# Government urged to adopt proactive cybersecurity against AI-driven threats



Government institutions are being urged to adopt a fundamentally different approach to cybersecurity in response to increasingly sophisticated cyber threats, which are now leveraging artificial intelligence (AI) to evolve rapidly. Traditional reactive measures, which respond only after threats become apparent, are considered inadequate to address the speed and complexity of contemporary cyber attacks.

Dominic Cheah, the Director of Technical Solutions Engineering, ASEAN at Tanium, highlights the need for a paradigm shift towards more proactive, continuous, and comprehensive security strategies. Tanium’s Autonomous Endpoint Management (AEM) platform is designed to meet these evolving requirements by providing real-time visibility and automation capabilities that significantly enhance government cybersecurity postures.

One of the key shifts discussed is moving from a reactive to a proactive endpoint security stance. Historically, government cybersecurity responses have been largely reactive, but this approach leaves critical vulnerabilities exposed. The Singapore Government’s Chief Information Security Officer, Justiin Ang, underscored this transformation as one of three strategic changes in the nation’s cybersecurity posture, advocating for increased automation and proactive security initiatives.

The Tanium AEM platform incorporates automated workflows such as Adaptive Actions, which allow security teams to deploy remediation efforts swiftly and at scale based on pre-set criteria. This not only reduces the risk of human error but also ensures non-compliance issues are promptly addressed without impeding government operations. The platform manages endpoint security throughout the device lifecycle—from onboarding to retirement—through automated security agent deployment, continuous monitoring, policy enforcement, and timely vulnerability patching, thereby decreasing the overall attack surface.

Real-time visibility is a central feature of the Tanium system, providing accurate, high-fidelity data from every endpoint. This capability enables security teams to detect and mitigate threats early, preventing escalation. Continuous monitoring ensures that government institutions maintain a comprehensive view of their IT environments at all times.

Another critical shift emphasised is the move from periodic to continuous security posture assessments. Traditional assessments, conducted at intervals, create security gaps potentially exploitable by adversaries. Continuous assessment models, supported by Tanium’s platform, enable constant evaluation and improvement of security status.

The Confidence Score feature within Tanium AEM offers administrators insights into the safety and effectiveness of deploying updates or patches by analysing real-world data from millions of endpoints globally. Additionally, Remediation Visibility consolidates vulnerability data with patch management workflows, enhancing collaboration between IT operations and security teams to prioritise and resolve critical vulnerabilities swiftly.

Justiin Ang also pointed to the importance of integrating zero-trust architecture and multi-layered security approaches to continuously verify all users and systems. He emphasised that these approaches must be supported by comprehensive monitoring and rapid response capabilities to maintain robust defence systems.

Furthermore, government institutions are encouraged to transcend mere compliance with security checklists and adopt dynamic, adaptive security strategies. Tanium AEM aids this evolution through automation playbooks—standardised, real-time guided procedures for routine tasks and troubleshooting—which ensure remediation efforts are consistently applied and responsive to ongoing conditions.

Beyond this, Tanium’s platform integrates with tools such as ServiceNow to maintain accurate, real-time configuration management databases (CMDBs), thereby improving the effectiveness of compliance efforts. These integrations reduce manual workloads and streamline processes, making security compliance both efficient and actionable. Continuous access to up-to-date compliance metrics allows organisations to swiftly adjust to new regulations or standards.

In summary, Tanium’s Autonomous Endpoint Management platform supports governments in adopting a proactive, continuous, and comprehensive cyber defence posture. By shifting away from reactive measures towards automation-driven real-time visibility and continuous assessments, government institutions can better anticipate, detect, and respond to cyber threats. This approach equips security teams with the agility and insight necessary to safeguard critical government systems in an increasingly complex threat landscape.

Dominic Cheah brings over two decades of cybersecurity expertise across multiple sectors, including finance, aviation, and multinational corporations, with extensive experience designing scalable security architectures for large enterprises and government organisations managing hundreds of thousands of endpoints.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://news.microsoft.com/en-cee/2025/01/28/governments-face-unprecedented-cyber-threats-ai-emerges-as-the-ultimate-defense-to-cybercrime/> - This article supports the claim that governments are facing increasingly sophisticated cyber threats and highlights the role of AI in transforming cybersecurity strategies. It emphasizes the importance of proactive measures over traditional reactive approaches.
2. <https://www.cisa.gov/ai> - CISA's initiative to use AI for strengthening cyber defense aligns with the need for government institutions to adopt more proactive and advanced cybersecurity strategies, especially in managing critical infrastructure.
3. <https://www.keepersecurity.com/blog/2024/12/10/how-governments-can-mitigate-ai-powered-cyber-threats/> - This resource discusses the rise of AI-powered cyber threats and the strategies governments can use to mitigate these risks, emphasizing the need for advanced AI security solutions in government cybersecurity.
4. <https://bigid.com/blog/ai-security-for-government-agencies/> - The article highlights the importance of AI in government cybersecurity for proactive threat detection and response. It underscores the integration of AI with traditional measures to enhance defense against sophisticated threats.
5. <https://fedscoop.com/why-ai-will-be-instrumental-in-advancing-government-cybersecurity/> - This report emphasizes AI's pivotal role in reshaping government cybersecurity to combat evolving threats, supporting the shift towards more proactive and comprehensive security strategies.
6. <https://www.tanium.com/products/autonomous-endpoint-management/> - Tanium's Autonomous Endpoint Management platform supports the article's discussion on shifting from reactive to proactive endpoint security strategies through real-time visibility and automation, which is crucial for modern government cybersecurity.
7. <https://news.google.com/rss/articles/CBMimgFBVV95cUxQbXI5cG5YNFhVMHljYmxBNkdiZGJwejhUaHVCYnFBNDNvbDNocm9qcTNpV1RBSERqdVVEQmFCQzdodlQzOWV1SUl5RmI3dEMxdXlzOExneFItM20yUTVkSlN5S0Q1eU5MLVltcnpjZHlrS3BiX1pySndHdlZOTkRFVi15Qm8ybGhwMzdvMW9GYjU3b18yQi02N2VR?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data