waystone | Compliance Solutions

MAS Advisory on AI-Driven Threats: Implications for Financial Institutions

Nithi Genesan May 5, 2026

As advanced AI systems gain the ability to autonomously discover and exploit vulnerabilities, MAS is urging financial institutions to strengthen their cyber resilience before these threats scale.

Background

17 April 2026 – The Monetary Authority of Singapore (MAS) issued an advisory to all Financial Institutions (FIs) following the emergence of frontier AI models capable of autonomously identifying and exploiting security vulnerabilities.

The advisory was prompted by two major developments – Anthropic's launch of Claude Mythos, a frontier model with autonomous vulnerability discovery capabilities released under restricted access, and OpenAI's release of GPT-5.4-Cyber, fine-tuned for defensive cybersecurity work. MAS notes that similar models from other providers are expected to follow, and access may not remain restricted.

To strengthen situational awareness, MAS emphasises that these advancements mark a new phase in AI-enabled cyber risk, requiring heightened vigilance and accelerated defensive readiness across the financial sector.

Key Risks

Frontier AI models represent a fundamental shift in the cyber threat landscape. Unlike previous generations, these models can autonomously probe systems for weaknesses – through source code analysis, web application testing, binary analysis, and protocol fuzzing – and move to exploitation with little human intervention.

When these capabilities become more widely available, the risk of misuse by malicious actors increases significantly – enabling attacks that are faster, more adaptive, and more automated than anything seen before. The shrinking window between vulnerability discovery and exploitation means that a reactive cybersecurity posture is no longer sufficient. FIs must shift to a proactive model, anticipating and defending against AI-driven threats before they materialise.

MAS highlights that AI-accelerated attacks may outpace traditional detection and response cycles, making continuous monitoring, rapid patching, and predictive threat modelling essential components of modern cyber resilience.

Recommended Measures

Given the speed and sophistication of emerging AI-driven cyber threats, MAS is urging financial institutions to adopt a more proactive and adaptive security posture. The following measures highlight key actions FIs should take to safeguard systems, enhance operational resilience, and prepare for the next wave of AI-enabled exploitation.

1. Validate basic cyber hygiene – FIs should ensure fundamental cyber security controls are in place. These may include MFA for privileged accounts, timely patching, malware protection, system hardening, and network segmentation — are consistently in place and regularly tested for effectiveness.

2. Vulnerability assessment and patch management – FIs should assess their current vulnerability and patch management policies and determine whether they are equipped to keep pace with the speed at which AI can now identify and exploit weaknesses.

Where patches are unavailable or cannot be deployed immediately, compensating controls – such as virtual patching – should be considered as a temporary measure to limit exposure while permanent fixes are planned and put in place.

3. Resilience for systems and cyber resources – Operational resilience must extend beyond systems. Immutable backups and regularly tested recovery procedures remain critical and FIs should also assess whether their cybersecurity teams can scale to meet AI-driven threat volumes.

4. Leverage AI for cybersecurity defence – AI can be a powerful defensive tool when adopted responsibly. FIs should explore integrating AI across risk assessment, threat modelling, secure development, penetration testing, and incident response – embedding it early in the system lifecycle in line with security-by-design principles.

5. Strengthen industry collaboration – Staying actively engaged with trusted information-sharing networks enables faster detection and containment through the timely exchange of threat intelligence, including emerging AI-driven attack patterns and supply chain risks.

6. Monitor AI model developments – The threat landscape will continue to evolve as AI capabilities advance. FIs should track relevant developments, access defensive AI offerings where appropriate, and stay current with guidance from regulators, industry bodies, and cybersecurity communities.

As frontier AI capabilities continue to advance, financial institutions will face increasingly sophisticated and automated cyber threats. MAS' advisory reinforces the importance of moving beyond reactive security and adopting a proactive, intelligence-driven approach. Strengthening foundational controls, accelerating detection and response, and integrating AI responsibly into defence strategies will help institutions maintain resilience and safeguard critical operations in a rapidly evolving threat environment.

How can Waystone help?

Waystone's APAC Compliance Solutions team supports financial institutions in navigating the evolving regulatory expectations surrounding AI-enabled cyber risks. Our specialists help firms interpret MAS' latest advisory, assess the implications for their existing cybersecurity and operational-resilience frameworks, and implement enhancements that align with supervisory expectations.

If you would like to discuss how this advisory applies to your institution or explore how we can support your compliance programme, please reach out to your usual Waystone representative or contact our team using the link below:

Contact us →