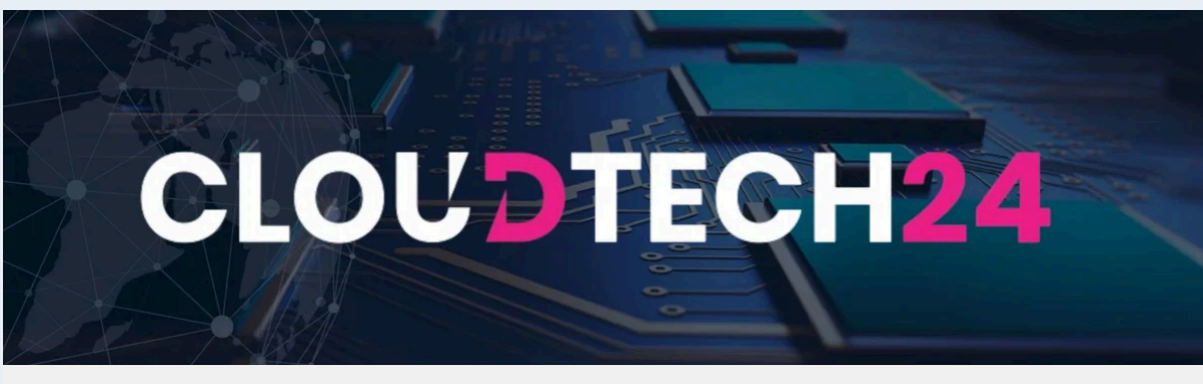




Morning ,

Each month, we take a look at a key cybersecurity trend and what this means for your organisation.

AI governance and the rise of shadow AI

Artificial Intelligence is transforming the way organisations work, helping employees improve productivity, automate tasks and make faster decisions. However, as AI adoption accelerates, businesses are facing a growing challenge: Shadow AI.

Shadow AI refers to employees using AI tools that have not been approved, monitored or governed by the organisation. Often adopted with good intentions, such as saving time, these tools can expose sensitive data, create compliance risks and reduce visibility over how business information is being processed. This is where AI governance becomes essential. Organisations that establish strong governance frameworks today will reduce risk and be better positioned to benefit from AI's potential tomorrow.



Top Tip - Create an AI policy

A clear AI policy is now a fundamental component of modern governance.

The goal isn't to stop people using AI. It's to ensure they use it safely, responsibly and within a governance framework that protects your organisation and its data. The policy should include key elements, such as approved AI tools, acceptable and prohibited use, data protection and confidentiality, human oversight, and employee responsibilities.

Need help with AI governance?

Contact us



Common AI mistakes to avoid

- Banning AI instead of governing it** - Attempting to block AI tools completely can result in employees using AI independently, creating 'Shadow AI' outside the visibility and governance of your IT and security teams.
- Allowing employees to upload sensitive data** - One of the biggest risks is employees entering confidential company data into public AI tools without understanding where the data is stored or processed.
- Not defining approved AI tools** - If employees aren't provided with secure, approved AI tools, they are more likely to adopt consumer AI platforms independently. Providing approved tools helps balance innovation with security.
- Failing to maintain human oversight** - AI-generated content can be inaccurate, biased or incomplete. Relying on AI outputs without human review can lead to poor decisions, compliance issues or reputational damage.

Important security advisory - Steep rise in 'ClickFix' style phishing attacks

This is where users are redirected to a fake verification page that impersonates a trusted service such as Cloudflare or Google reCAPTCHA and tricks users into infecting their own devices.

CLICK HERE for more information and advice



Exciting partnership with NinjaOne

Leading technology backed by our expert 24/7 monitoring, management and support.

Our clients rely on us to provide technology solutions we genuinely trust and we're highly selective about the vendors we choose to work with.

Over the past 18 months, we've thoroughly evaluated NinjaOne's platform in real-world environments, assessed the quality of their solutions, support, product innovation, and account management, and confirmed that they share our customer-first approach and commitment to excellence.

We look forward to a successful partnership and delivering even greater value to our clients.



Celebrating our 10th anniversary!

A major milestone for CloudTech24

Over the past decade, we've grown into a trusted managed IT and cybersecurity partner supporting more than 250 organisations in the UK and beyond.

Huge thanks to our customers, partners and team members who have been part of our journey. Here's to the next decade!

Customer update - Microsoft move to phishing resistant authentication

Microsoft is continuing to move organisations towards a more secure, passwordless sign-in experience. To help customers prepare, CloudTech24 will be using Microsoft's Registration Campaign to ensure all users have Multi-Factor Authentication (MFA) configured through Microsoft Authenticator.

Once Microsoft Authenticator is in place, users will then be prompted to complete the setup for Passkey / Passwordless sign-in. **This will be enforced from 15 September 2026.**

CLICK HERE for our step-by-step PDF guide

Last Month's Security Monitoring Stats

695

Real world security events handled by our team

2,426

Phishing emails caught and remediated

1.6m

Vulnerabilities remediated by CT24 specialists

CloudTech24, 36-37, Albert Embankment, London SE1 7TL, United Kingdom

[Unsubscribe](#) [Manage preferences](#)