CYBIT

Microsoft Solutions Partner

MICROSOFT NEWSLETTER, OCTOBER 2026

Protecting the data. Proving the identity.

Microsoft Newsletter

PART TWO OF THREE

CONTENTS

Inside this edition

	Data protection and identity	**3**
01	**Microsoft Purview and data protection**	**4**
	DLP alerts are changing in Defender XDR	5
	Network data protection reaches general availability	5
	Labels on sites and protection on files	5
	More targeted DLP controls for SharePoint	6
	Endpoint DLP, stored files and device coverage	7
02	**Microsoft Entra ID and security**	**8**
	Check where you use memberOf	9
	Entra Connect and Cloud Sync	9
	Device synchronisation comes to Cloud Sync	9
	Checking Conditional Access licence coverage	11
	Finding the applications that still rely on NTLM	12
	Project Perception	12
	Where Cybit can support	**13**
	About the author	**15**

Section start pages listed right.

OCTOBER 2026

Data protection and identity

Part two of three. The changes that need a decision, not just a read.

Two of the items in this part carry dates. From 12 October, Purview data loss prevention alerts are recorded as behaviours in Defender XDR rather than appearing in the incident queue.

Before 3 November, any use of the memberOf rule operator needs a supported replacement.

The rest is configuration worth reviewing while you are in there, including a detail about sensitivity labels that catches a lot of organisations out.

IN THIS PART

- DLP alerts in Defender XDR change on 12 October.
- Network data protection reaches general availability.
- What a site label does not do to the files inside it.
- memberOf retires on 3 November.
- Device sync arrives in Entra Cloud Sync.
- NTLM, Secure Boot and Project Perception.

SECTION 01 — 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**

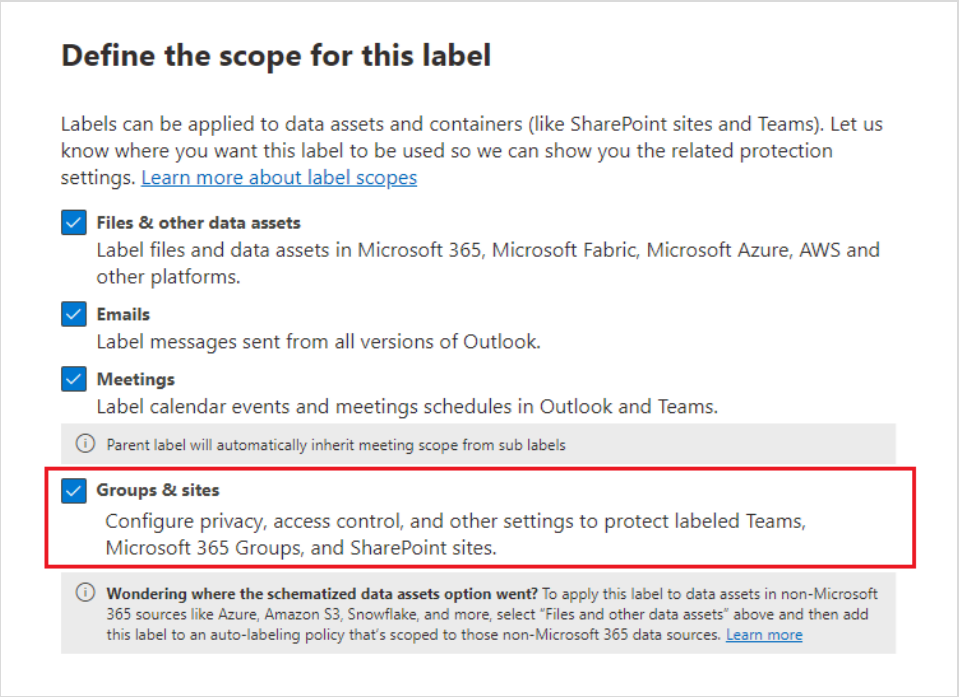
Labels on sites and protection on files

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**

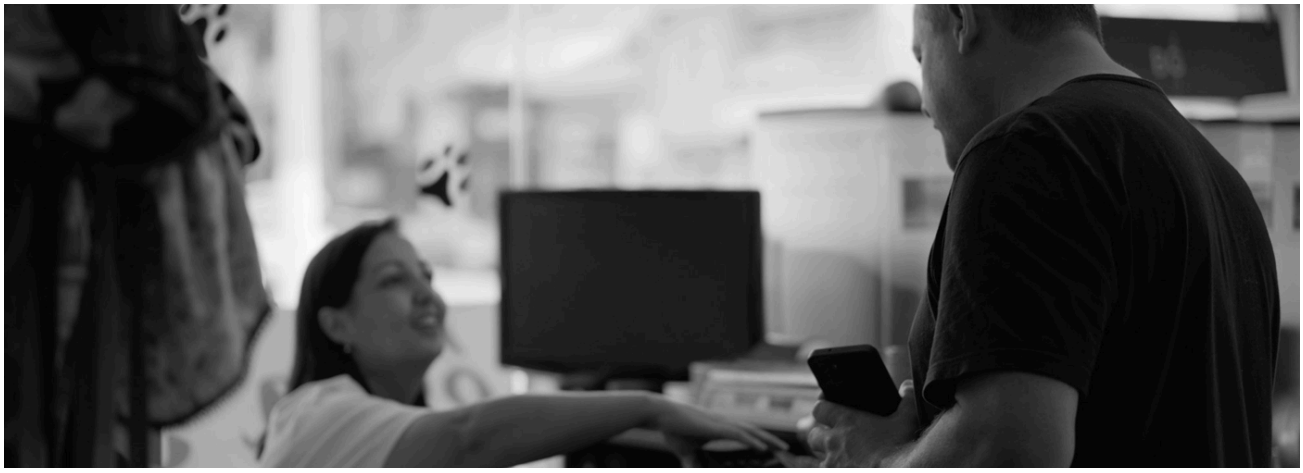
Endpoint DLP, stored files and device coverage

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 02 — 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**

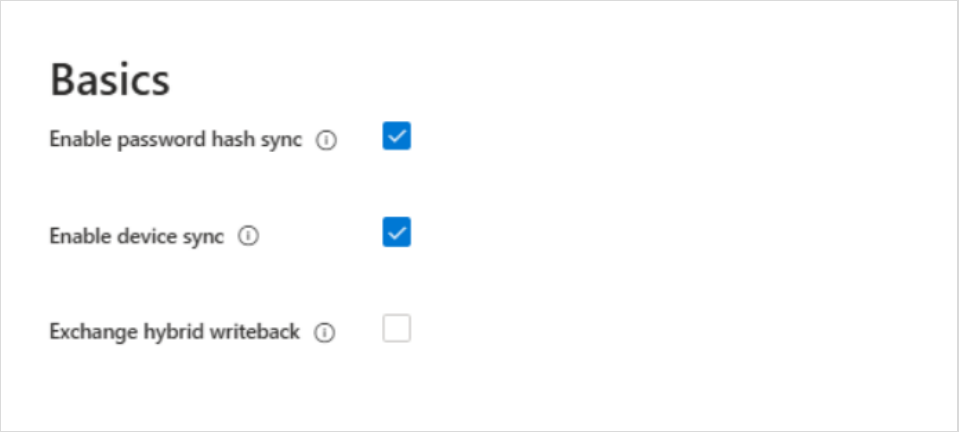
Device synchronisation comes to Cloud Sync (preview)

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.

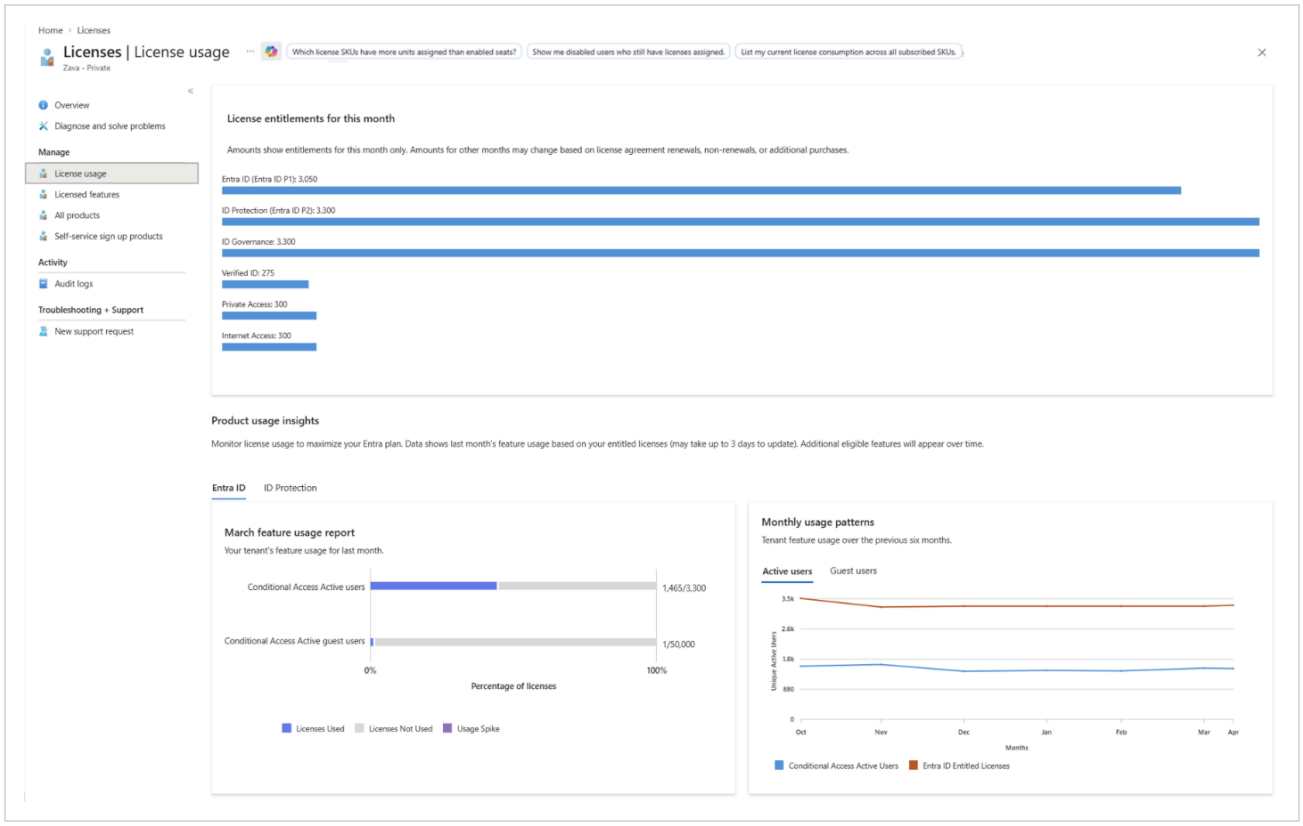
The change gives new tenants this protection through security defaults. Existing tenants should review their own configuration. Organisations using Conditional Access need to check their device code flow policies, including any business requirement for an exception.

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**

Where Cybit can support

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.

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

This is one part of our October Microsoft newsletter. The other parts follow over the coming weeks, and the full edition is available on request.

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

03300 577350
hello@cybit.com
cybit.com

PREDICT. PROTECT. PERFORM.

CYBIT