First Technology Group

FirstNet Technology Services | FirstDigital | the crm team | GALDONDATA A FIRSTNET GROUP COMPANY

BUI INNOVATION DELIVERY RESULTS | TechSonic | First Horizon

.top_stories

//barry_neethling

25th May #168

New for This week!

- As a user of Microsoft technologies, you are receiving this publication to stay informed about critical topics such as Microsoft licensing, price increases, end-of-life dates, technical updates, security notices, and more.
  If you do not want to continue receiving TOP STORIES, click on the unsubscribe link at the bottom of the mail.

- **Another 3 New vendors Watchguard, Claroty & Black Kite** are added.
- **Microsoft EoL section Updated for April 2027 -** all about modernisation!
- **DarkWeb Weekly Intelligence Report #168-** Mythos is lurking in the Shadows
- **Did You Know Microsoft does not do Licensing?** So what DO they do?
- **Understanding E7 and the "Step-up"** - It's not what you do, it's how much you do it!
- **The Multiple Equivalent Offer Trap** - Many columns to confuse - read it again!
- **W365 Frontline gets a new name** - With more complicated licensing.
- **AI Powered CRM Housekeeping** - For a Price - find out more.
- **Modern Work Plan Comparison with E7** - Lots to read - beware of mistakes
- **Microsoft releases mitigation for YellowKey** - closing the barn door
- **The New Phish** - The new MFA bypass without hacking anything. Human beware!
- **Claude Mythos** - Many skeletons in the cupboard.

Microsoft Modernisation April 2026-2027

Microsoft Modernisation strategy has been updated. This addresses key EoL dates, price increases and updates up to 1 April 2027

DarkWeb Weekly Intelligence Report #168

We scan the DarkWeb continuously for Hacker signals and Ransomware attacks.
Click above for the report from our live dashboard that we will publish weekly (but actually updated continuously).
This is part of the DarkWeb monitoring services included with many of BUI's managed services offerings. **This report is live, and this is a "snapshot" of the top 10 events as of Sunday Afternoon.**

TOP STORIES #167

Click button above for last weeks news.

Visit FirstMarketPLace Link here for New Additions

Watchguard, Claroty & Black Kite have been added for this week.
See below for Linkedin [Try out our AI](#) to see whats been added since launch.

Our LinkedIn

Movie releases

Get all the releases for the next 4 weeks in South Africa. The long awaited **Mortal Kombat 2** is now screening in May along with **Masters of the Universe and Mandalorian & Grogu now screening**

TOP STORIES ARCHIVE

Register with the link above and get access to the entire TOP STORIES Archive with an AI to help you find what you want. You can also find all the vendors added to FirstMarketPlace and get a whole lot of detail about them!
It's in Beta so it could make mistakes.

Did You Know?

Microsoft licensing is not just licensing anymore

The old Microsoft renewal process was fairly simple. Count the licences, renew the Enterprise Agreement, argue about the discount, get some investment funding, and move on.

That world is disappearing.

Microsoft is now selling a much bigger mix of services, Azure consumption, Copilot, AI, security, support, and business automation.
The danger is that customers may focus only on the licence price, while the real money quietly moves into consumption, add-ons and support commitments.

This is where things can get expensive.

Before renewing, customers need to understand who actually needs what, which users genuinely justify premium licences, how Azure consumption is being controlled, and what

contract protections should be negotiated before signing.

Just putting everyone on the biggest bundle is not a strategy. It is usually a very expensive shortcut.

First Technology Group can help customers take a more interconnected view across licensing, Azure, support, security and long-term Microsoft strategy.
The goal is not only to reduce cost, but to make sure the money being spent actually delivers value by bringing a TEAM of experts to the negotiating table to help make sense of it all.

Please contact your First Technology Group account manager before your next Microsoft renewal turns into a very polished invoice with a nasty aftertaste.

Request Account Manager

SUBSCRIBE TO TOP STORIES

Microsoft News This Week

Understanding E7 and the "Step-up"

This time around, this upgrade, the 1st time in a decade, is NOT just a simple upgrade, it is **THE** AI platform play for Microsoft, and this article written by Lane Shelton from Directions on Microsoft is warning that this has to be treated with the same level of seriousness that you would if you were entering into a full EA contractual negotiation.
I REALLY recommend that you read it!

The Step-up Trap

It appears harmless (other than the money), sign the step-up amendment, and life carries on - simple..... well, it's NOT simple, and that is the problem!
A Step-Up can quietly set your future pricing, renewal baseline, commercial structure, and negotiating position before you have properly modelled the **real** cost.
That includes Azure consumption exposure, Unified Support impact, AI usage patterns, and all the other little Microsoft “extras” that tend to appear after the excitement has worn off and finance starts asking difficult questions.

Microsoft knows that AI FOMO is real.
They also know their financial year ends on 30 June, so don’t be surprised if the pressure arrives from above, wrapped in a beautiful AI vision story and a deadline.

This is not about saying no to E7. It may be the right direction for many customers.

It is about not saying "yes" like a rabbit staring into the headlights!

Before signing anything, customers should understand their *actual* E5 usage, Copilot adoption, Azure trajectory, support commitments, server footprint, and renewal timing.
The E7 decision should be used as leverage across the whole Microsoft relationship, not wasted on a rushed Step-Up that Microsoft has framed on its own terms.

Please contact your First Technology account manager to connect you with our experts in ALL our specialist divisions to help you assess your current Microsoft consumption and to negotiate the best possible value proposition from Microsoft. The recommended path is to include this process as part of evaluating your Support options, either from Microsoft or First Technology Group's Universal Support, or even from both!

Directions: Understanding M365 E7: Beware the Step-Up Offer

Avoiding the Multiple Equivalent Offer Trap

Steven Kelly from Directions on Microsoft has a very useful warning on Microsoft's Multiple Equivalent Offer, MEO, strategy.
The offer may look attractive because the Year One pricing across several renewal options is made to look roughly equivalent, especially when Microsoft adds discounts and "savings" from replacing third-party tools.
The trap is that those discounts fade, the Microsoft dependencies harden, and by the next renewal the customer may have less leverage, fewer alternatives, and a much higher Microsoft spend, which can also push up Unified Support.
This is one to read before your next EA renewal, especially if the proposal looks almost too neatly balanced. It probably is.

Please contact your First Technology Group account manager to connect you with our specialists, to help understand the impact of this and where Universal Support from First Technology Group which is a FIXED cost that is not linked to your licensing bill or it's duration.
As I emphasised in TOP STORIES #166 last week, you have to look at your Licensing, Azure, and Support bills holistically with a TEAM of experts supporting you.
If you do not do this, you are guessing, not negotiating.

Directions - Microsoft's Multiple Equivalent Offer (MEO): How to Avoid the Trap

---

Windows 365 Frontline gets a new name

Microsoft has renamed Windows 365 Frontline to Windows 365 Flex, which is a much better name for what it actually does.

"Frontline" always sounded a bit too narrow. "Flex" makes more sense, because this is really about giving people a Cloud PC when they need one, not necessarily giving everybody a full-time Cloud PC that sits there burning money while nobody is using it.

Dedicated Mode allows one licence to provision up to three Cloud PCs, each assigned to a specific user, but only one active session at a time. This works well for shift workers, part-time staff, rotation teams, contingent workers and people who need a proper Cloud PC, but not 24 hours a day.

Shared Mode is different. One Cloud PC can be shared non-concurrently by a group of users, again with one active session at a time. That is useful for retail assistants, contractors, task workers, training scenarios and other users who need quick access to a managed Cloud PC without persistent personal data.

The important bit, the licensing and core capability have not really changed. The name has. But don't dismiss this as just Microsoft repainting the signboard again. Windows 365 and Azure Virtual Desktop are moving quickly, and this is another signal that Microsoft wants Cloud PCs to become a lot more practical for flexible, distributed and cost-sensitive workforces.

See the Microsoft announcement below, and check the Windows 365 Flex documentation carefully before assuming how many Cloud PCs you can provision and how many users can be active at the same time.
This is exactly where a small misunderstanding can become an expensive licensing conversation.

Please contact your First Technology account manager to connect you with our W365 experts to help address the licensing issues and where this technology is practical to deploy for your environment as there are many technical, licensing (and latency) hoops to jump through to make sure you are getting the correct solution, or conclude that it is not!

Windows 365 Gets a New Name

Microsoft Sales gets AI-powered CRM housekeeping

Microsoft has added AI-powered Data Enrichment to Dynamics 365 Sales Premium.

The agent reads recent seller emails linked to opportunities and suggests updates to fields such as close date, budget, stakeholders and other opportunity details.

That sounds useful, because CRM data is usually only accurate for about five minutes after someone is shouted at to update it!

But remember, this is AI processing work in the background, so check the licensing and consumption model before switching it on.

Please contact your First Technology Group account manager to connect you with our Dynamics 365 and licensing specialists before your AI-powered CRM cleanup quietly becomes an AI consumption bill.

AI-powered Data Enrichment for opportunities

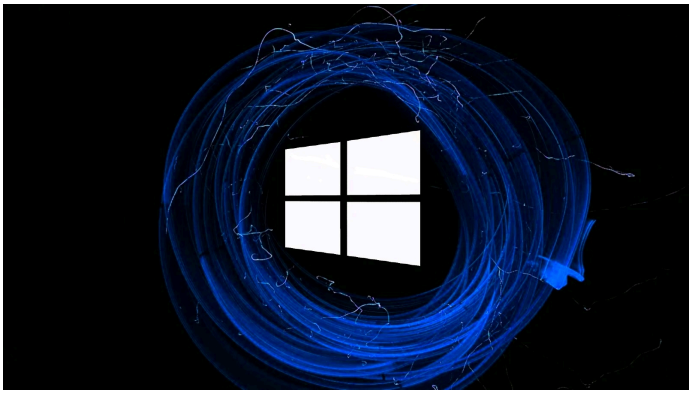
Modern Work Plan Comparison documents now include E7

Microsoft has updated the Modern Work Plan Comparison documents for SMB, Enterprise, US Government, and Education customers.
Most of the changes are exactly where you would expect them, Microsoft 365 E7 and Agent 365. The Enterprise documents now include new sections for Agent Observability, Agent Governance, and Agent Security. That makes it easier to see what is already included in a Microsoft cloud subscription, and what needs Agent 365 or Microsoft 365 E7.
Reading these changes carefully matters because Microsoft 365 E7 is now the big new bundle, combining Microsoft 365 E5, Microsoft 365 Copilot, Agent 365 and Entra Suite.
Agent 365 is not there to build agents, it is there to observe, govern and secure them. That distinction matters. Otherwise you may buy the “agent” licence and then discover it does not do what the name made you think it did.
Funny how that happens!

Also remember, Microsoft documentation is useful, but it is not always perfect. Comparison tables, FAQs, licensing guides and Product Terms are NOT in sync or even 100% accurate. Before you renew, step up, or assume something is included, speak to your First Technology Group licensing specialist.
A small mistake in a Microsoft table can become a very large mistake in your budget.

Microsoft Modern Work Comparison Guide May 2026 incl. E7

Security



Microsoft Releases Mitigation for Yellowkey No Time Machine available

In **TOP STORIES #167** I covered YellowKey with a blunt warning.
If a Windows 11 notebook was protected only by standard TPM-based BitLocker and it disappeared, you could no longer simply assume the data was safe.

Microsoft has now published mitigation guidance for CVE-2026-45585, the BitLocker security feature bypass linked to YellowKey.
Cybersecurity News reports that the issue affects Windows 11, Windows Server 2022 and Windows Server 2025, and works through the Windows Recovery Environment, WinRE.
The mitigation is important, but let's not pretend it is magic.
It helps protect machines you still control.
It does not fix notebooks that have already been stolen, lost, donated, recycled, handed to an employee's cousin, or left in that mysterious "old equipment" cupboard nobody wants to own.
If the device has already gone, the horse has bolted. And in this case, the horse may be holding a USB stick.

Microsoft's mitigation involves modifying the WinRE image and removing the risky autofstx.exe entry from the BootExecute registry value, then re-establishing BitLocker trust. Microsoft is also recommending that organisations move away from TPM-only BitLocker and use TPM plus PIN for stronger protection.

The message is simple that you can no longer treat BitLocker as a checkbox.

Review high-risk Windows 11 notebooks first, especially executives, finance, HR, legal, developers, administrators, and anyone carrying customer data, pricing models, credentials, confidential mail, or sensitive documents.

Check the basics properly.

- Is BitLocker enabled?
- Is it TPM-only or TPM plus PIN?
- Is Secure Boot enabled?
- Is USB boot restricted where practical?
- Is BIOS or UEFI protected?
- Are recovery keys safely escrowed?
- Are Windows, firmware and BIOS updates current?
- Is Intune, Defender for Endpoint, or your endpoint platform reporting the real state of the device?

For devices already stolen or disposed of, assume you may have a data exposure problem until proven otherwise. Disable the device, revoke sessions, reset credentials, review MFA methods, block access through Conditional Access and check sign-in activity.
Remote wipe is useful only if the machine comes online and connects to the internet. If it stays offline, it will not wipe.
That is not a security control, that is still just a wish with a Wi-Fi wand.

Please contact your First Technology Group account manager to connect with our security and endpoint specialists to review BitLocker, WinRE mitigation, Secure Boot, Intune compliance, and stolen-device response, and to assist in implementing the mitigation before the next notebook turns into someone else's goldmine.

Dave's Garage on YellowKey

Microsoft Releases Mitigation for YellowKey

The New Phish: How OAuth Consent Bypasses MFA

For years we trained users to spot fake login pages, strange links and dodgy emails.
The bad news, the click has changed.
The Hacker News article explains how attackers are now abusing OAuth consent screens.
The user is not tricked into handing over a password, instead they are tricked into approving access.
They go to a legitimate Microsoft sign-in page, complete MFA, click accept, and walk away thinking they have done the right thing.
They have not.
They may have just given an attacker a refresh token with access to mail, files, calendars and contacts.

MFA did its job. The user did what the screen asked. The attacker still got in, because the attack sits at the consent layer, not the password layer.

This is why the human being remains the weakest link, but not always because they are careless.
Sometimes the system asks users a question they do not properly understand, using language that sounds harmless, like “read your mail”, “access your files”, or “maintain access to data”.
They could have legitimately granted access to different systems and at different times using a single OAuth consent.
Separately, this would appear fine, but together, access is now granted across all, and only one needs to be "dodgy".
In business language, that can mean the attacker has approved access to invoices, contracts, HR files, board packs and customer data, long after the user has closed the browser and gone home.

Microsoft’s own guidance now makes it clear that organisations need to control user consent, review OAuth applications, monitor risky app permissions, and use admin consent workflows where appropriate.

Do not train users only to fear bad spelling and strange links. That battle has moved on. Users now need to understand consent prompts, AI agent permissions, browser extensions, third-party SaaS connectors and why clicking “Accept” can be just as dangerous as typing in a password.

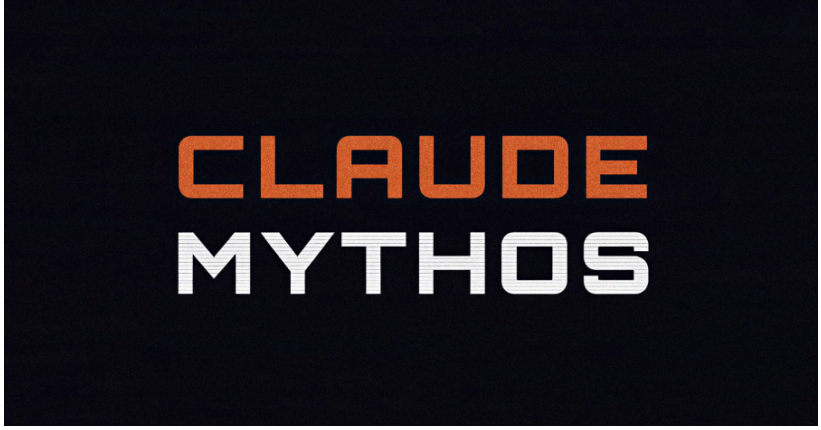
Contact your First Technology Group account manager to connect you with our security and training specialists. This is exactly the type of human-focused security training customised for your business that needs to be updated before users innocently approve the next breach.

The new OAuth Phishing Click

Cloud & AI

Claude Mythos Starts Finding the Skeletons in the Code Cupboard

AI is not only writing code anymore. It is now finding the nasty stuff hidden inside it.



Anthropic says its Project Glasswing, using Claude Mythos, has already helped uncover more than 10,000 high or critical severity vulnerabilities across widely used software.
That is impressive, and terrifying at the same time.
The good news is that AI can help defenders find problems faster.
The bad news is that attackers get the same idea, and they do not need a steering committee, budget approval, or a six-month procurement process to start using it.

This is why AI adoption cannot be separated from governance, security, developer controls, data protection and proper training.

Please contact your First Technology Group account manager to connect with our Cloud, AI and Security specialists before your users and developers quietly turn AI into yet another unmanaged business risk.

Claude Mythos AI Finds 10,000 High-Severity Flaws
