

STRENGTHENING SECURITY ACROSS OUR CLIENT ENVIRONMENTS

Update from our Chief Security Officer, Rob Brewer: We are rolling out a standard set of baseline security controls across all managed client environments to strengthen protection against modern cyber threats and reduce risk.

These controls are designed to create a secure-by-default environment, improving how identities, email, and collaboration tools are protected - without adding unnecessary complexity for users. By enforcing stronger authentication, limiting high-risk actions, and enabling enhanced monitoring, we significantly reduce exposure to common threats such as phishing, credential compromise, and unauthorised access.

The approach focuses on **three key outcomes**:

- **Stronger protection** against evolving cyber threats
- **Reduced attack surface**, limiting opportunities for misuse or data exposure
- **Improved visibility and response**, enabling quicker detection and remediation of suspicious activity

While most changes have minimal impact to users, together they deliver a meaningful uplift in security posture and help ensure your environments remain resilient, compliant, and aligned with best practice.

[Email us for more information](#)

KEY CYBERSECURITY TREND

AI-driven cyber attacks



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

AI is the biggest driver of change in cybersecurity. Attackers use AI to automate phishing, exploit vulnerabilities faster and create adaptive malware. AI can analyse public and stolen data to craft **highly realistic, tailored attacks**, which means they have a much **higher success rate**. AI-powered attacks can also learn from failed attempts and adjust in real time, using polymorphic malware that **changes to evade detection**.

Key impact

- **Faster and more frequent attacks** mean traditional security response models struggle to keep up
- **Huge increase in attacks** as there is a lower barrier to entry for cybercrime. Almost 90% of organisations have been the target of AI-powered cyberattacks over the last 12 months.
- **Regulatory and compliance exposure**, as AI-related breaches often involve personal data leakage, AI misuse or governance failures.

Priorities for action

- **Adopt AI-powered security tools** - for real-time threat detection, behavioural analytics and automated response
- **Shift from reactive to proactive security** - continuous monitoring, predictive threat modelling and automated patching and response
- **Implement Zero Trust architecture** – continuous authentication and least-privilege access
- **Secure AI use internally** and improve employee training.

If you want to discuss the implications for your organisation, simply book a discovery call at a time that suits you.

[Book a Discovery Call](#)

THIS MONTH'S QUICK WIN



Check if your domain is protected

We all need to protect our organisations from email-based threats. To do this your email configuration needs to be setup correctly, authenticated and DMARC-compliant. If left unprotected, your domain has little defence against spoofing and impersonation attacks, leading to reputational damage.

[Analyse your domain for FREE with CloudTech24 - CLICK HERE](#)

DOMAIN SECURITY - FAQs



How do I secure my domain?

There are a number of ways to secure your domain, including authentication using SPF records and DKIM. Whilst these go some way to securing your domain, it's better to have a managed service to know that your protection is configured correctly and it is being proactively monitored.

What is included in advanced domain security?

CloudTech24's service incorporates hosted DMARC analysis, hosted DKIM, SPF, BIMI and MTA-STS and TLS-RPT. It integrates seamlessly with existing systems and includes: expert support, compliance assurance and 24/7 management and reporting for proactive threat management.

What are the benefits of advanced domain security?

Advanced domain security will help you to safeguard your staff, prevent spoofing attacks, and strengthen your overall cybersecurity posture. The service ensures legitimate emails reach intended recipients, safeguards your domain's reputation by preventing misuse and aligns with global email authentication standards and regulations.

[CLICK HERE for more information on domain security](#)