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

18th May #167

New for This week - YellowKey - You MUST read!

- 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 mariadB, Waves and Flowgear** are added.
- **Microsoft EoL section Updated for April 2027 -** all about modernisation!
- **DarkWeb Weekly Intelligence Report #167-** Mythos is lurking in the Shadows
- **Webinar -** You have no process for reading PDF's! But you will, if you attend!
- **GitHub CoPilot Usage Billing** - It's not what you do, it's how much you do it!
- **The Multiple Equivalent Offer Trap** - Many columns to confuse.
- **Win11 being taught to Hurry Up** - Amazing what a clean-up can do.
- **YellowKey** - How to turn a stolen Notebook into Gold.
- **Mythos cracks a MAC** - Researchers found a hole in record time
- **GenAI Ruins training plans** - being taught not to click on links is yesterday's news.
- **Microsoft Wins the Control Plane** - Microsoft may just succeed with its AI gambit.

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 #167

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 #166

Click button above for last weeks news.

Visit FirstMarketPLace Link here for New Additions

mariadB, Waves and Flowgear 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**

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.

You have no process for reading PDF's!

First Digital Webinaar

Register to attend the Nintex webinar here on May 21st

Deploy intelligent workflow that detects issues, routes work, and learns over time.

Request Account Manager

SUBSCRIBE TO TOP STORIES

Microsoft News This Week

GitHub Copilot moves to usage-based billing

Advanced GitHub Copilot tasks have, until now, been measured using Premium Requests. Each Copilot plan included a monthly allocation, with extra usage available on a Pay-As-You-Go basis.

That changes from 1 June 2026.

GitHub is replacing Premium Requests with GitHub AI Credits. Each Copilot plan will still include a monthly allowance, but consumption will now be tied much more closely to actual usage. In other words, a quick coding question and a long agentic coding session will no longer be treated as the same thing.

The heavier the task, the more it costs.

Longer prompts, bigger outputs, cached context, more advanced models and multi-step coding sessions will consume more credits. GitHub says this is because Copilot has moved from being a simple coding assistant to something closer to an agentic development platform, and the old Premium Request model no longer reflects the real compute cost.

For customers, the practical point is simple, Copilot is becoming more consumption-based. You will need to understand which users are doing lightweight work, which users are running heavier AI coding workflows, and how budget controls are being managed.

1 GitHub AI Credit equals $0.01 USD, and code completions and Next Edit suggestions remain included in paid Copilot plans without consuming AI Credits.

Please contact your First Technology account manager to connect you with our Licensing and GitHub experts to assist with understanding how you are impacted by these changes and to budget more accurately for the future.

GitHub Copilot is moving to usage-based billing

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 11 is finally being taught to hurry up

Last week we covered Microsoft's hidden Low Latency Profile, which gives Windows 11 a short CPU boost when you click something, making apps, menus and Start feel much snappier.

Now Microsoft is also working deeper down in the Windows interface itself. The company is optimising WinUI 3, the framework used by newer parts of Windows 11, including File Explorer and Notepad. Early work has reduced object allocations by 41%, transient allocations by 63%, function calls by 45%, and time spent in WinUI code by 25%.

In other words, Microsoft is not just pressing the "go faster" button for a few seconds, it is also trying to make the interface less bloated in the first place.

This matters because users do not judge a PC only by benchmarks. They judge it when Start opens slowly, File Explorer drags its feet, Outlook takes forever, and the right-click menu behaves like it has gone for tea.

If Microsoft gets this right, Windows 11 could start feeling noticeably more responsive, especially on the 16GB machines many businesses are still trying to keep alive. But don't treat this as a reason to buy weak hardware. Treat it as one more reason to build cleaner Windows images, remove junk, control background agents, and still aim for 32GB RAM wherever possible as you need to leave breathing room for AI capability you do not even know you will need!

Please contact your First Technology account manager to connect you with our deployment experts to ensure that we are helping you build debloated, optimal images that get the most out of your PC's resources today, allowing you to be well prepared for these new performance improvements in the near future.

Microsoft's Windows 11 UI Is About to Get Much More Responsive

Security

Yellowkey turns a stolen notebooks data into gold

This is a scary example of how quickly you can be impacted by a new vulnerability. News first broke publicly on 13 May, and within days we had a serious issue to deal with.

Most importantly, do not panic, but you must acknowledge that this is a VERY REAL problem.
YellowKey is a publicly released BitLocker bypass affecting Windows 11 and Windows Server 2022/2025 through the Windows Recovery Environment.
It appears most relevant to devices using default TPM-only BitLocker, although TPM plus PIN should be treated as a risk reduction step, not a magic force field.

Organisations should urgently review high-risk Windows 11 laptops, harden boot and recovery paths, consider TPM+PIN for sensitive devices, restrict USB boot, protect UEFI settings, *and treat already stolen TPM-only affected devices as potential data exposure events rather than assuming BitLocker alone protected them.*
Current public reporting says the published YellowKey proof of concept affects Windows 11 and Windows Server 2022/2025, and the published PoC has not been shown to work on Windows 10.
That is NOT a reason to delay Windows 11. Unsupported Windows 10 devices are accumulating risk, and staying there is not a strategy.

There is a darkly funny side to this, if you lost your keys, YellowKey has apparently come to your rescue.
But do not treat this as a recovery method but rather as a security incident.

YellowKey
I find the name for the bypass interesting.
Yellow is sometimes associated with gold, and if that notebook contains customer data, HR files, legal documents, pricing models, credentials or confidential emails, the thief may have found the equivalent of the "pot of gold".
If that Windows 11 device was protected only by standard TPM-based BitLocker, and it is still sitting somewhere with the data intact, it may have just become a lot more interesting to the wrong person.

What do I do?
First, identify high-risk Windows 11 notebooks.
Executives, finance, HR, legal, developers, administrators and anyone carrying sensitive data.

Then, check and implement the basics.

- BitLocker recovery keys backed up properly?
- TPM enabled?
- Secure Boot enabled?
- USB boot disabled where practical?
- BIOS/UEFI administrator password set? (be VERY careful here - get help for this)
- BitLocker TPM plus PIN applied to high-risk devices? (Check how with OEM)
- Windows patched?
- BIOS and firmware updated, but tested first?
- Intune, Defender for Endpoint, or your endpoint tool reporting the real device state?

For notebooks already stolen, the horse has bolted.
You can no longer assume encryption saved you.
Confirm whether BitLocker was enabled, whether it was TPM-only or TPM plus PIN, whether Secure Boot was enabled, whether the device was compliant, and whether the recovery key was safely escrowed.
Then kill access.
Disable the device, revoke Microsoft 365 sessions, force a password reset, review MFA methods, block access through Conditional Access and check sign-in logs after the theft.
Remote wipe is useful only if the device comes online. If it stays offline, it will not wipe. That is not a strategy, that is a "wish with a Wi-Fi wand".
If sensitive data was on the device, escalate properly.
Security, legal, compliance and the data protection officer need to decide whether this is just a stolen asset, or a reportable incident.
BitLocker still matters.
But the question has changed. It is no longer, “Was it encrypted?”.
It is, “Can you prove it was protected well enough when it disappeared?”

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

Dave's Garage on YellowKey

BitLocker Bypassed with USB stick

Mythos finds first macOS Kernel Exploit on M5

Here is nasty reminder that ALL computing systems are increasingly vulnerable, and though the Apple "walled garden" is generally more secure, it can no longer be assumed to be more secure. Using MAC's to improve your security can no longer be a strategy.

Researchers at Calif say they used Anthropic's Mythos Preview AI tool to build a working macOS kernel exploit in five days. It targets macOS 26.4.1 on Apple M5 hardware and reportedly bypasses Apple's Memory Integrity Enforcement, which is supposed to make this type of memory attack much harder.
This is not the usual "Macs don't get viruses" conversation.
The bigger story is that AI-assisted vulnerability research is getting frighteningly productive.
Human insight proved essential for bypassing the novel MIE mitigation.

The Human/AI partnership meant what took elite researchers weeks or months can now happen much faster, and yes, the bad guys will also notice.
They always do.

The exploit is a local privilege escalation, meaning the attacker first needs code running on the Mac. But once that happens, it can move from a normal user to root. In simple terms, the bad code gets the keys to the building.

Windows, Linux and macOS are all now in the firing line.
The operating system "badge on the lid" is not a security strategy.

Mythos assists in finding macOS Kernel Exploit

GenAI Has Shattered Decades of Cybersecurity Training

For years we have told users not to click strange links, not to open dodgy attachments, and not to trust emails from long-lost Nigerian princes with cash-flow problems. That helped us, mostly.

Not anymore

Gartner is warning that GenAI has broken the old cybersecurity awareness model. The problem is not only that attackers can now write better phishing emails. They can write perfect emails, in your style, in your language, with no spelling mistakes, no weird grammar, and no obvious red flags.
In other words, the bad guys have finally learnt to spell!
The human being remains the weakest link, as always. AI has just made that link easier to find, easier to pressure, and easier to fool.
The risk is also no longer only incoming phishing attacks.
Employees are creating new risks themselves by using personal AI tools for work, pasting sensitive company information into public GenAI platforms, and downloading unapproved AI tools because they help them get work done faster.

That is the uncomfortable bit. People are not being reckless because they are stupid. They are not even aware that their actions are reckless. To them they are just using tools that are useful!

Traditional annual training, posters, and "don't click the link" reminders are not going to fix this. Gartner says GenAI adoption is creating new attack surfaces and that traditional awareness efforts are failing, with 57% of employees using personal GenAI accounts for work and 33% entering sensitive information into unapproved tools.

Users now need practical, continuous, real-world training that deals with AI-powered phishing, deepfakes, prompt injection, fake approvals, fake voices, and fake urgency.

The new rule is simple.
If the request is unusual, urgent, financial, sensitive, or slightly weird, verify it through another channel. Even if it sounds like your boss. *Especially* if it sounds like your boss.
A little friction is no longer inefficiency. It is survival.

Please contact your First Technology Group account manager to connect you with our Training experts who specifically address this issue, and to go further and provide training that is customised for the business you are in.

Gartner Warns GenAI Has Shattered Decades of Cybersecurity Training

---

Cloud & AI

Microsoft leads the next AI battleground, the agent control plane

The enterprise AI conversation has moved on. For the past two years it has been about models, GPT versus Claude versus Gemini, but new VB Pulse survey data shows the real fight is now over who controls the layer where agents actually run, plan, call tools, access data and prove to security teams that they behaved.

The numbers tell the story. Microsoft Copilot Studio and Azure AI Studio lead enterprise agent orchestration with 38.6% primary platform adoption in February, up from 35.7% in January, and no other platform within 13 percentage points.
OpenAI's Assistants and Responses API holds second at 25.7%, and Anthropic has just appeared in the tracker at 5.7%, its first measurable foothold. Microsoft is, in plain language, the enterprise default.
The reason matters. A model is relatively easy to swap, route one workload to Claude, another to GPT, another to Gemini. An agent runtime is not.
Once your workflows, tool permissions, credentials, audit logs, sandboxed execution and operational monitoring live inside one provider's environment, switching providers becomes less like changing a model and more like changing infrastructure. **That is exactly why Microsoft's distribution advantage through Microsoft 365, Teams, Entra ID and Azure is so important. The pieces required to govern agents properly, identity, permissions, audit, observability, are already in place for most Microsoft customers.**

Buyers are voting accordingly.

Security and permissions ranked as the top orchestration platform selection criterion at 37.1%, with control over agent execution rising sharply, while pure flexibility across models and tools fell.

The market is shifting from optionality toward governance, which is exactly the conversation Microsoft's Agent 365 launch (covered last week) was built for.
David Weston, Microsoft's CVP of AI Security, summarised it neatly, without a unified control layer, agents operate in silos, governance is inconsistent, and gaps appear in security.

There is a warning embedded in the data too.
Vendor lock-in concern rose from 23.2% to 25.7%, the only risk category that increased. Around 35% of enterprises expect to run a hybrid control plane, combining provider-native orchestration with external orchestration, rather than handing the whole stack to one vendor.

This is sensible, and it is the conversation South African customers should be having now, before agentic workloads scale. The question is not which agent platform looks shiniest, it is which one already integrates with the identity, data and governance estate you have, and what your exit options look like.

Please contact your First Technology Group account manager to connect you with our Modern Work and security specialists who can map your existing Microsoft estate against an agentic roadmap, prioritising Copilot Studio and Agent 365 where they fit, while keeping your control plane options open.

Microsoft leads the next AI battleground, the agent control plane