WIRED for the FUTURE

MAY 2025

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

Are cloud security concerns **slowing you down**

Ever feel like you could do more with the cloud? You should - it makes work easier, boosts productivity, and unlocks smart tech like AI. But one big thing holds businesses back: Security concerns.

New research shows over 90% of businesses are planning big cloud changes in the next two years, with many driven by AI. But instead of going all-in on public cloud, nearly 70% are considering shifting at least part of their workloads back to private cloud or on-premises servers.

Not sure what the cloud does? Let's rewind...

The cloud is an online space for storing data, running applications, and accessing files from anywhere, reducing the need for bulky in-house servers. Here are the different types:

Public cloud – The most common setup, where businesses rent space from big providers like Amazon Web Services (AWS) or Microsoft Azure.

Private cloud – Dedicated just to your business, either hosted by a provider or managed in-house.

Hybrid cloud – A mix of public and private cloud.

On-premises – The traditional method, where businesses keep their own in-house servers.

With cyber threats getting smarter, many businesses have concerns over security in the public cloud. That's why hybrid cloud is becoming popular - it balances flexibility, security, and cost.

Things to consider if you're thinking about making changes:

- What kind of data do you store? If it's highly sensitive data (like customer details or financial records), a hybrid or private cloud setup could give you more control.
- Are your current systems cloud-ready? Some older software doesn't play nicely with the cloud. A hybrid approach lets you modernize without everything breaking down.
- How strong is your security? No matter what cloud setup you choose, you still need good security practices. Think strong passwords, multi-factor authentication, and regular security check-ups.

If you're not sure which approach is right for your business, now's the time to ask. A solid cloud strategy can save you money, boost security, and help you make the most of AI.

Need some advice?
We can help, get in touch.

DID YOU KNOW...

Call quality is about to improve in Teams

Microsoft Teams is introducing an AI-powered "Super Resolution" feature designed to improve video call quality.

This technology makes low-resolution, poor-quality video streams better, providing sharper visuals during meetings. It's especially great for anyone with a slower internet connection, as it upscales video in real-time to give a better viewing experience.

One thing to note: It's only available if you're using a Copilot+ PC, and because of the battery it uses, it only works when you're plugged into power.

5 Reasons to be wary of AI

Artificial intelligence (AI) is an incredible tool. It's revolutionizing industries, advancing medical research, and making businesses more productive. But like any powerful technology, it can also be used for the wrong reasons – and it's important you're aware of it.

Cyber criminals have discovered that generative AI (the same kind of AI that powers tools like ChatGPT and Copilot) makes their scams faster, smarter, and more convincing than ever...

1. AI-generated malware
Malware (malicious software) isn't new, but AI has made it quicker to produce, harder to detect, and more effective at bypassing security measures. Cyber criminals use AI to write malware that looks like legitimate browser extensions, software downloads, and even innocent-looking files like PDFs or images.

Stay safe: Keep your security software up to date and never download software or browser extensions from unknown sources.

2. Fooling security systems
Most cyber security software works by spotting known malware patterns. By slightly tweaking existing malware, scammers can create thousands of unique versions that security systems don't recognize.

Stay safe: Regularly update your security software to keep up with evolving threats. AI-powered security tools can also help to detect suspicious activity.

3. AI-powered password cracking
Cyber criminals are now using AI to break into accounts faster than ever. AI can test millions of password combinations per second, analyze leaked passwords, and even predict passwords based on common patterns.

Stay safe: Use strong, unique passwords for every account and enable multi-factor authentication (MFA) to add an extra layer of security.

4. Smarter phishing scams
Phishing emails used to be easy to spot – bad grammar, weird phrasing, and suspicious links were all giveaways. But with AI, scammers can create perfectly written, highly personalized messages that look exactly like they came from a trusted colleague or supplier.

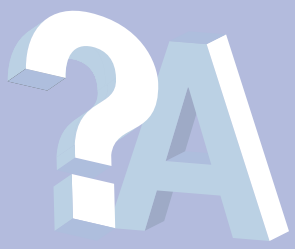
Stay safe: Always verify unexpected emails, especially if they request payments, login details, or sensitive information. Hover over links before clicking and double-check sender addresses.

5. Deepfake impersonation
Imagine getting a video call from your CEO asking you to process an urgent payment. You recognize their voice and face... but it's not actually them. AI-generated deepfakes can clone voices and faces to trick employees into transferring money or sharing sensitive data.

Stay safe: If something seems unusual or too urgent, verify the request by calling on a known number or confirming in person.

AI-powered scams are evolving fast, but you don't have to be an easy target. A strong security culture, smart policies, and the right tools can help keep your business safe.

If you're not sure whether your cyber security is up to scratch, we can help with a security audit. Get in touch.



Q: What's the best way to back up my business data?

A: Use the 3-2-1 rule: Make three copies of your data, across two different media types, with one offsite backup. (We can help you set this up.)

Q: What's the biggest cyber security mistake small businesses make?

A: Things like ignoring software updates and using (or reusing) weak passwords. It usually comes down to employees needing better and more frequent security awareness training.

Q: How can I tell if my data is secure?

A: Running regular security audits, encrypting data, and enforcing strong access controls will help - as will working with a trusted support partner who can monitor your systems.

NEW TO MICROSOFT

Try this new and improved Teams calendar

Microsoft Teams has a new and improved calendar that works better with Outlook and makes scheduling easier than ever.

You can now manage someone else's calendar, see multiple time zones, and get a better monthly view of your schedule. Plus, Copilot and Places bring smarter booking and workplace features right into Teams.

Want to try it out? Just go to the Calendar app in Teams and turn on "New Calendar" in the top-right corner. If you don't like it, you can switch back any time.

This is how you can get in touch with us:
CALL: 416.572.3805 | **EMAIL:** info@wiredforthefuture.com
WEBSITE: wiredforthefuture.com

WIRED for the FUTURE