FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

From Hype to Resilience: How Kaspersky Is Guiding APAC Through AI-Driven Cyber Risk

Adrian Hia
Managing Director for Asia Pacific Japan (APJ) at Kaspersky
in conversation with
Kenny Yeo
Director at Frost & Sullivan

Building Cyber-ready Enterprises in a Digital-first World

As AI transforms boardrooms and digital strategies, cybersecurity can no longer be an afterthought. In this exclusive Transformational Growth Leadership interview, Adrian Hia, Managing Director for Asia Pacific Japan (APJ) at Kaspersky, joins Frost & Sullivan's Kenny Yeo to discuss how enterprises can harness AI safely, address talent shortages, manage IT/OT complexity, and implement practical steps to build true cyber resilience.

Why AI Transformation Matters Now

Kenny Yeo: *Why is AI transformation so important today, especially with security blind spots around privacy and protection?*

Adrian Hia: From a business standpoint, AI is no longer optional, and organizations must learn to harness it. AI helps improve lives, supports smarter and timelier decisions, and strengthens business performance. At Kaspersky, we already rely heavily on AI for malware analysis and filtering false positives. But it's important to remember that while AI is a powerful tool for defenders, it is also a tool for cybercriminals. That dual nature makes strong cybersecurity indispensable when embracing AI.

Solving the Cybersecurity Skills Shortage in APAC

Kenny Yeo: *Is the shortage of skilled cybersecurity professionals as severe as it seems?*

Adrian Hia: Yes, the shortage is very real. Across Asia, many universities are only just starting to introduce cybersecurity modules into their computing programs. While tens of millions of graduates are emerging with strong programming skills, it will likely take another four to five years before we see enough trained cybersecurity professionals.

In the meantime, organizations must make do with existing talent by retraining and cross-training staff. A network engineer, for example, could be upskilled into a cybersecurity engineer, or those managing endpoints could be trained in cyber defense. This deliberate investment in retraining is the most practical stopgap measure until the talent pipeline matures.

Reducing IT/OT Complexity for Stronger Cyber Defenses

Kenny Yeo: *The second major issue we hear from enterprises is complexity. Organizations are juggling multiple IT systems: cloud, on premises, hybrid, and a patchwork of cybersecurity tools, creating an overwhelming environment. What are your customers telling you when you discuss this issue of complexity?*

Adrian Hia: Many customer environments today are fragmented. Some enterprises rely on 40 or 50 cybersecurity vendors, while others manage 100 or even 200 solutions. This grew out of rapid digitization, where CISOs and CIOs had little time to build mature frameworks before the next wave arrived, so they bought point solutions to fix immediate problems, adding layers of complexity.

The picture is improving. Many organizations are becoming more self-aware, and new roles such as chief risk officers, heads of perimeter security, and incident response leaders are helping streamline cybersecurity. On the vendor side, consolidation is reducing fragmentation through mergers, acquisitions, and integrated platforms. At Kaspersky, we have introduced an open Extended Detection and Response (XDR) platform that unifies IT and OT threat intelligence in one place to help reduce complexity.

True resilience still requires balance. Regulators often require multi-tier, multi-vendor firewalls to mitigate supply chain risk. Simplification matters but relying on a single provider is not the answer. The right mix depends on each organization's goals and risk appetite.

I would say, start by redefining the endpoint. It's not just PCs and phones; think IP cameras, vehicles, and industrial controllers. Build strong "first-point protection" at the endpoint, then extend visibility across network and cloud with Network Detection and Response (NDR) and Network Traffic Analyzers (NTA) in both IT and OT. Kaspersky's open XDR is designed to give CISOs a unified asset view across corporate IT and industrial environments because attacks can originate from either side.

Seeing Your Organization Through the Eyes of a Cyber Attacker

Kenny Yeo: *Another area we often hear about is external visibility. Many companies still don't look at themselves through the eyes of an attacker. Why is this a blind spot, and how should organizations address it?*

Adrian Hia: In a geopolitically fractured world with reduced information sharing, threat intelligence (TI) is essential. Prevention beats cure. Kaspersky's global research teams monitor Advanced Persistent Threats (APTs) and criminal ecosystems like dark-web chatter, closed-forum signals, leaked credentials for sale. We have been able to warn clients 1–2 weeks ahead of incidents, giving time to prepare. You won't stop everything but blocking 80–90% of attempts dramatically lowers risk. Just as Business Intelligence (BI) shaped strategy for decades, TI should guide cybersecurity decisions.

> "Technology comes after awareness, training, and rehearsals. Align the top team first and then build." — Adrian Hia

The First Step Every Organization Can Take Toward Cyber Resilience

Kenny Yeo: *What's the single most important step for organizations at any maturity level?*

Adrian Hia: The first step is awareness at the board and C level. Many executives who drive digital transformation and approve budgets still lack a deep understanding of cybersecurity. That is why we developed Kaspersky's Keeps Program, a gamified tabletop exercise that engages leadership teams in crisis simulations and helps CEOs, CFOs, and CHROs understand their roles when a cyber incident occurs. CISOs often struggle to gain board level attention because they are not part of the executive table, and investments are prioritized for business growth. Raising awareness at the top changes that dynamic. Once leaders are aligned, organizations should run regular cyber drills, just like fire drills. Awareness, training, and rehearsals create resilience, and technology can then be layered on this foundation to strengthen defenses.

Final Thoughts: A Human-centered Path to Cyber Resilience

This roadmap isn't technology-first. It starts with people and process: elevate leadership awareness, institutionalize drills, and then integrate platforms to tame complexity and close visibility gaps across IT and OT. In the era of AI, that's how resilience is built deliberately and from the top down.

Adrian Hia | Managing Director for Asia Pacific Japan (APJ) at Kaspersky

Adrian Hia serves as Managing Director for APJ at Kaspersky, where he leads regional business with a strategic approach that aligns sales, marketing, and partnerships. He has built robust teams across ASEAN, Hong Kong, and Taiwan to strengthen the company's regional impact and results. With a core focus on digital transformation and cybersecurity, Adrian's expertise spans product marketing and key account management. His mission at Kaspersky is to help fortify the digital landscape, making it a safer space for both businesses and individuals.

Alejandra Parra | Research Analyst, Frost & Sullivan

Kenny Yeo is Director, ICT and Head of the Asia Pacific Cyber Security Practice at Frost & Sullivan, based in Singapore. With 20 years across research, consulting, advisory, team leadership, and business development, he focuses on how cybersecurity enables enterprise digital transformation and secure DX outcomes. His expertise spans cybersecurity, IoT, smart retail, industrial, and e-government.

Join the Movement: Build Cyber Resilience with Frost & Sullivan

At Frost & Sullivan, we help leadership teams operationalize resilience linking AI-driven transformation to pragmatic cybersecurity outcomes.

Next steps on your growth journey:

- Book a Growth Strategy Session – Align your cybersecurity transformation strategy with Frost & Sullivan's proven frameworks for success.
- Engage with Growth Experts – Collaborate with our growth coaches to discover tailored solutions that address your organization's unique challenges.
- Join the Growth Council – Become part of an exclusive network of forward-thinking cybersecurity experts and innovators shaping the future of the industry
- Explore New Growth Opportunities – Identify partnerships and technologies that simplify stacks while enhancing protection.

Annexure: Essentials for Leaders Closing the Cyber Gap

To deepen your understanding of the themes discussed, Frost & Sullivan has curated the following analyses that highlight growth opportunities, strategic imperatives, and technological advancements across the cybersecurity landscape They provide critical insights for strengthening threat resilience, accelerating innovation, and enabling secure digital transformation:

- Data Security Posture Management Market
- External Attack Surface Management Sector
- Global Surveillance Solutions Growth Opportunities
- Extended Detection and Response (XDR) Industry
- Cloud-native Application Protection Platform (CNAPP) Market

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN