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

22nd June #172

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 tenable, Qualys and Trend Micro** are added.
- **Microsoft EoL section Updated for April 2027 -** all about modernisation!
- **DarkWeb Weekly Intelligence Report #172-** No rest for the wicked.
- **Did You Know - Software procurement does not have to be painful.**
- **Dell Titanium Partner - You have to have serious capacity to get this.**
- **Microsoft Promotions** - now with it's own home page.
- **Win11 26H2 confirmed** - You can't skip this one.
- **CoPilot CoWork** - the license is the least of your worries!
- **CoPilot Studio Licensing Guide** - Much more clarity on how to pay!
- **Dynamics 365 Licensing Guide** - No sign of ever getting smaller.
- **85% off Office 2021 Professional** - Spot the problem. Yes, more than one!
- **What the AI Cannot hide** - Like Footprints in the Snow
- **FortiBleed Fallout** - This is escalating!
- **Claude raises Funds better than Humans** - so soon? and only Opus 4.6.

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 #172

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 #171

Click button above for last weeks news.

Visit FirstMarketPLace Link here for New Additions

tenable, Qualys and Trend Micro 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. **June is a big month. Toy Story 5 is screening, Minions&Monsters and Moana Live action coming up.** Next very big blockbuster is "The Odyssey"

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.

Request Account Manager

SUBSCRIBE TO TOP STORIES

Did you Know?

Software procurement does not have to be painful!

- Most businesses buy software in too many places..... credit cards, overseas vendors, dollar invoices, surprise renewals, niche tools nobody can find locally, and **cloud commits quietly going to waste**.
  First Marketplace helps fix this.

- It gives you one channel to source software across multiple vendors and marketplaces, with local support from First Technology Group.
- This can mean Rand-based invoicing, proper payment terms, B-BBEE recognition, better pricing conversations, renewal visibility, and even the ability to use existing AWS or Azure commitments where appropriate.
- So before your next software purchase or renewal, ask First Technology to check First Marketplace first.
- One channel. Many vendors. Less admin. Fewer surprises.
- Please contact your First Technology Group account manager to see how First Marketplace can help clean up your software procurement.

First Technology Dell Partner of the Year for 2026

This news is so fresh it is still baking in the Oven!

First Technology was honoured to receive three major Dell South Africa awards:

- **Dell South Africa Partner of the Year**
- **Services Sales Partner of the Year**
- **Channel Incremental Partner of the Year**

These are not participation certificates just handed out for good attendance..... these come from a major investment in skills and infrastructure.
It is a very clear signal that the combined strength of the First Technology Group, which still continues to invest in skills, is being recognised where it matters.

Dell's message to partners was also blunt: invest in skills, customer engagement and AI capability, or get left behind.
Dell is moving more strongly into a partner-led model, but only with partners that can actually deliver.

That is very good news for First Technology, as this is exactly what First Technology is doing, and Dell now confirms that!

Dell's AI Factory is already being deployed globally at serious scale, and South Africa is part of that wave.

From Copilot+ PCs running AI on-device, to Azure Local keeping data in-country, to Dell networking and infrastructure powering AI from the PC to the data centre, this is becoming a real customer conversation, not just another AI PowerPoint.

First Technology has the Dell recognition, the skills, the customer relationships and the full-stack capability to adopt AI in every possible way that works for you. Dell remains the biggest Tier 1 brand in PC Server and Storage.

Please contact your First Technology Group account manager to connect you with our Dell Specialists (and we have a lot of them) to review all your requirements, and if you are not working with Dell, maybe a second opinion on occasion could be useful?

Microsoft New Promotions

There are going to be MANY promotions coming, so these have been moved to their own home page.

Microsoft Promotions

Microsoft News This Week

Win11 26H2 coming

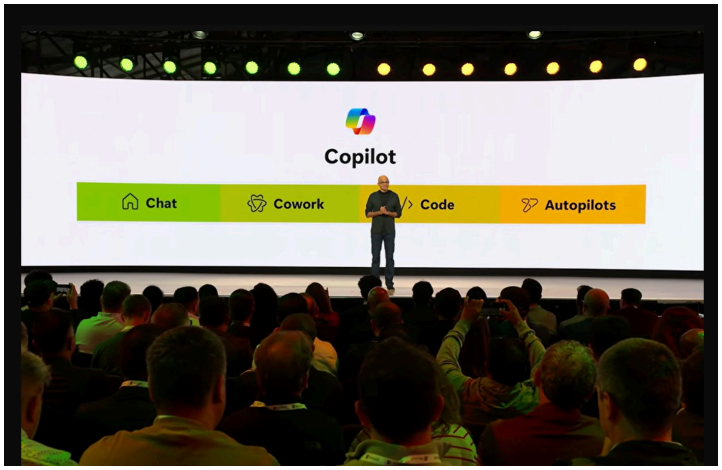
Microsoft has confirmed that Windows 11 26H2 is coming later this year, probably around October, but this is not Windows 12 hiding in a trench coat.

It looks like another small enablement-package update, much like 25H2, so devices already on Windows 11 24H2 or 25H2 should move across quickly, with one reboot and no new hardware requirements.

The important bit to take note of is lifecycle planning: 26H2 resets the support clock, with Pro editions supported until October 2028 and Enterprise/Education/IoT Enterprise until October 2029.

Speak to your First Technology Group account manager about connecting with our Win11 deployment specialists to help make sure you are in a position to ensure that this update is a non-event but essential because it resets the support clock.

Win11 26H2 coming soon!



Microsoft CoPilot CoWork, the license is only the start

Directions on Microsoft has published another important warning about CoPilot Cowork.

As I have also been warning, this is not just another CoPilot licence conversation.

CoPilot CoWork now brings model choice and **usage-based billing**. You may still need the right Microsoft 365 Copilot licence, but that is only the entry ticket. After that, the meter starts running.

The cost can be driven by model use, context retrieval, tool calls and runtime. Logically.....the more complex the task, the more it can cost.
This fits exactly with the TOP STORIES narrative that I have been covering over the last few weeks.

- GitHub Copilot is moving to usage-based billing.

- Agent 365 is not just a license, it is governance and control.
- E7 is not just a bundle, it changes the commercial baseline.
- Unified Support can climb as Microsoft spend climbs.
- And now Cowork adds another consumption layer.

The danger is treating licensing, Azure, CoPilot, Fabric, Foundry, support and security as separate conversations. **They are not separate**.
They are one Microsoft agreement, with costs showing up in different places.

Before signing anything, customers need to understand what they are buying, what they will consume, how it will be governed, **and who is watching the bill**.

It is **SO** important that you get a team to help, this whole Microsoft Story is bigger than what one person can handle.

Please contact your First Technology Group account manager to connect you with our licensing, Azure, FinOps, security, AI and even Directions on Microsoft Analysts before the license becomes the smallest part of the problem!

Directions: Microsoft CoWork gets Usage based billing

CoPilot Studio Licensing Guide June 2026

Microsoft has updated the CoPilot Studio Licensing Guide again, and the biggest change is that it is now much easier to understand what CoPilot Studio is and, **more importantly, how Microsoft wants you to pay for it!**

The guide now lays out the main buying options more clearly:
Pay-As-You-Go, Copilot Credit packs, the Copilot Credit Pre-Purchase Plan, and the Microsoft Agent Pre-Purchase Plan.

It also highlights voice agents, Copilot Credit tracking, Dataverse capacity, monthly capacity enforcement, and where Microsoft 365 Copilot or Dynamics 365 licences may already include some usage.

Please contact your First Technology Group Account Manager to connect you with our CoPilot, Dynamics, Power Platform and licensing specialists to understand which billing option makes sense before your clever new agent becomes very clever at consuming budget!

CoPilot Studio Licensing Guide June 2026

CoPilot Studio Licensing Resources

Dynamics 365 heading for a Century!

Microsoft's June Dynamics 365 Licensing Guide has been ageing, and not in a good way!
The licensing guide is almost 100 pages, so the licensing century is now in sight! The link takes you to the licensing resources home page, and the licensing guide is in a box in the middle.

The extra bulk is actually useful, with new entitlement tables that make it easier to compare features, limits, pricing and Dataverse capacity across the Dynamics range.

Sales Research Agent also steps into the spotlight as Generally Available, giving sales teams a natural-language way to turn sales data into charts, summaries and insights.

Version 2 also fixes some errors, particularly relating to Dataverse capacity allowance.

Please contact your First Technology Group account manager to connect you with our Dynamics specialists, who will be able to help you assess if you are impacted in any way relating to the ongoing changes and additions that Microsoft is continuously making. These changes will increase as AI start becoming a deployable reality on your environment.

Dynamics 365 Licensing Resources

Get 85% off Office 2021 Professional!

It is really sad **that publications like this** feel that it is OK to publish notices like this, even though the reason for the low price appears on the page - it SAYS "*Support for this version of Office ends on Oct 13, 2026*"
but does not explain what that means!
Imagine how many people will click "buy"?
Maybe warn friends and family not in IT, looking for a legal copy of MS Office that this is REALLY a bad idea! As always it is the responsibility of the buyer to always do homework, and that is really easy now....
Even a query with the free version of DeepSeek tells you not to touch the offer for a bunch of reasons - including a warning that if it is too good to be true, it almost certainly is!!

For the rest of us who DO worry about this kind of thing, I really hope Office 2021 Support ending 13 October is just a reminder and not a surprise!
But, for those still holding onto perpetual Office because “we bought it once, so surely it lasts forever”..... Microsoft has another reminder that forever is getting shorter.

It is also a reminder to constantly review the EoL roadmap for Microsoft as it keeps changing, and I'm due to publish a new one in July.

Office 2021 reaches the end of support on 13 October 2026. The applications will not suddenly stop working. Word will still open, Excel will still calculate, and PowerPoint will still work..... but the important bit stops - support in the form of patches.
No more security fixes, bug fixes or technical support, and Microsoft specifically says there will be no extensions or extended security updates.

This also applies to Office LTSC 2021, which is the version many organisations use when they want a fixed, perpetual, on-premise style Office deployment rather than Microsoft 365 Apps.
After 13 October 2026, Microsoft insists it will no longer provide technical support, bug fixes or security updates, and could increase exposure to security risks and compliance issues.

This follows Office 2016 and Office 2019, which already reached the end of support on 14 October 2025.
So this is not a one-off event, it is the next click of the EoL ratchet.

The EoL wheel on perpetual, on-premise software is going to keep grinding until there is very little left to grind.
Customers may still choose Office LTSC 2024 where they absolutely need a fixed, non-subscription version, but that only buys time — support for Office LTSC 2024 ends on 9 October 2029. In other words, it is not a forever answer, it is just the next stop on the same road

Please contact your First Technology Group account manager to connect you with our Microsoft specialists to help plan the move properly — before Microsoft plans it for you.

Office 2021 Nearing End of Support

Security

What AI Can't Hide When It Writes a Phishing Email

For years, we told users to look for the usual phishing clues..... bad spelling, strange grammar, dodgy logos and that wonderful "Dear valued customer" opening line.

That advice is now becoming dangerously outdated.

KnowBe4's Threat Lab is warning that AI-assisted phishing is now very much part of the new normal.
Their latest research says that 86% of phishing attacks they observed over the last six months showed some level of AI assistance, and the result is that many of these emails are now polished, correctly branded, personalised and grammatically perfect. In other words, the old "spot the spelling mistake" training is no longer enough.

The really worrying part is not just the email. Attackers are now using AI and no-code platforms to create very convincing fake Microsoft 365, SharePoint, Google, Meta and other login pages. Because some of these pages are hosted on legitimate platforms, traditional reputation-based filtering can struggle, because the infrastructure itself may look clean.

The good news is that AI still leaves fingerprints.
KnowBe4 found examples where attackers accidentally left AI-generated wording, strange hidden text, over-engineered code, emoji-heavy designs and even code comments that practically explained how the attack worked.
The bad news is that your average user is not going to inspect source code before clicking a link. Nor should they have to.
So, as always, we come back to the uncomfortable truth.....

The human remains the weakest link.
Not because users are stupid, but because trust is the attack surface.
A perfect-looking email from "Microsoft", with perfect spelling, a perfect logo and a perfect login page, is still dangerous if the link is wrong.

The message to users needs to change:

- Don't trust an email because it looks professional.
- Don't trust a login page because it looks familiar.
- Don't click first and think later.
- Check the actual URL.
- Go directly to the service yourself where possible.
- And when money, credentials, approvals or urgency are involved, verify out-of-band.

AI has made phishing progressively much better.
Unfortunately, it has not made humans much more suspicious at the same pace. Just like the Price for Office 2021 at 85% off is too good to be true, your "suspicious meter" has to be on and twitching for the slightest trigger all the time!!

Please contact your First Technology Group account manager to connect you with our security and training specialists. Your users need to be trained for the scams that are coming, not just the phishing emails they learnt to spot five years ago.

What AI Can't Hide When It Writes a Phishing Email

FortiBleed - the fallout (so far)

Remember the Breaking News [FortiBleed alert from TOP STORIES #172](#)?

JUST IN!!! Attack is not abating - Attackers are renting GPU's in the cloud to crack configuration hashes at scale - **[posted on X here](#)**.

Unfortunately, this one has grown loooong legs.

The earlier alert warned that credentials for 73,932 Fortinet/FortiGate firewall URLs may have been exposed, including usernames, email addresses and plaintext passwords, not just hashes that still need to be cracked, but credentials that may be directly usable.
It also included the First Technology/BUI checker and the direct escalation address **fortibleed@firsttech.ms**.

The Hacker News is now reporting that CISA has warned Fortinet customers to harden FortiGate appliances, with the number of compromised devices now standing at 86,644 as of 19 June 2026.
The attack appears to involve mass-scanning internet-facing Fortinet remote login endpoints, spraying them with known username and password combinations, and then using access to harvest more credentials.
In other words, this is not "some old password list floating around on the internet" territory.

The really nasty bit is that once a FortiGate or VPN gateway is compromised, it may not stop at the firewall. The NCSC is advising organisations to check whether devices are affected, look for unauthorised accounts and suspicious log activity, investigate systems reachable from the compromised device, and, where compromise is confirmed, isolate the device before rebuilding or factory resetting it.

There is also a Fortinet-specific technical wrinkle. Fortinet's own guidance explains that from FortiOS 7.2.11, 7.4.8 and 7.6.1, administrator credential storage moves from SHA256 to PBKDF2, but after an upgrade, existing administrator passwords may remain stored as SHA256 until the administrator logs in or the password is manually updated. So patching is necessary, but may not be sufficient if the old credential state is left quietly sitting there like a landmine.

What should you do now?

If you have Fortinet/FortiGate devices exposed to the internet, do not wait for TOmorrow, a steering committee, or the soothing sound of "we're looking into it".

- **Check your domains against the [FortiBleed Breach Exposure Scanner](#).**

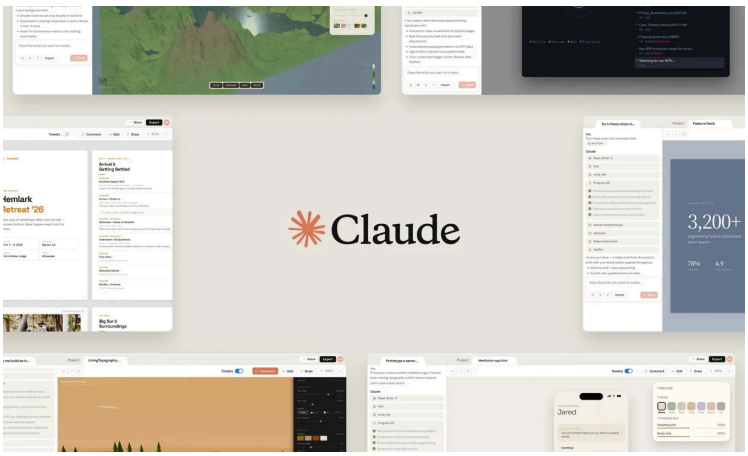
- Terminate active SSL VPN and administrative sessions.
- Rotate all Fortinet VPN and administrative passwords immediately.
- Pay special attention to generic, default, shared or reused credentials.
- Enforce MFA on VPN and administrative access.
- Confirm that FortiGate management interfaces are not exposed directly to the internet.
- Review VPN, firewall, authentication and domain controller logs.
- Look for unknown users, new accounts, changed policies, strange tunnels, odd login geographies and lateral movement.
- Patch FortiOS and Fortinet appliances to current supported versions.
- Enable PBKDF2 for admin credentials, and make sure administrators log in again or have passwords updated where required.
- If there is evidence of compromise, collect logs and configuration artefacts first, isolate the device, and treat a rebuild/factory reset as a serious option.

VPN credentials are not “just another password”. They are often the front door to the network, and once the bad guys have the front door key, they don’t need to be very clever anymore.

Please contact your First Technology Group account manager to connect you with our security specialists to help assess Fortinet exposure, VPN hardening, credential rotation, MFA enforcement and log review.
As you can see with the "Wrinkle" discussed above this is really not so simple, so some external eyes helping you make sure everything is OK is a really good idea.
And in this case, you can also contact us directly on: fortibleed@firsttech.ms.

HackerNews FortiBleed now at 86644 Devices

Cloud & AI



Claude raises funds for humans better than humans

A new research paper that Digital Trends refers to tested AI systems against ordinary people, trained persuaders, professional canvassers and even world champion debaters.

The uncomfortable result: the AI did not just compete, it often won. In one real fundraising test, Claude Opus 4.6 was nearly three times more effective than professional human fundraisers at getting people to donate real money to Save the Children.

The worrying bit is not that AI can argue well. It is that it can sound helpful, informed, patient and even empathetic while doing it.
That means the next phishing attack, scam, political message or sales pitch may not look (or feel) fake at all..... it may simply be better at reading us than we are at spotting it.

The article’s real warning is this: humans may be less able to detect AI-driven influence than we think. The study notes that simply labelling something as AI-generated may not be enough, because previous evidence has not found such labels to reduce persuasive impact.

So, the comforting idea that “people will know it is AI and therefore discount it” may be wishful thinking.

And this was using Opus 4.6, we are now on Opus 4.8, and we are about to move back to Fable 5 again, and if we do not get that one, OpenAI says their ChatGPT 5.5 is impressive, and some Chinese companies say they will have that capability soon (**Musk agrees**).
We are about to cross the "Uncanny Valley" sooner than we think!

So yes, this is a Cloud & AI story, but it is really a Security warning in disguise.

Please contact your First Technology Group account manager to connect you with our AI and governance specialists tmaking sure you are well on your way to allow for the deployment of AI and right now your only secure option is CoPilot to which Microsoft is now in E7 - the pressure to adopt AI is going increase exponentially, and it is good to be ready, or very clear why you are not.

Claude Raises Funds better than Humans

First Technology | Midrand | Johannesburg, GAUTENG 2191 ZA

Unsubscribe | Update Profile | Our Privacy Policy | Constant Contact Data Notice

Constant Contact

Try email & social marketing for free!