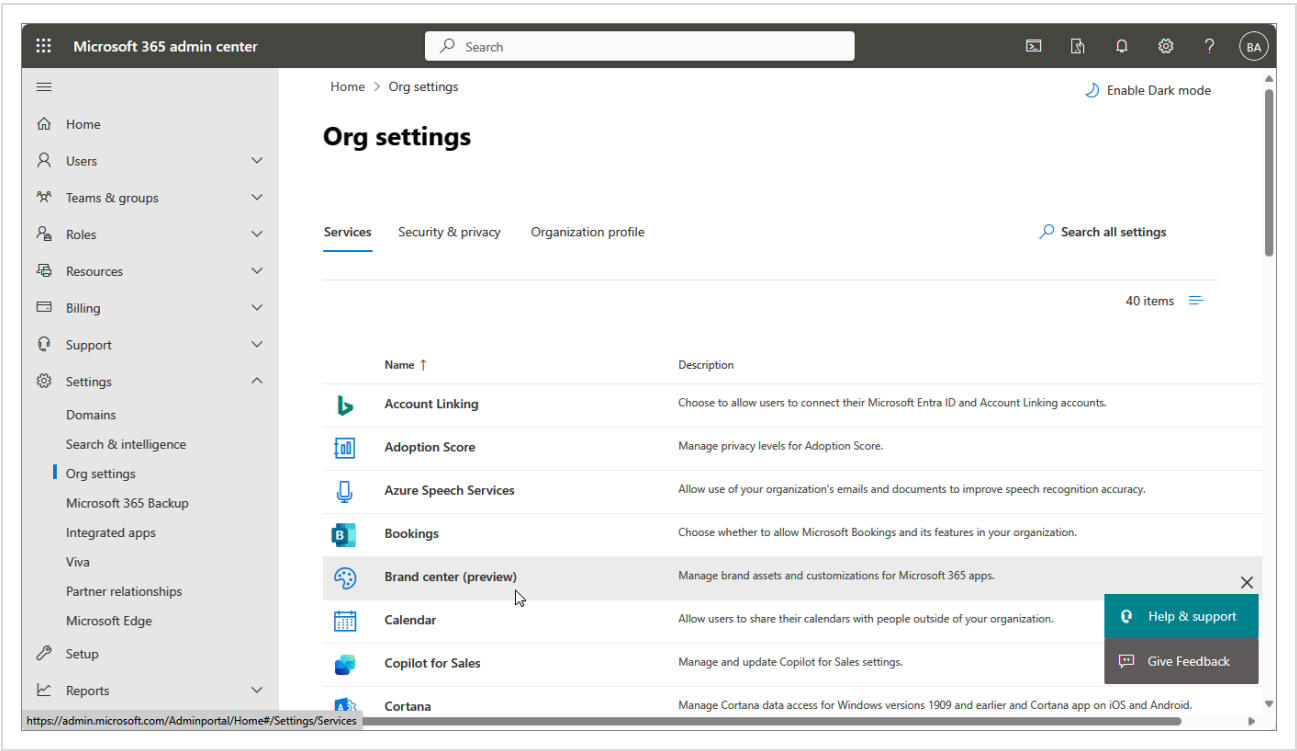
currently uses PowerShell or CSOM, and the relevant Copilot and SharePoint Advanced Management prerequisites apply.

Read more: [SharePoint Authoritative Sites, Microsoft Learn](#)

Keeping brand assets consistent

Microsoft 365 Brand Centre is worth revisiting if teams struggle to find the correct logos, fonts or templates. SharePoint’s established Brand Center provides a central place to manage organisational brand assets. Recent Copilot updates also allow brand kits to be created from a brand guideline document.

If your organisation has several versions of its logo, old templates and fonts being passed around by email, give the underlying assets some attention first. Agree which material is current and who maintains it. That gives staff, and the tools they use, a dependable starting point.



BRAND CENTER APPEARS UNDER SETTINGS, ORG SETTINGS, SERVICES IN THE MICROSOFT 365 ADMIN CENTRE

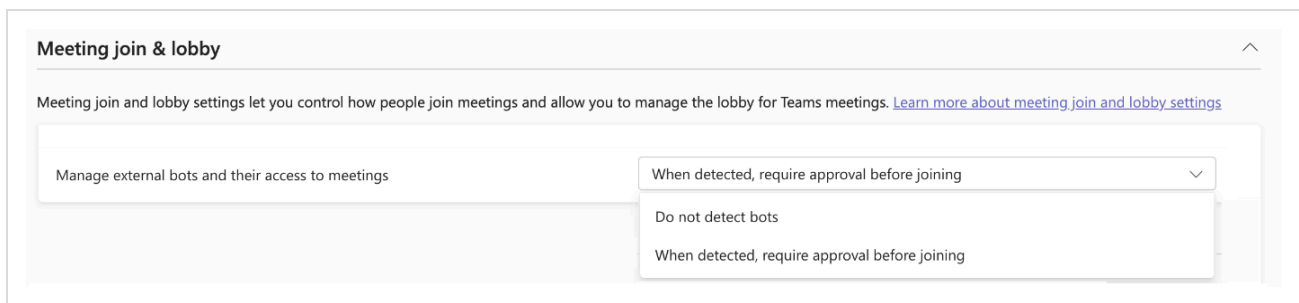
Read more: [SharePoint Brand Center, Microsoft Learn](#)

Who can bring a meeting bot into the conversation

External note taking and transcription tools can be helpful. People attending a meeting need to understand when another service is recording or processing the discussion.

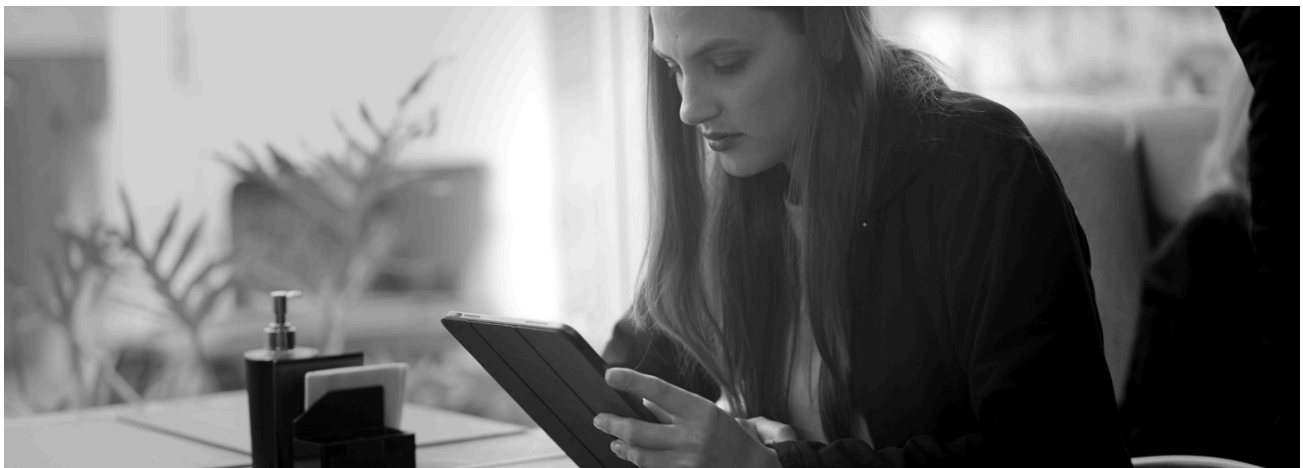
Teams provides controls to identify detected external bots and require explicit admission through the lobby. Detection has limitations, so staff awareness remains part of the process.

Review the meeting policies used for customer conversations and sensitive internal discussions. Decide which tools are approved, who can admit them and what participants need to be told. It is a straightforward policy discussion that is much easier to have before a confidential meeting is recorded.



MEETING JOIN AND LOBBY: EXTERNAL BOTS CAN BE REQUIRED TO SEEK APPROVAL BEFORE JOINING

Read more: [Manage external bots and their access to meetings, Microsoft Learn](#)



AGREE WHO CAN ADMIT A RECORDING TOOL BEFORE THE MEETING, NOT DURING IT



SECTION 02 — INFORMATION PROTECTION

Microsoft Purview and data protection

DLP alerts are changing in Defender XDR

Starting 12 October.

If your security team investigates Purview data loss prevention alerts through Defender XDR, check this change before it reaches your tenant. Microsoft plans to enable a built in rule that records these signals as behaviours, reducing the alerts appearing in the incident queue.

The investigation data remains available in the BehaviorInfo and BehaviorEntities Advanced Hunting tables, and DLP alerts remain in the Purview portal. Teams that rely on the Defender incident queue will need to review how they identify and respond to these events.

To retain standard DLP alerts in that queue, an administrator can disable **Set-As-Behavior, Data Loss Prevention (DLP) Alerts** under Settings > Microsoft Defender XDR > Alert tuning.

Agree the approach with whoever monitors your security alerts, including any external provider. Check reporting and response workflows before the rollout so that responsibility for reviewing DLP events remains clear.

Read more: [Microsoft Defender XDR: DLP alerts will be set as behaviors by default](#)

Network data protection reaches general availability

In August we covered Purview's developing ability to protect information being sent to web and AI applications. The integration with Entra Global Secure Access reached general availability in September.

This extends data loss prevention controls to supported text, file and AI interactions at the network layer. It gives organisations another way to apply policy when sensitive information is being sent to an unapproved service.

For example, you might want to warn someone before they paste customer information into an external AI tool, or block a particular type of file upload. The right response depends on the information and the business process. Start with a clear scenario, understand the activity and test the effect on users before expanding enforcement. Check the applicable Purview and Entra Internet Access licences as part of that work.

Read more: [Microsoft Purview network data security, Microsoft Learn](#)

Labels on sites and protection on files

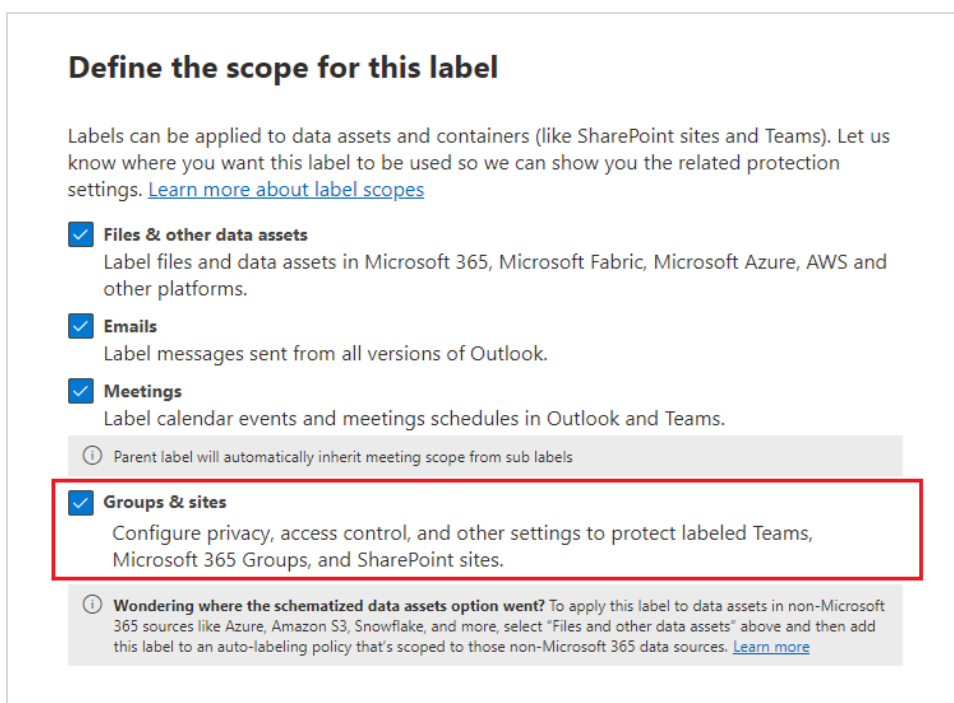
A configuration review worth booking in.

Sensitivity labels for Teams, Microsoft 365 Groups and SharePoint sites remain a useful

part of the information protection picture. They can help control the privacy and sharing settings of the collaboration space.

There is a detail here that deserves attention. Applying a label to a site does not automatically apply that label or its encryption settings to every document inside it. The site's controls and the files' protection need to be considered together.

Take a confidential project workspace as an example. Review who can join, how external sharing works and how sensitive documents are labelled. Then check what happens when someone downloads a file or shares it elsewhere. Walking through that sequence makes gaps much easier to spot.



LABEL SCOPE: GROUPS AND SITES IS CONFIGURED SEPARATELY FROM FILES AND OTHER DATA ASSETS

Read more: [Use sensitivity labels to protect collaborative workspaces, Microsoft Learn](#)

More targeted DLP controls for SharePoint (public preview)

One preview feature worth adding to a SharePoint protection review allows DLP policies to restrict access to sensitive files for specified external domains or individual external users. It applies to SharePoint and OneDrive and could help where different partners need different sharing arrangements.

Test the recipient rules carefully, including overlapping allow and block entries. The

preview has limitations: image files are excluded, and this action does not support user notifications or overrides. Include the helpdesk in the trial so staff know where to go if access is blocked.

Read more: [Help prevent sharing sensitive items via SharePoint and OneDrive with external users, Microsoft Learn](#)

Endpoint DLP, stored files and device coverage

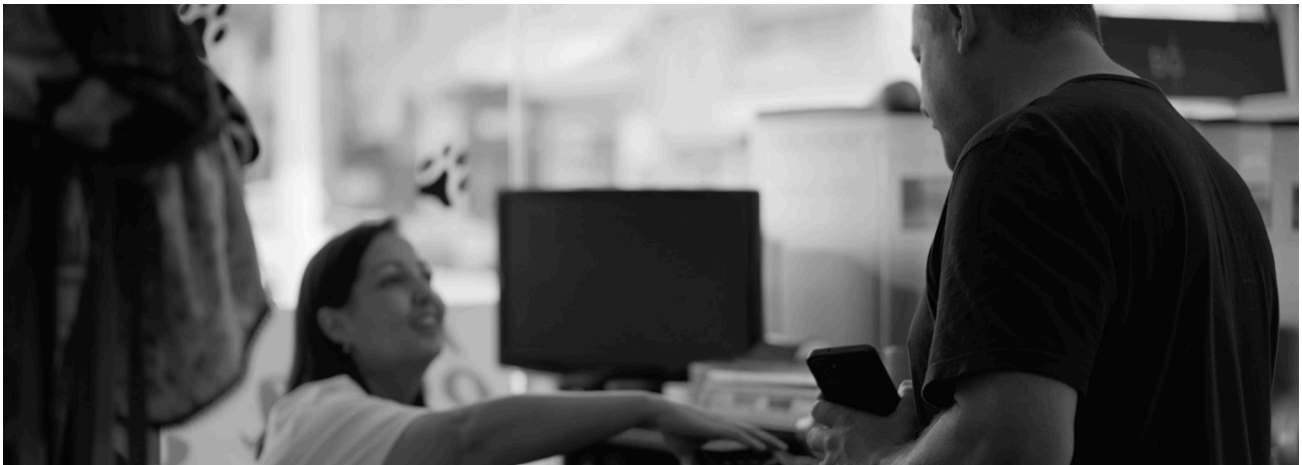
New guidance for on demand classification on Windows endpoints covers sensitive files that have been sitting untouched on a device. An administrator can scan these files without waiting for someone to open, edit or share them. Check the scanning prerequisites and consumption charges before planning a wider scan.

For organisations with Macs, the macOS 27 Endpoint DLP changes are in preview and introduce permission requirements that need preparation. Microsoft specifies client version 101.26072 or later. Include permission status

in your checks when trialling the operating system update.

Microsoft has also clarified a coverage difference. DLP controls for access by applications outside a restricted app list are supported on Windows, but not on macOS. Test the controls on each operating system your staff use, including what happens after a SharePoint file is downloaded.

Read more: [On demand endpoint classification](#) | [macOS 27 preparation](#) | [Endpoint DLP capability comparison](#)



PROTECTION HAS TO TRAVEL WITH THE FILE, NOT JUST SIT ON THE SITE



SECTION 03 — IDENTITY AND SECURITY

Microsoft Entra ID and security

Check where you use memberOf

Action required before 3 November.

Microsoft is ending the preview of the memberOf rule operator. After 3 November, affected dynamic groups, dynamic administrative units and entitlement management auto assignment policies stop updating and retain their last known state.

That can be easy to miss. An existing group may still be present, with its current members, while changes elsewhere in the organisation are no longer reflected in it. If that group

controls access or assigns licences, the consequences can extend beyond group administration.

Ask your IT team to identify every use of the operator, establish what depends on each configuration and test a supported replacement. Include any downstream Teams, SharePoint, licensing and Conditional Access dependencies in the review.

Read more: [memberOf retirement notice, Microsoft Learn](#)

Entra Connect and Cloud Sync

Microsoft's minimum version requirement for Entra Connect Sync took effect on 30 September. Versions below 2.5.79.0 are affected by a synchronisation stop. If you synchronise an on premises directory into Microsoft 365, confirm the installed version and check that synchronisation is healthy. Upgrade to a currently supported release where needed.

We introduced Cloud Sync migration in June's newsletter. Microsoft's guidance continues to favour a phased approach, with custom rules, writeback and other dependencies checked before moving objects. Each object must be managed by one synchronisation tool at a time.

Read more: [Entra Connect version requirements](#) | [Cloud Sync migration guidance](#)

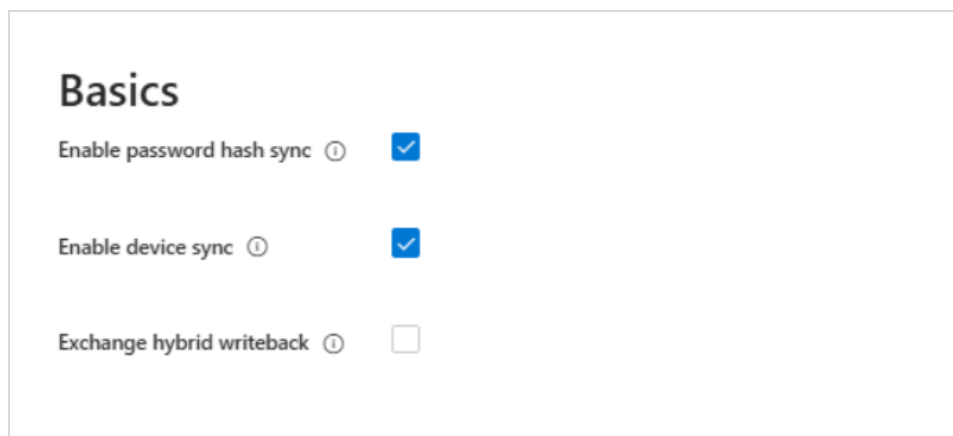
Device synchronisation comes to Cloud Sync (preview)

Device synchronisation has been a barrier for some organisations considering a move from Entra Connect Sync. Microsoft now offers a Cloud Sync preview that synchronises Active Directory computer objects into Entra ID, allowing those devices to become hybrid joined once the required configuration is in place.

The feature is disabled by default. It requires provisioning agent version 1.1.1107 or later and an AD to Entra Cloud Sync configuration.

Administrators also need to check the device registration configuration and permissions for each relevant forest.

This is a reason to revisit an earlier Cloud Sync assessment if devices were the sticking point. Pilot a small group of computers and confirm hybrid join and access behaviour before extending the scope. Other migration dependencies still need to be assessed.



ENABLE DEVICE SYNC SITS ALONGSIDE PASSWORD HASH SYNC IN THE CLOUD SYNC BASICS CONFIGURATION

Read more: [Configure device sync with Microsoft Entra Cloud Sync \(preview\), Microsoft Learn](#)

Device code flow blocked for new tenants using security defaults

Since 1 July this year, newly created Entra tenants using security defaults block device code flow. This sign in method helps devices with limited input capabilities authenticate, but attackers have also used it to persuade people to authorise access through phishing.

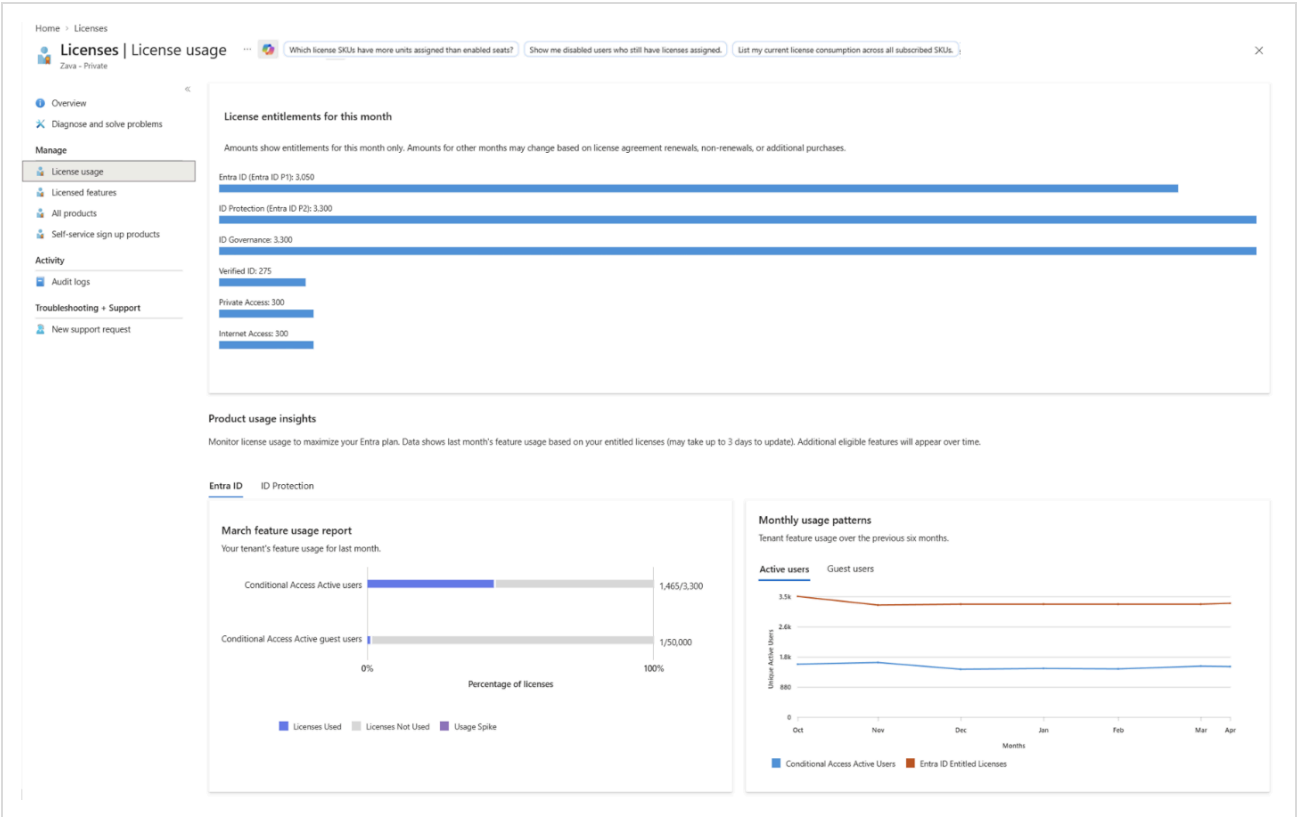
The change gives new tenants this protection through security defaults. Existing tenants should review their own configuration. Organisations using Conditional Access need to check their device code flow policies, including any business requirement for an exception.

Read more: [Configure security defaults for Microsoft Entra ID, Microsoft Learn](#)

Checking Conditional Access licence coverage

Licence coverage can become difficult to track as policies reach more users. Entra licence usage insights now give administrators a view of feature use alongside purchased entitlements, including Conditional Access usage for P1 and risk based Conditional Access usage for P2.

Use the figures to identify possible gaps, then check the users and features involved against your agreement. This is particularly relevant where licences have changed or a policy originally created for one department now covers the wider organisation.



LICENCE USAGE INSIGHTS SHOW ENTITLEMENTS ALONGSIDE CONDITIONAL ACCESS ACTIVE USERS

Read more: [Microsoft Entra licence usage insights](#) | [Microsoft Entra licensing](#)

Assigning external users to access packages

An entitlement management improvement allows an external user to be assigned directly to an access package using their email address before they exist in your directory. For a supplier or contractor joining a project, this can simplify the access process. Set the

appropriate assignment policy, expiry and review arrangements, and check the governance licensing required.

Read more: [Govern access for external users in entitlement management, Microsoft Learn](#)

Finding the applications that still rely on NTLM

NTLM retirement planning starts with finding where the older authentication protocol is still being used. In an established environment, that can involve applications and services whose original owners have moved on.

Use Microsoft's auditing guidance to build a picture of those dependencies. Identify an owner for each one and agree a supported path forward with the application vendor where necessary. Test changes with a representative

group of users and keep a recovery plan for systems that prove more complicated than expected.

This is useful work to start ahead of enforcement changes. An inventory with named owners and a migration plan will make the next stage much easier to manage.

Read more: [Advancing Windows security: disabling NTLM by default](#)

Secure Boot certificates need a deployment check

Microsoft's Secure Boot certificate transition runs through 2026. For IT teams, the useful check is whether the required updates have reached the devices in the estate, including machines that spend long periods offline.

Use Microsoft's playbook to review readiness, firmware dependencies and deployment status. Test representative hardware before broad

changes, and include recovery arrangements in the plan. Certificate expiry needs careful handling because it affects the continuing security of the boot process. Avoid treating it as a routine patch that can be assumed complete from a deployment assignment alone.

Read more: [Secure Boot playbook for certificates expiring in 2026](#)

Project Perception (public preview)

Microsoft's Project Perception brings multiple AI

agents into security operations, using shared

An evaluation should show whether the team can follow how an agent reached its conclusion, which actions require approval and how it handles incomplete information. Test a scenario where the proposed response could interrupt a business service. Those answers will

matter as much as the speed of the investigation.

We will be following how the preview develops, particularly around operational control and how it fits into existing security services.



PROJECT PERCEPTION: RED, BLUE AND GREEN AGENT TEAMS WORKING FROM SHARED CONTEXT

Read more: [Rethinking security for the age of AI, Microsoft](#)



SECTION 04 — CLOUD PLATFORM

Azure

Checking the resilience of an existing Azure environment

An availability zone review is a sensible exercise when an Azure environment has grown beyond its original design. Zones are separate locations within a region, and the resilience you achieve depends on how each service is deployed and configured.

Choose a business critical application and trace its dependencies. Look at the application servers, identity services, network path and data layer. Check what would happen if a zone became unavailable, how the application would recover and who would be responsible for the recovery work.

Also review backup and regional recovery requirements. They address their own failure scenarios and need to be tested. A recovery plan becomes much more credible once someone has walked through it and recorded the outcome.

Want a second pair of eyes on a resilience review? Speak to your Cybit account manager and we will scope it with you.

Private connectivity between Azure and AWS (public preview)

Azure Multicloud Interconnect for AWS is worth following if your systems or data are spread across both platforms. It provides a new option for private connectivity between them.

The preview has important planning constraints. Microsoft's published region list does not currently include a UK region, and the

preview has a 1 Gbps limit and no SLA. Those details need to be considered alongside data location, traffic volumes and costs on both sides. For now, customers with a suitable non production use case can use the preview to assess how it might fit a future design.

Read more: [What is Azure Multicloud Interconnect?](#) | [Availability and limits](#)

Windows App client side endpoints for Azure Virtual Desktop

Beginning in early October 2026, Windows App will start using three new wildcard fully qualified domain names for client side service traffic to Azure Virtual Desktop. These domains are already included in the cloud side connectivity requirements.

If your organisation applies network controls to devices running Windows App, you must allow these endpoints before activation. If the

endpoints are not reachable, users may experience sign in and connection failures.

This is a client side change for Windows App and is separate from the previous cloud side domain update. Organisations that have already completed the cloud side update should still review proxy, firewall, VPN, DNS filtering and Secure Web Gateway policies that

If these endpoints are unavailable, blocked, or inspected in a way that interrupts the connection, users may experience failures during sign in, resource discovery, connection or an active session.

Read more: [Required FQDNs and endpoints for Azure Virtual Desktop](#) | [Unified cloud.microsoft domain for Microsoft 365 apps](#)

Azure Copilot Troubleshooting Agent

The Azure Copilot Troubleshooting Agent is now generally available. It is a built in Azure Copilot capability that helps customers investigate and resolve operational issues faster.

Available through both Azure Copilot and Support and Troubleshooting in the Azure

portal, it brings troubleshooting insights, operational context and recommended actions into a single experience, which shortens the route from detection to resolution.

Read more: [Azure Copilot announces general availability of the Troubleshooting Agent](#)

Agentless migration of SMB file shares to Azure Files (public preview)

Azure Storage Mover now supports agentless migration of on premises SMB file shares to Azure Files (SMB) in public preview. You can move file data from Windows Server or NAS shares into Azure without deploying, registering or maintaining a migration agent on premises.

With agentless migration, the Storage Mover service connects directly to your SMB share over an existing private connection, either VPN or ExpressRoute, and copies data to the destination Azure file share. Source credentials are stored securely in Azure Key Vault, and

Storage Mover's managed identities handle access to both the source secrets and the target share. Configure source and target endpoints, create a job, and start the copy from the Azure portal or Azure CLI.

Agentless SMB migration joins Storage Mover's existing agent based paths for SMB and NFS sources, giving businesses more flexibility to modernise file storage.

Read more: [Migrate on premises SMB file shares to Azure Files using agentless migration, Microsoft Learn](#)



RESILIENCE IS A DESIGN DECISION, NOT A DEFAULT



SECTION 05 — DATA AND ANALYTICS

Fabric, data agents and Power BI

Assessing SQL databases for a Fabric migration

Fabric Migration Assistant for SQL databases reached general availability in August. It helps assess and prepare database schemas for migration, with data movement supported through Copy Jobs.

If you have an older SQL application under review, this provides a useful way to explore suitability. Start by establishing which database features and integrations the application relies on. Involve its supplier, check the migration

findings and test a representative workload before deciding on the target platform.

The tool can support the assessment. The application still needs a clear support position, a workable cutover plan and a tested recovery route.

Read more: [Migrate SQL Server to SQL database in Microsoft Fabric using Fabric Migration Assistant](#)

Data agents gain more ways to answer questions

Following August's Microsoft 365 Copilot coverage, Fabric Data Agents can now be integrated into Copilot Studio through Fabric IQ Data MCP. This gives organisations another way to bring analytical answers into their own agents.

Advanced DAX generation is also in preview. It allows a data agent to work through a more detailed approach to querying a semantic model before answering.

Pick a small set of business questions with known answers when testing either capability. Include questions that should return different results for different users, so you can assess access controls as well as accuracy.

Read more: [Advanced DAX generation for semantic models in Fabric data agents \(preview\)](#)

Activator and business events (preview)

Fabric Activator can publish a structured business event into Real-Time hub when a condition in the data is met. That event can then be used by other processes.

For example, a fall in stock below an agreed threshold could prompt a replenishment

workflow. Agree who receives the event, what action should follow and how repeated alerts will be handled. The business process needs an owner throughout the trial.

Read more: [What is Fabric Activator? | Business events overview in Fabric Real-Time hub](#)

Improvements for report readers and authors

The latest Power BI updates include modern visual defaults and theme customisation, a generally available date picker slicer and comments within organisational apps. Report owners also gain more selective controls over semantic model refreshes, including schema, data and individual tables.

There is a governance detail to review too. Copilot summaries can use visuals hidden behind display bookmarks. Row level and object level security continue to apply. Hiding a visual should therefore never be your access control mechanism.

Take a familiar report through the updated experience with one of its regular readers.

Check whether the date selection is easier to use, whether the theme remains consistent and whether the summary answers the questions people normally ask.

OCTOBER CHECK

Power BI Desktop releases from March 2026 and earlier lose the ability to save and share reports through OneDrive and SharePoint. Confirm that your report authors are running a current supported version before the end of the month.

Read more: [See what's new in Power BI, Microsoft Learn](#)



REPORTING PEOPLE CAN ACT ON WITHOUT CHECKING IT TWICE



SECTION 06 — DATES AND DECISIONS

Platform lifecycle and planning ahead

October and November checks

Several of these dates appeared in August. They are back here because the remaining window for action is now short. Confirm the position against your own inventory and give each outstanding item an owner.

DATE	CHANGE	WHAT TO CONFIRM
1 October	Legacy Entra risk policies retire	User risk and sign in risk controls have moved into Conditional Access and been tested
12 October	Defender XDR records DLP alerts as behaviours	The monitoring approach is agreed with your security team or provider
13 October	Windows 11 24H2 Home and Pro, and Windows 10 Enterprise 2016 LTSC, reach the end of standard updates	Affected devices have an upgrade or replacement plan
October	Office LTSC 2021 reaches end of support	The replacement plan, including application, add in and document compatibility testing
October	Final ESU year for Windows Server 2012 and 2012 R2 ends	Remaining systems have an agreed migration or retirement plan
End of October	Final Exchange Server 2016 and 2019 ESU period ends	Progress towards Exchange Online or a supported Exchange Server release, including application and device dependencies
3 November	The memberOf rule operator is retired	The replacement work described in the identity section is complete
November	Windows 11 23H2 Enterprise and Education reach end of updates	Centrally managed devices and those used by remote staff
November	Support ends for .NET 8 and .NET 9	Application owners have a supported upgrade path agreed with developers or vendors

Installing a newer .NET runtime on its own does not establish that an application has been migrated successfully. Ask the application owner for evidence of testing, not just the installed version.

Into 2027

12 January 2027: Windows Server 2016 reaches end of extended support. If a migration project is still waiting for approval, factor in testing and the year end change calendar when agreeing its delivery date.

Approval in November or December, with delivery in the new year, is a realistic route. Approval in January is not.

CYBIT'S VIEW

Most of the dates above have been in the diary for a while. What separates the organisations that handle them well is not awareness, it is ownership. Every item on this list needs a named person, a decision and a date, even if that decision is to accept the risk for another quarter.

If you would like a second opinion on where your own estate sits against this calendar, we can run through it with you and mark the items that carry real operational risk.



EVERY DATE ON THE LIST NEEDS A NAME AGAINST IT



WHERE CYBIT CAN SUPPORT

From insight to impact

If any of these updates affect your plans, speak to your Cybit account manager. We can help you work through the licensing and technical detail, identify the systems or users affected and agree what needs to happen next.

That might be a focused review of identity and access, a Copilot readiness or Microsoft 365 licensing assessment, a Windows or server migration plan, or a closer look at how Fabric and Power BI could support your reporting. For previews, we can help define a sensible evaluation and the questions it needs to answer.

If you are unsure where to begin, bring us the business process or system that is causing the most difficulty. We can start there.

Where we can help this month

- Identity and access review, including memberOf and Conditional Access.
- Purview and data protection configuration review.
- Copilot readiness and Microsoft 365 licensing assessment.
- Windows, Exchange and server migration planning.
- Azure resilience and cost review.
- Fabric, Power BI and reporting modernisation.

Cybit Flexcare 2.0 keeps this work going after the project closes, with the monitoring, governance and change support that keeps a platform current rather than correct on the day it went live.

OUR PROMISE

Build together. Deliver together.
Succeed together.

CYBIT

ABOUT THE AUTHOR



Peter McLeavery

SOLUTIONS ARCHITECT

Translating complex technology into practical outcomes

Peter McLeavery is a Solutions Architect at Cybit and one of our leading Microsoft specialists, with deep expertise across Microsoft 365, Azure, Copilot and the broader modern workplace ecosystem.

With over a decade of hands on experience helping organisations modernise their environments, Peter is known for translating complex technology into clear, practical solutions that deliver measurable value. He works closely with IT and business leaders to optimise their Microsoft licensing, simplify their architecture, and unlock capabilities they already own but have not yet fully used. Recently he has been focused on helping customers prepare for the shift toward AI enabled operations, including Copilot readiness, data governance, automation and secure by design configuration.

Peter regularly leads Cybit's customer education sessions, webinars and advisor workshops, where his blend of technical depth and real world pragmatism makes him a trusted voice. Whether he is guiding organisations through Microsoft 365 E7 planning, building proof of concepts in Copilot Studio, or improving day to day workplace efficiency, Peter is passionate about helping customers turn Microsoft technology into meaningful, scalable outcomes.

Contact Peter on peter.mcleavery@cybit.com

GET IN TOUCH

Equinox House, Silver Fox Way
Cobalt Business Park
Newcastle Upon Tyne, NE27 0QJ

03308 284838

hello@cybit.com
cybit.com

PREDICT. PROTECT. PERFORM.

CYBIT