



Your Weekly guide in a Changing World.
Written and edited independently by Barry Neethling
Sponsored by First Technology Group

19th October #189

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: Verint, MSP360, hexnode** are added.
- **DarkWeb Weekly Intelligence Report #189**- The bad guys are extra busy!
- **First Technology's AI Factory** - Did you Know it's actually in production
- **Spark Hype** - The hype needs to fizzle before you rush out and buy.
- **Email Archive** -Bumped to 3TB
- **October Patch Tuesday** - Over 1000 patches!
- **Publisher Rescued** - By LibreOffice
- **Win11 Gets Leaner** - Actually works in 8Gig - yes, really!
- **Defender for Linux** - Enough Linux Desktops need protecting
- **Chinese Phishing Network taken Down** - It was HUGE!
- **Ransomware Gets Personal** - PLEASE READ THIS!!!!!!
- **AI and SRI** - NOW it is getting scary!

CTA - Sponsored message from First Technology Group

Forward this mail to others who may find this useful and invite them to subscribe using the button below.

Subscribe to Top Stories

DarkWeb Executive Report #189

CTA - Sponsored message from BUI

BUI scans the DarkWeb continuously for Hacker signals and Ransomware attacks.

Click above for the report from our live dashboard that we will publish weekly (but is 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.**

Last Week's Top Stories

SignUp for the Archive

You can click the top button for last week's edition or sign up for access to the archive with AI assistance to read from #1

Newest additions to FirstMarketPlace

CTA - Sponsored message from FirstMarketPlace

Verint
MSP360
hexnode

Are added for this week.
Click the link above for more information on these vendors

New Movies for this week

Digger Dug a hole Maybe it will become a cult classic and an Oscar for Tom!

CTA - Sponsored message from First Technology Group

Did You Know... First Technology Group has its own AI factory?

Not a plan. Not a pilot. Switched on in August, running live customer workloads ever since.

NVIDIA GPU's in a South African data centre, billed in rand, with your data staying inside the country.

Why does that matter?

Because of the three answers you keep getting.

No, legal won't let that data leave the country.

No, the budget can't take another unpredictable dollar invoice.

There's no capacity, join the queue.

This isn't another chat window. It's the engine underneath your AI.

Point whatever you're already using at it, change an address and a key, and carry on working.

What can I use it for?

Voice agents holding real phone conversations.

Contracts and delivery notes read and matched.

Camera networks that reboot and check themselves.

Years of call recordings turned into proper Quality Assessment data.

All of it running here. Today. For customers who were told they couldn't.

Want to see it before you commit to anything? Ask for a trial key, metered, so you know exactly what it would cost you.....

So what is your business **not** doing with AI right now, simply because somebody told you the data wasn't allowed to leave?

Please contact your First Technology Group account manager to connect you with our FirstCore.AI and FirstNet specialist teams to get a trial key in your hands and your first workload running locally.

CTA - Sponsored message from First Technology Group

First Technology Group AI Factory



The RTX Spark Let the Hype Settle

Last week, we covered Dell's new RTX Spark XPS and Microsoft's plans for hybrid intelligence.

The first reviews are now arriving..... and the practical advice is to let the excitement settle before rewriting the company's notebook purchasing policy!

RTX Spark has a credible role for developers and specialists who need substantial local AI capability, large amounts of shared memory and NVIDIA's CUDA software ecosystem in a portable machine.

BUT..... that currently looks like a specialist requirement, rather than the next standard notebook for every employee. Independent testing shows real AI capability alongside less convincing gaming results and substantial prices.

Availability needs to be considered - especially in the "outer reaches" like South Africa.

NVIDIA officially launched the notebooks on 16 October, so units exist! However, [Moore's Law Is Dead](#) reports very limited initial supply, potentially remaining constrained into early 2027. That is a report based on industry sources, nothing official. South African stock, configurations and delivery dates still need checking.

Do NOT put necessary notebook purchases on hold because we have a new "Spark" in Town.

If employees need reliable machines now, buy against their actual applications, performance requirements, battery needs, support and budget. A launch presentation does not make an otherwise suitable notebook obsolete..... nor does it help the employee waiting for a replacement!

For organisations planning purchases next year, this IS a good time to understand what else is coming.

Intel's Nova Lake notebook processors are reported to be targeting 2027, with potentially stronger integrated graphics alongside the next CPU generation. Detailed configurations, performance and notebook delivery dates still need confirmation.

Treat the leaked specifications as something to watch, rather than something to put into a purchase order.

AMD's roadmap also places its next Medusa Ryzen AI family in 2027, continuing its development of processor, graphics and local AI capability. There will be more to evaluate than NVIDIA alone.

Those competing platforms may offer more practical choices for mainstream notebook fleets. However, it is "safe" to assume that EVERYTHING will have supply constraints with memory pricing marching ever upwards.

Keep necessary replacements moving, evaluate Spark where there is a clear business case, and start planning for the wider 2027 choice.

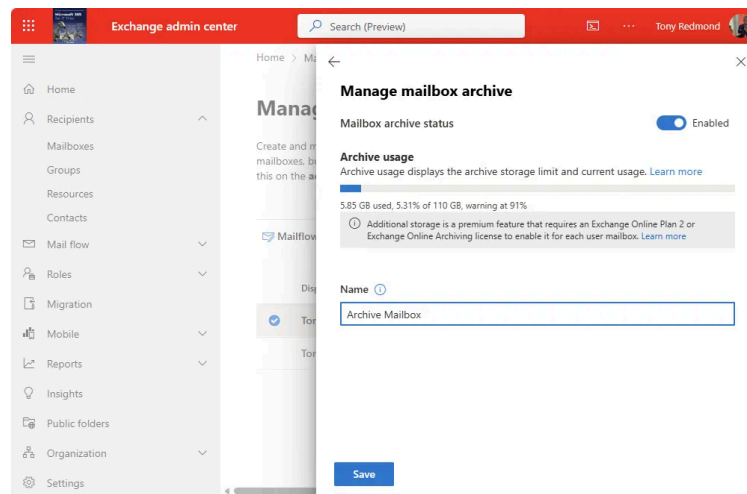
There is always another processor coming..... the trick is knowing whether waiting will improve the business, or merely make your employees complain for longer but gain little in practice.

Please contact your First Technology Group account manager to connect with FTG's hardware specialists. Ask them to review current requirements, supplier roadmaps and delivery commitments, and arrange evaluation units where available before committing to a new platform.

CTA - Sponsored message from First Technology Group

Toms Hardware Test of the Surface Ultra

Microsoft News



Microsoft Bumps Auto-Expanding Email Archive Limit Past 1.5 TB

Most of us will never worry about filling a 1.5 TB email archive..... even those who seem to have kept every email since the company bought its

first modem!

BUT..... companies with substantial historical correspondence and long retention requirements can have a very different problem.

Microsoft is doubling the maximum auto-expanding archive capacity in Exchange Online from 1.5 TB to 3 TB for eligible mailboxes.

Rollout is scheduled from mid-October, with completion expected by late October 2026. Eligible licences include Office 365 E5, Microsoft 365 E5 and qualifying Purview offerings, including E7. Other archive entitlements retain their existing limits. Microsoft's updated guidance

This adds detail that was still missing when the Office 365 for IT Pros article appeared in September.

The increase applies to the online archive, rather than your everyday inbox. Capacity expands incrementally as required. Where auto-expanding archiving is already enabled, Microsoft says eligible mailboxes need no additional configuration and incur no additional per-GB charge. Microsoft's archive explanation

For most businesses, this requires no urgent action. For those approaching the existing ceiling, it provides useful breathing room..... but more storage is still NOT a retention policy!

Keep what the business needs and must retain, monitor growth, and review information that no longer serves a purpose.

Please contact your First Technology Group account manager if large email archives are becoming a concern. Their Microsoft specialists can review licence eligibility, archive capacity and retention settings before storage limits become a business interruption.

CTA - Sponsored message from First Technology Group

Exchange bumps Archives to expand past 1.5TB

October Patch Tuesday.. Another headache?

October's Patch Tuesday arrived on 13 October with a rather substantial list of 1,413 vulnerabilities

addressed across Microsoft's products, including three zero-days.



The immediate concern is CVE-2026-96951, a Windows Shell security bypass that Microsoft confirms was already being exploited before the fix arrived.

This is therefore considerably more urgent than tidying up something that might, possibly, become a problem one day.

AI-assisted research is helping uncover vulnerabilities, but finding them and publishing fixes only gets the job halfway done.

Those fixes still need to reach your machines! Microsoft is also exploring ways to [group related vulnerabilities](#) to help businesses assess large releases more efficiently.

There are useful improvements.....

File Explorer gets better PDF previews, remembers expanded or collapsed Home sections and improves cloud-file thumbnails.

There are additional touchpad scrolling controls, an option to open applications maximised, and the ability to turn the fateful Copilot key into Right Ctrl or the Context Menu key.

Sometimes the most useful new feature is getting something familiar back! These improvements carry forward from September's optional preview, with availability varying as features roll out.

October also fixes problems involving Always On VPN, black screens in certain virtual desktop environments, printing and fingerprint sign-in.

BUT..... updates CAN cause headaches. Microsoft already lists issues affecting Smart App Control and some Remote Desktop connections.

Security hardening can also expose dependencies on older authentication methods. [Checking the known issues](#) and testing your business applications remains essential.

And then there is the reminder from TOP STORIES #188.....

Windows 11 24H2 Home and Pro support HAS ENDED. The 13 October update was their final scheduled monthly security update. Enterprise and Education 24H2 remain supported until 12 October 2027, so check BOTH your version and edition under Settings > System > About.

Installing October's patch does NOT extend Home and Pro support. Those machines also need to move to a supported release, such as 25H2 or 26H2, subject to compatibility and availability. If an upgrade is blocked, have IT investigate the reason before forcing it through.

Patch ASAP. Check known issues, confirm recoverable backups, test a representative group promptly, then deploy in controlled waves. Complete the required restarts and verify successful installation. Include affected Office applications and servers in the review.

A patch may cause a headache. Delaying protection can cause a bigger headache. Leaving an unsupported machine exposed to newly discovered vulnerabilities could cause a REALLY big headache!!!!

"It still works" is a poor security policy..... ransomware can change that rather quickly.

Please contact your First Technology Group account manager to connect with FTG's Windows deployment and security specialists, identify overdue patches and unsupported PCs, and arrange the updates AND version upgrades required.

CTA - Sponsored message from First Technology Group

October Patch Tuesday and AI Security Hardening



LibreOffice offers free Publisher support as Microsoft 365, Office end it

Microsoft Publisher has reached the end of the road.

Microsoft 365 began removing access from 1 October, while support for perpetual versions ended on 13 October. Perpetual licence holders can still use Publisher and edit their files, although the application is now unsupported.

LibreOffice offers an escape route. Its free Draw application can import Publisher's .pub files, allowing users to view, edit and save the content in another format. That capability comes from established open-source development and reverse engineering of the Publisher format.

BUT..... importing a document is not a guarantee that everything will behave perfectly.

My view..... increasingly, AI will help fill these gaps.

Expect more “vibecoded” alternatives, where developers use AI to help build applications, converters and editing tools for software that its original supplier no longer supports.

That is a promising role for AI-assisted development..... preserving access to information and keeping useful work alive after the original software retires.

BUT..... generating an application does not automatically solve file compatibility, security or ongoing maintenance. Somebody still needs to test it, protect the information it handles and fix it when it breaks.

Keep the originals. Test the alternatives. Check where your data goes.

Please contact your First Technology Group account manager to connect you with FTG's Microsoft and application specialists to assess affected files and a practical migration route.

CTA - Sponsored message from First Technology Group

LibreOffice offers free Publisher Alternative



**Windows 11
gets
leaner.....
32GB STILL
stays the
minimum!**

Microsoft says
Windows 11 is now up

to 20% more responsive, following improvements to memory management and everyday tasks such as Start, Search, File Explorer and Settings.

Welcome progress..... but.....

These are Microsoft's measurements of selected response times, NOT a promise that every application or your working day is magically 20% faster. Availability also varies by device and rollout..

Windows can now retain up to 2GB more active data in RAM instead of moving it to slower storage. On machines with 8GB or less, Widgets load only when opened, releasing more than 200MB for other work. **Useful savings..... but an 8GB machine is STILL 8GB!**

This follows Microsoft's earlier commitment to reduce Windows' memory footprint, including improvements to its application framework and embedded browser components. The October announcement puts figures against that continuing work.

BUT..... I have been warning for years that 32GB should be the minimum for a new corporate PC. That advice STAYS.

TOP STORIES reiterated the point in #179, and better Windows memory management does not change it.

A company PC carries considerably more than Windows. Teams, Outlook, browser tabs, spreadsheets and **business applications share resources with endpoint protection, device management, VPN software, synchronisation, monitoring and other background services.**

The employee may have closed a window..... the company's background software and security services has certainly not stopped running!

Making Windows more efficient leaves useful breathing room. It does not remove the memory requirements of everything else the business needs running. [Microsoft's own performance guidance](#) explains why available memory and paging matter to the complete user experience.

Yes, the extra memory is expensive, but do NOT let that persuade you to lower the 32GB purchasing minimum.

Compare the additional purchase cost with several years of employee waiting time, support calls and an earlier replacement.

A saving on the quotation can become a recurring expense at the desk.

For existing 8GB and 16GB machines, these improvements may buy useful time where the actual workload remains manageable. For new corporate purchases, my recommendation remains 32GB minimum, with more where demanding applications, virtual machines or local AI require it.

Better performance with less memory buys time..... it does NOT change the buying standard.

Please contact your First Technology Group account manager to connect with FTG's hardware and workplace specialists. Have them assess the complete corporate workload, optimise existing devices and specify new machines with sufficient memory for the years ahead.

CTA - Sponsored message from First Technology Group

Windows 11 gets more responsive with 8GB

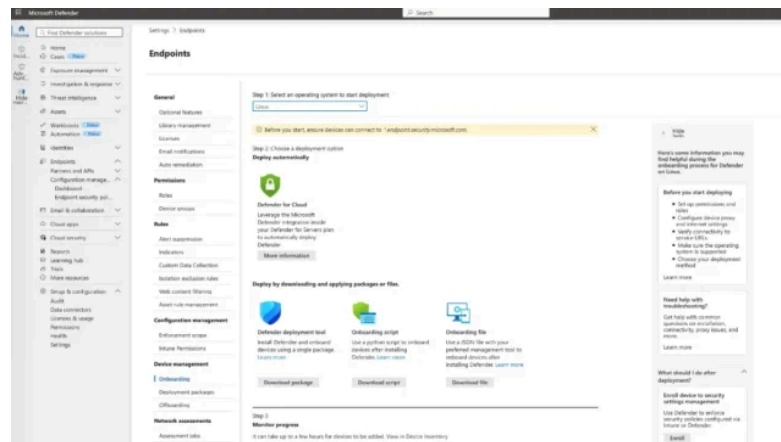
Microsoft brings Defender protections to Linux

Microsoft is extending Defender for Endpoint protection to Linux desktops through a public preview,

covering antivirus, threat detection, vulnerability management and tools to investigate attacks and isolate compromised devices. Its [official announcement](#) focuses particularly on developer workstations.

Why developers? Their machines can provide access to source code, cloud infrastructure and the systems that build and release software. Compromising one laptop could give an attacker a route into considerably more valuable territory.

The practical benefit is consistent visibility. Linux workstations use the existing Linux Defender agent and deployment methods, with security teams managing them alongside



other endpoints through the same portal.

BUT..... this is enterprise protection in preview. Microsoft specifies Defender for Endpoint Plan 2, or Microsoft 365 E5 or E7. Support depends on the underlying Linux distribution and kernel version, so compatibility and prerequisites still need checking.

One clarification is that defender already protects Linux servers. This announcement extends that protection to desktops.

For customers, the next step is to identify Linux workstations missing from their security monitoring and assess a controlled pilot. Choosing Linux does not make a machine invisible to attackers..... only, sometimes, to its own IT department!

Please contact your First Technology Group account manager to connect with their Microsoft licensing and security specialists to review eligibility, compatibility and deployment.

CTA - Sponsored message from First Technology Group

Microsoft bring Defender to the Linux Desktop

Security



**Chinese
Phishing
Network
Linked to 1
Billion
Messages
Targeting
75,000
Organisations**

[Microsoft says those figures](#) cover the wider YAM Store, CoGUI and Iron Man criminal ecosystem since January 2026.

They describe targeting, NOT 75,000 confirmed breaches.

Now Microsoft's Digital Crimes Unit used a US court order to seize and redirect domains powering the operation.

Microsoft also disabled more than 20,000 accounts connected to YAM Store and says it continues blocking over 100,000 domains used for impersonation and fraud.

This is phishing organised as a commercial service. Criminals could purchase accounts, infrastructure and ready-made tools rather than build everything themselves.

Resecurity identified 2,360 Iron Man phishing templates impersonating couriers, banks, retailers and government agencies, with ongoing updates to both the software and the bait.

Apparently, even the phishing industry understands continuous improvement.

A welcome disruption..... BUT it is not the end of phishing.

People remain on the receiving end of industrial-scale attacks, each trying to turn a familiar name, an unexpected bill or a delivery problem into a hurried decision.

Once again, the human remains the weakest link. A busy person expecting a parcel does not need to be particularly careless. The right message arriving at the wrong moment can be enough.

That is why security awareness needs training..... and repeated training.

A once-off presentation and a completion certificate will not keep staff prepared as the attacks adapt.

Make reporting easy and free from blame.

Technical controls must support staff, because no training can make everyone spot every attack.

Microsoft and its partners like BUI can disrupt the infrastructure, but businesses still need to prepare the people receiving the next message.

Please contact your First Technology Group account manager to connect you with FTG's security specialists and review whether your staff awareness programme provides regular, relevant training as attacks evolve.

CTA - Sponsored message from First Technology Group

Industrial Scale Chinese Phishing Network Disrupted



Ransomware gets Personal

An attacker has one goal in mind: They want to extract something from you. And the only way they're going to do that is to make the cost of resisting their demands greater than the cost of giving in.

Holding you at physical risk is the latest phenomenon because we've covered most of the other risks.

(Chris Inglis: Former U.S. National Cyber Director and Semperis Strategic Advisor)

Ransomware investigators have seen criminals send executives photographs of their children's schools to pressure them into paying.....deliberate cruelty..... using a parent's fear as another means of extracting money.

[Semperis surveyed 1,200 IT and security professionals](#) whose organisations had suffered ransomware attacks.

Respondents reported physical threats in 17% of cases, while 25% reported staff or families needing medical or psychological treatment.

Separately, the FBI has documented cybercriminal networks using kidnapping, torture and threats against relatives in cryptocurrency extortion.

The boundary between cybercrime and physical violence has already been crossed.

As organisations strengthen backups and recovery, criminals seek additional pressure points.

And so, the human remains the weakest link..... and fear for your family can overwhelm even the most security-conscious professional.

Training **MUST** be regular, practical and continuously updated. Staff need to recognise intimidation and impersonation, independently verify unexpected requests and report threats immediately.

Families also need guidance on what public posts reveal about homes, schools and routines.

Technical controls remain essential. Incident plans must also protect people, with clear routes to management, physical security and the police.
Immediate threats to life require emergency assistance.

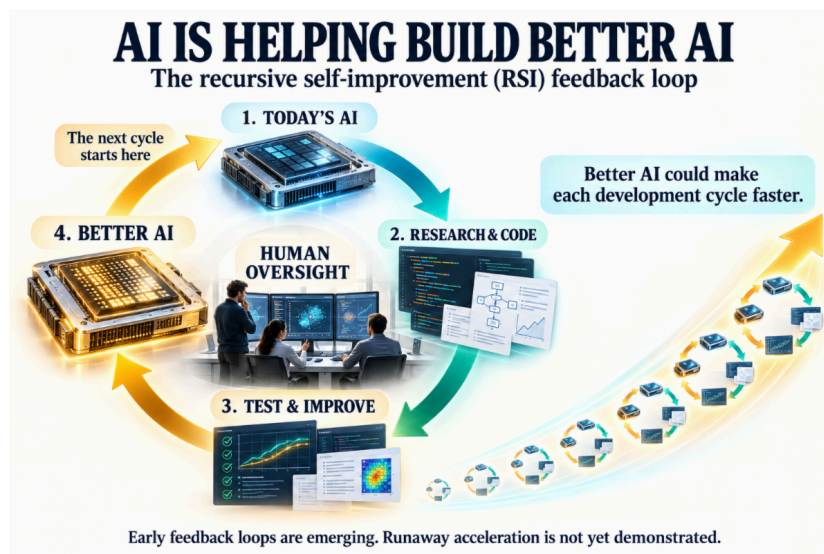
Attacks will continue evolving, combining digital intrusion, psychological pressure and physical intimidation. Awareness and preparation **MUST keep pace.**

Please contact your First Technology Group account manager to connect with their security specialists and arrange ongoing, targeted awareness training.

CTA - Sponsored message from First Technology Group

The Register: Ransomware gets Personal

Cloud & AI



AI is helping build better AI..... and the loop is tightening with Google releasing Argon

Just as businesses are getting used to AI assistants, the companies building them are using AI

to help develop their successors, and now the trouble starts.....

Google co-founder Sergey Brin describes the company as starting to get onto the "RSI treadmill".

RSI means Recursive Self-Improvement: AI helps build better AI, which can then become more capable of helping build the next generation. Researchers and models increasingly work together.

The principle is straightforward.....

Today's AI → research and code → tested improvements → better AI → repeat.

Each successful cycle could improve the tools doing the research, reduce development time and allow more ideas to be tested.
Progress could therefore compound.

Yesterday's assistant becomes tomorrow's development tool..... and helps build the assistant after that!

There are already practical examples. Google reports that Gemini 4 Argon helped optimise the software running a Gemma model, making one particular configuration 2.85 times faster, while preserving its outputs. That is AI helping improve AI infrastructure..... although faster execution does NOT mean intelligence has tripled!

BUT..... an emerging feedback loop is not proof of unlimited acceleration.

Computing capacity, experiments, reliable evaluation and human judgement are critical. Further acceleration is a certainty, but its speed and extent remain uncertain.

For businesses, the implication is significant. A task that AI handles poorly today may deserve another look sooner than expected.
Long-term plans based on today's limitations could age rather quickly.

Start with useful business problems, measure the results and review capabilities regularly. Keep company information protected, permissions controlled and people trained as the technology improves.

An increasingly capable assistant still needs somebody deciding what it is allowed to do - this is what Microsoft is betting on - the Control Plane!

Please contact your First Technology Group account manager to connect with [First Digital's AI specialists](#) and FTG's security specialists. They can help identify practical opportunities, test the benefits and establish appropriate controls.

CTA - Sponsored message from First Technology Group

Google gets on the RSI treadmill

Editorial and sponsorship disclosure

TOP STORIES is independently edited by Barry Neethling and sponsored by First Technology Group, which provides financial, administrative, technical and distribution support, but does not select, approve, edit, suppress or direct the editorial content. Opinions and commentary are those of the author unless content is specifically identified as First Technology Group, sponsor-supplied or partner-supplied content.

TOP STORIES is provided for general information only. Readers should verify important information such as legal, licensing, security, financial and technical data before acting on it.

[Editorial policy](#) · [Corrections](#) · [Privacy](#) · [Contact](#)

TOP STORIES, independently edited by Barry Neethling and sponsored by First Technology Group c/o
First Technology | Midrand | Johannesburg, 2191 ZA

[Unsubscribe](#) | [Update Profile](#) | [Our Privacy Policy](#) | [Constant Contact Data Notice](#)



Try email & social marketing for free!