December 2025
Infographic
Sponsored by Lumen

The AI Security Shift: Fuelling the Next Stage of Cybermodernisation

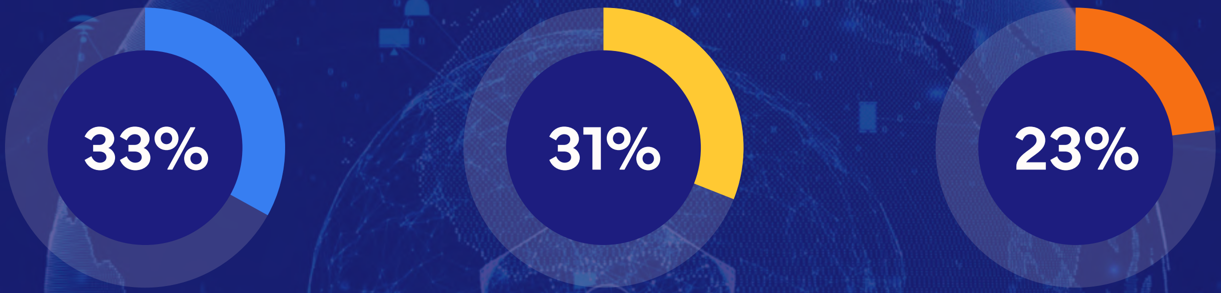
Sakshi Grover
Senior Research Manager
Cybersecurity Services,
IDC Asia/Pacific

Yih Khai Wong
Senior Research Manager
Cybersecurity Services,
IDC Asia/Pacific

Securing the future

Aligning cybersecurity and modernisation priorities ensures defences evolve with technology, safeguarding business continuity and trust.

Asia/Pacific enterprises' top 3 security investment priorities



33% Cloud-native application protection (CNAPP and cloud SecOps)

31% Managed security services (MSS/MDR)

23% Endpoint security (includes EDR, EPP, XDR, ATP)

Source: IDC's Asia/Pacific Security Study, 2025

Path to resilience: Where modernisation objectives meet security

Modernisation objectives

- → Consolidation and unified security management
- → Compliance with evolving global and regional regulations
- → Reduce incident frequency and business impact
- → Increase transparency and better security controls
- → Build cyber-resilience and ensure business continuity

Source: IDC's Asia/Pacific Security Study, 2025

Top modernisation priorities for Asia/Pacific enterprises

51%
Cloud security

45%
Identity and access management

42%
Data protection and recovery

39%
Improving IT/OT security

34%
Governance, risk, and compliance

The AI Security Shift: Fuelling the Next Stage of Cybermodernisation

December 2025 | #AP242545IG | Sponsored by Lumen

IDC

Critical imperatives towards a trusted and resilient cybersecurity strategy

Asia/Pacific enterprises’ top 3 resiliency strategies

35%

Implementation of redundancy mechanisms

- ✓ Prevent incidence for single-point-of-failure
- ✓ Undisrupted availability and strengthen business continuity
- ✓ Enhanced incident response and recovery time

34%

Automated breach isolation and containment systems for rapid incident control

- ✓ Ensure consistent deployment of security policies
- ✓ Reduce analysis paralysis, shortening breach dwell time
- ✓ Compliance with regulatory frameworks

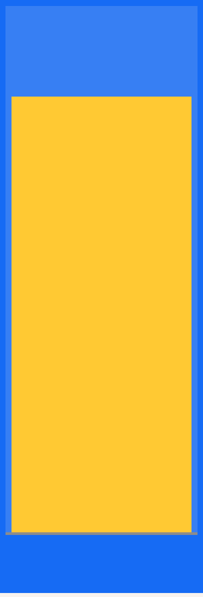
23%

Secure data protection protocols

- ✓ Ensure data governance, integrity, and confidentiality
- ✓ Gain customer and stakeholder trust
- ✓ Enhance data recovery capabilities

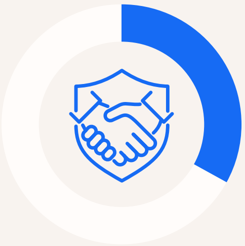
Source: IDC’s Asia/Pacific Security Study, 2025

The race to modernise resilient security



83%

of Asia/Pacific enterprises are looking to partner with service providers to deliver their top security investment priorities



33%

of Asia/Pacific enterprises are adopting a unified security platform approach and rely on MSSPs to fill talent gaps

Managed security service providers (MSSPs) help enterprises translate operational metrics into business-level ROI indicators, enabling CISOs to build stronger, data-driven business cases for board approval.

As security investments grow, enterprises shift their focus from building defences to ensuring resilience, turning to trusted service providers to guide, operationalise, and scale strategies.

Source: IDC's Asia/Pacific Security Study, 2025

The CISO's guide to organisational resilience

Four stages of enterprise security maturity

Stage 1:

Adopt

- Foundational monitoring and alerting
- Basic threat detection and response capabilities
- Foundational security architecture and compliance framework

Stage 2:

Integrate

- Consistent security monitoring across different environments
- Proactive threat hunting and vulnerability management
- Secure-by-design principles, security embedded into systems and applications

Stage 3:

Scale

- Scale MDR capabilities across different locations
- Leverage security analytics and automation for threat management
- Security investments happen at scale, not in silos

Stage 4:

Optimise

- Continuous monitoring using AI-driven threat intelligence and predictive analytics
- 24 x 7 next-gen security operations centre (SOC) capabilities
- Security priorities discussed at board level

Source: IDC, 2025

Tool sprawl adds integration complexity

Reducing tool sprawl and integration complexity is critical as enterprises advance through security maturity stages.

How many tools does the average enterprise have to manage?

30–35

tools across cybersecurity and data protection, underscoring the growing **complexity of tool sprawl and integration challenges.**

What percentage of Asia/Pacific enterprises have these tools deployed in hybrid environments?

53%

Data protection tools

35% cloud-native	**12%** on-premises

48%

Cybersecurity tools

39% cloud-native	**14%** on-premises

Source: IDC's Asia/Pacific Security Study, 2025

Defining the shift from hybrid chaos to unified intelligence

The journey towards unified and intelligent security platforms

Stage	Approach	Integration level	Outcome
1 Fragmented	Best-of-breed tools, low integration	Siloed visibility	Duplication, alert fatigue
2 Coordinated	Best-of-breed with moderate/high integration	Shared workflows and partial data exchange	Improved response efficiency
3 Unified	Single platform with moderate integration	Centralised policies, common controls	Simplified management, lower risk
4 **Intelligent platform (Target state)**	Unified or hybrid with **high integration**	Full visibility and orchestration via AI	Autonomous detection, predictive defence, business-aligned resilience

Source: IDC, 2025

The future of cyberdefence: Unified, intelligent, and co-managed

As Asia/Pacific enterprises advance towards AI-enabled defence, success will depend on unifying fragmented tools, operationalising intelligence, and co-creating outcomes with MSSPs.

Three pillars of the future-ready security model

Unified platforms — End-to-end visibility and orchestration across hybrid environments.

Intelligent operations — AI-driven detection, automated triage, and predictive threat modelling.

Collaborative ecosystem — MSSPs delivering scale, talent depth, and cross-industry intelligence.

In the intelligent era, cybersecurity is not just about protection! It's about partnership, prediction, and preparedness.

Source: IDC's *CIO Sentiment Survey*, 2025 (n = 146)

Message from the sponsor

LUMEN®

Beyond protection: Powering AI-enabled co-managed cybersecurity to deliver resilience and operational intelligence tailored for the modern APAC enterprise.

Modern APAC enterprises are under pressure to consolidate fragmented security tools, close talent gaps, and align resilience with business priorities. By simplifying complexity and enhancing resilience, Lumen enables organisations to protect critical assets while driving business continuity. Backed by deep expertise, best of breed technologies and solutions, Lumen transforms fragmented defences into a unified, future-ready security foundation.

Find out more

IDC Custom Solutions

December 2025 | #AP242545IG | Sponsored by Lumen

IDC Custom Solutions produced this publication. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.