

CONNECT NEWSLETTER - OCTOBER 2026

Good Morning,

Each month, we take a look at a key issue or trend, as well as any technology updates, and what this means for your organisation.

Microsoft and Google Tenant Security: Small Misconfigurations, Big Risks

Microsoft and Google's cloud platforms offer flexibility, scalability and resilience, but a simple misconfiguration can leave sensitive data exposed to cybercriminals. In fact, many cloud security incidents stem not from sophisticated attacks, but from avoidable mistakes such as overly permissive access rights, unsecured storage, or a lack of multi-factor authentication (MFA).

Fortunately, our 24/7 Managed IT Support customers can be secure in the knowledge that CloudTech24 look after Microsoft 365 and Google Workspace tenant alignment and baselining, helping strengthen your tenant security.

Not a 24/7 IT Support customer? Take a look at the quick wins and mistakes to avoid in the section below or [contact us](#) for advice.

Is your cloud environment secure?

Now is the time to find out.

Schedule a call today and take the first step towards a more secure posture.

[Contact our expert team for details](#)

Quick wins for better cloud security

- Enable** Multi-Factor Authentication (MFA) for all users
- Review** user permissions regularly and remove unnecessary access
- Disable** dormant accounts and unused applications
- Monitor** for unusual login activity and configuration changes
- Ensure** critical cloud data is backed up and recoverable.



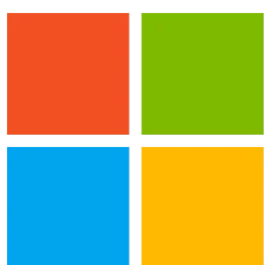
Common mistakes to avoid

- Assuming** your cloud provider is responsible for all aspects of security
- Granting** users excessive privileges 'just in case'
- Failing** to review access rights when employees change roles or leave
- Taking** a "set and forget" approach to cloud security.



Want to know more?

Read our blog post on Cloud Misconfiguration: The Hidden Security Risk Lurking in Microsoft 365

[CLICK HERE to read the article](#)

Microsoft retires EWS: What is the impact for your business?

Microsoft is retiring Exchange Web Services (EWS), an older technology that lets applications connect to Microsoft 365 email, calendars and contacts.

Phased disablement began on 1st October 2026, with permanent retirement on 1st April 2027. Affected integrations must move to Microsoft Graph before then.

How could this affect you?

Applications that connect to your Microsoft 365 mailboxes behind the scenes are most at risk, such as:

- CRM platforms that sync emails, contacts and appointments
- Helpdesk systems that turn emails into tickets
- Booking tools and calendar integrations
- Email backup, archiving and migration software
- Custom scripts and automated mailbox workflows.

Microsoft 365 email isn't being switched off, but any of these that still rely on EWS could stop working. On-premises Exchange Server is not affected.

What should you do?

Identify which applications use EWS, confirm your suppliers' migration plans and test any updates. Temporary access is only a short-term fix.

If you use business software that connects to Microsoft 365 email or calendars, [contact CloudTech24](#) to find out whether it could be affected and what action is needed.

Last Month's Monitoring Stats

797

Real world security events handled by our team

2,306

Phishing emails caught and remediated

2.4m

Vulnerabilities remediated by CT24 specialists

31 mins

Average time to fix

Good

Customer satisfaction

1761

Tickets closed for clients

