IN PARTNERSHIP WITH:

aryaka

C-SUITE SURVEY

THE NETWORK RECKONING: WHY SOUTHEAST ASIA'S ENTERPRISES ARE REBUILDING CONNECTIVITY FROM THE GROUND UP

Powered by:

FUTURECIO
Leading Enterprise Transformations

cxociety

CONTENTS

aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com

FUTURECIO
Leading Enterprise Transformations

FutureCIO is about enabling the CIO, his team, the leadership and the enterprise through shared expertise, know-how and experience - through a community of shared interests and goals. It is also about discovering unknown best practices that will help realize new business models. For more information, visit www.futurecio.tech

Introduction

IT leaders across Indonesia, Malaysia and Singapore describe networks buckling under demand nobody quite planned for, and a security model that looks unified in name only for many. A four-question pulse survey lays out both problems in numbers.

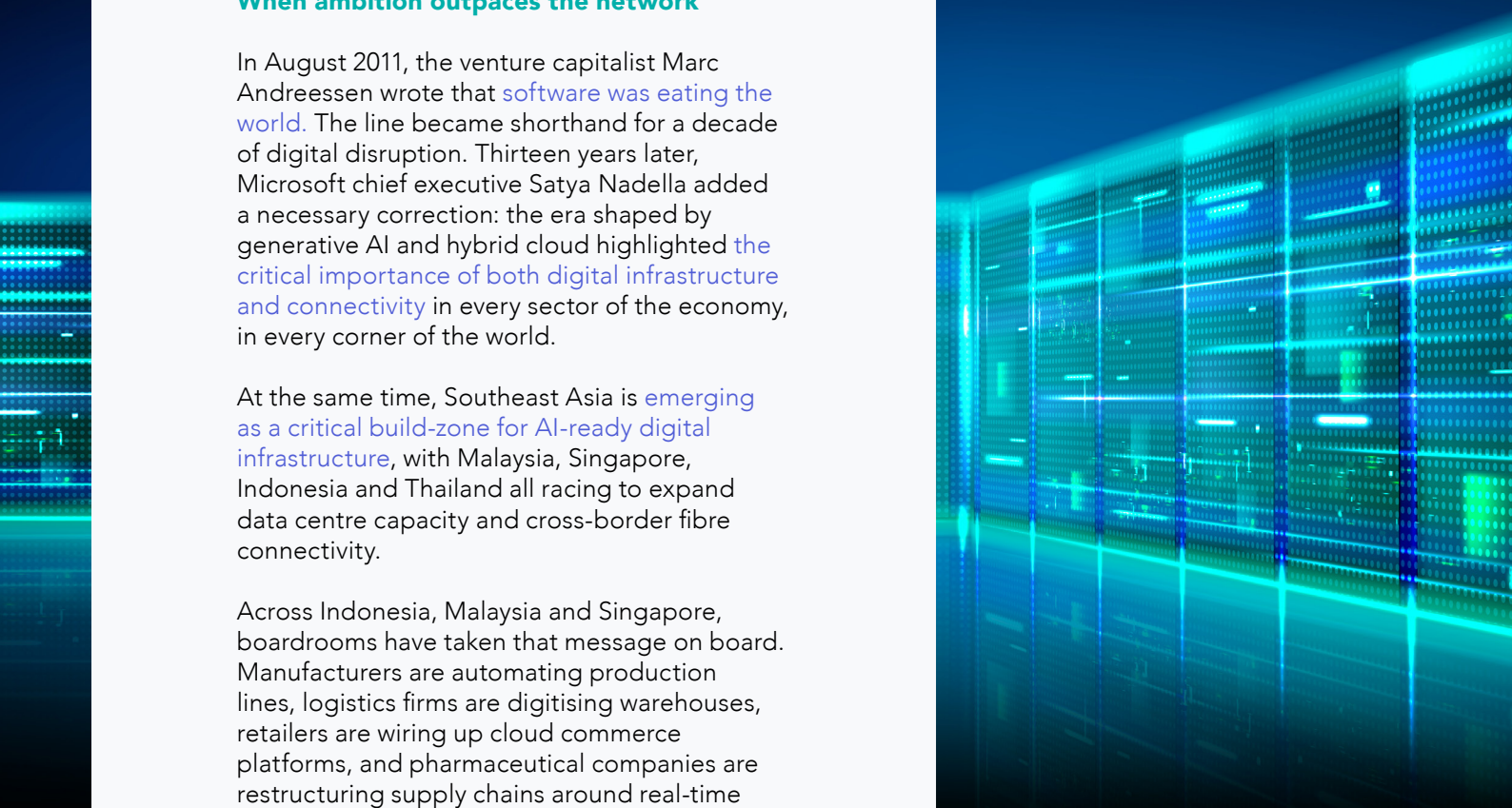
When ambition outpaces the network

In August 2011, the venture capitalist Marc Andreessen wrote that software was eating the world. The line became shorthand for a decade of digital disruption. Thirteen years later, Microsoft chief executive Satya Nadella added a necessary correction: the era shaped by generative AI and hybrid cloud highlighted the critical importance of both digital infrastructure and connectivity in every sector of the economy, in every corner of the world.

At the same time, Southeast Asia is emerging as a critical build-zone for AI-ready digital infrastructure, with Malaysia, Singapore, Indonesia and Thailand all racing to expand data centre capacity and cross-border fibre connectivity.

Across Indonesia, Malaysia and Singapore, boardrooms have taken that message on board. Manufacturers are automating production lines, logistics firms are digitising warehouses, retailers are wiring up cloud commerce platforms, and pharmaceutical companies are restructuring supply chains around real-time data.

A Cxociety Research pulse survey, conducted in partnership with Aryaka, of the region's enterprise IT leaders suggests that the infrastructure underneath all of this is starting to give way.



Methodology

The respondents represent a strategic cohort across Indonesia, Malaysia and Singapore, with a strong focus on senior decision-makers. The job-level breakdown reinforces the report's focus on strategic cost and commercial return:

- Executive and C-suite accounting for 13%
- Senior leadership (and upper management) made up 13%
- Mid-level managers comprised 33% of respondents
- Heads of departments round out the group at 41%

The survey sample spans a variety of key industries within economies of Indonesia, Malaysia and Singapore:

- Natural resources & heavy industries (40%), infrastructure, construction & logistics (20%), consumer & retail (13%), public sector & essential services (11%), financial & professional services (9%), and technology, telecom & media (6%).

This comprehensive profile of senior leadership across a broad spectrum of enterprises in ASEAN enables the report to understand the strategic pivots that businesses in the region need to make to capture the promise of technology and drive forward innovation, despite the prevailing unpredictability of economic environments.

Findings

The analyst firm IDC put a number on that strain in a January 2025 Spotlight report, Unified Networking and Security Platform Accelerates Network Transformation: more than 35% of Asia-Pacific enterprises are seeing bandwidth demand grow by over 50% a year, pushed along by cloud migration, e-commerce, real-time analytics and, increasingly, generative AI applications hungry enough to strain wide area networks (WANs) that were never built for this kind of load.

Gartner's 2026 strategic roadmap for enterprise networking flags that agentic NetOps — AI systems that autonomously manage, troubleshoot and optimise infrastructure — will move from experimental to mainstream, with 50% of organisations expected to use agentic NetOps with minimal human involvement by 2027, up from nearly zero in 2025.

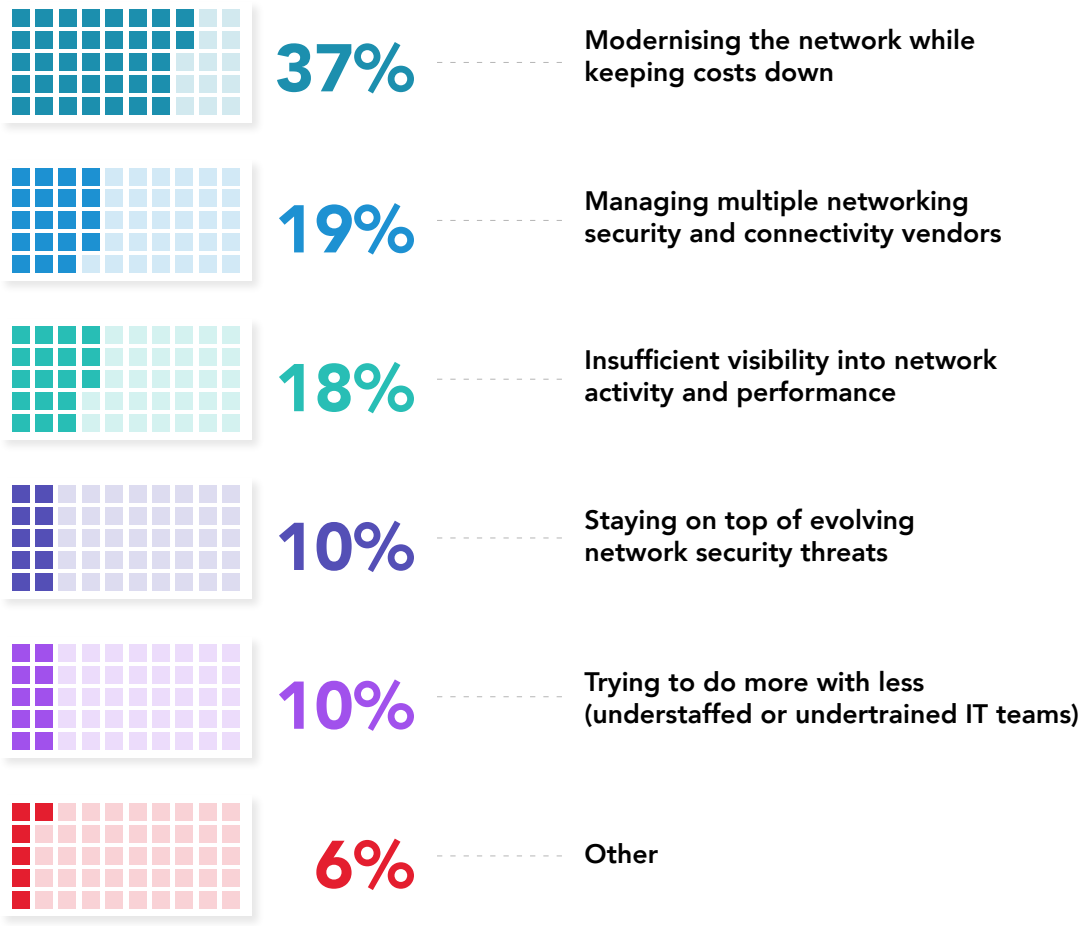
That automation pressure is arriving at a moment when enterprise confidence in existing defences is low: PwC's 2026 Global Digital Trust Insights survey found that 60% of business and technology leaders now rank cyber-risk investment among their top three priorities, yet only 6% express confidence across all areas of their security posture.

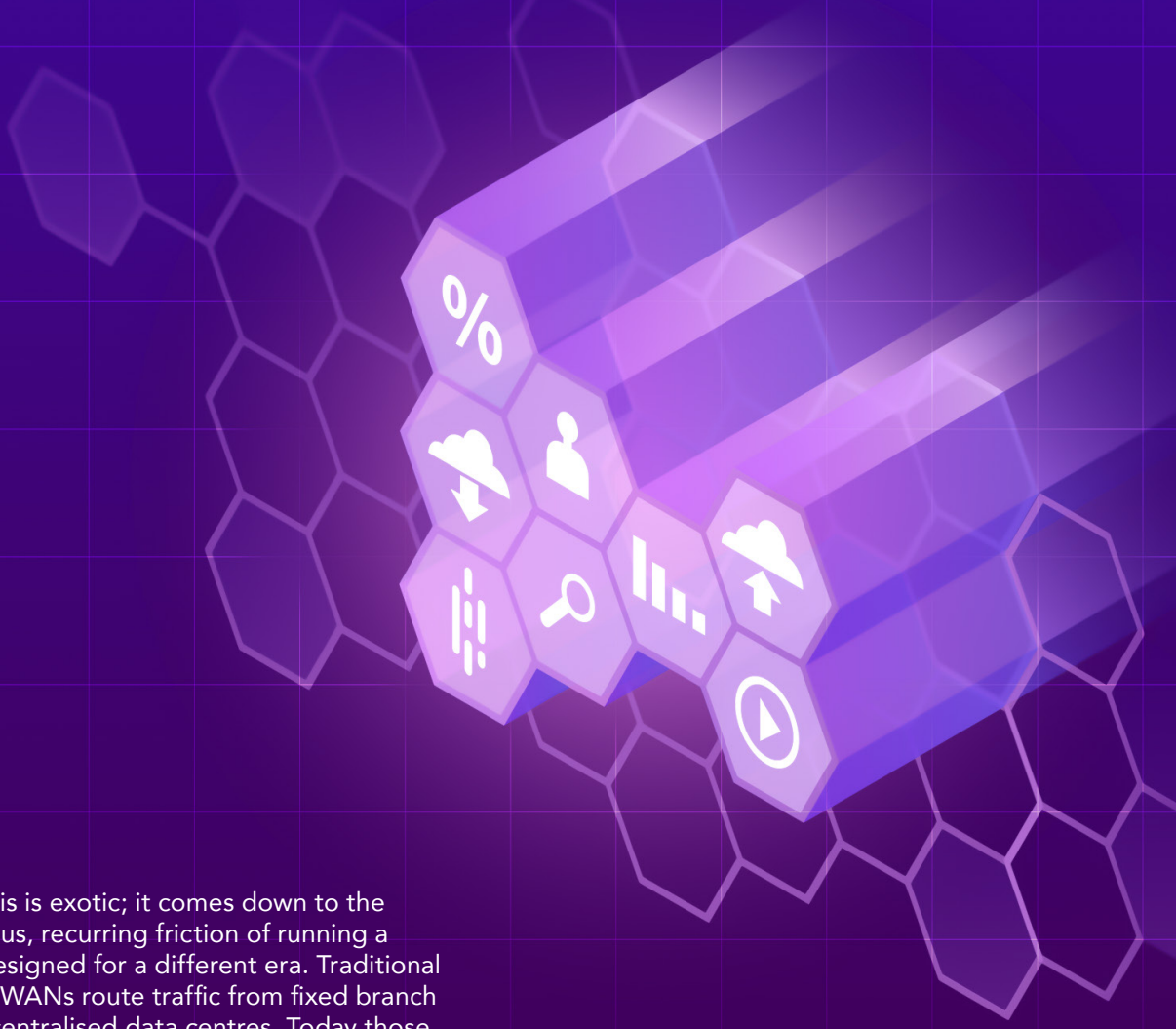
Where does that pressure actually land? The Cxociety Research pulse survey breaks it down:

Figure 1

n= 100

What is your top day-to-day networking challenge?



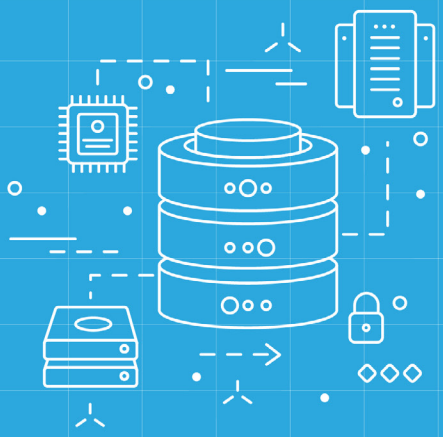


None of this is exotic; it comes down to the unglamorous, recurring friction of running a network designed for a different era. Traditional enterprise WANs route traffic from fixed branch offices to centralised data centres. Today those same networks must support hyper-distributed cloud platforms and a mobile workforce, without a matching rise in operating or capital expenditure.

Buying more bandwidth is not the fix; in fact, it contributes to the operating expenditure. Without changing how traffic is routed and inspected, added capacity just raises the cost of running an architecture that's already struggling.

They are looking to swap them for cloud-native, zero trust WAN alternatives that promise up to 50% lower connectivity costs alongside the low-latency, multi-cloud access that generative AI workloads demand.

Three-quarters of IT leaders surveyed in the Cxociety Research pulse survey say they plan to retire legacy Multiprotocol Label Switching (MPLS) circuits within two to three years.



Calculating the cost of sprawl

For much of the past decade, security teams answered every new gap in the attack surface predictably: they bought another tool. As workloads shifted to public cloud and workforces became distributed, that meant next-generation firewalls, secure web gateways, cloud access security brokers and dedicated software-defined wide area network (SD-WAN) appliances. Each one plugged a specific hole but introduced its own management console.

IDC's research reaches a similar conclusion, arguing that years of layering security products onto existing stacks have produced not resilience but paralysis.

As IDC analysts Ghassan Abdo and Pete Finalle put it, piecemeal purchasing across the industry has left businesses with "overlapping or duplicate features" among tools that were never designed to work together, plus the added cost and management complexity that follows.

The practical fallout is easy to see once you know where to look. Security analytics sit in one vendor's console while performance data lives in another's, so blind spots persist long enough to slow detection and drag out incident response. Policies get re-entered by hand across separate systems, which is exactly how misconfiguration and drift creep in.

Then there's the matter of time: keeping dozens of appliances patched and orchestrated eats into hours that IT teams could otherwise spend on architecture and planning, a problem made worse by the 10% of surveyed organisations that already describe themselves as understaffed or undertrained.

Vendor sprawl is now the single biggest daily headache for 19% of regional IT leaders, and another 18% say they just don't have visibility into network performance and threat activity.

The stakes are highest at the operational technology (OT) and Internet of Things (IoT) edge, where factory floors, automated warehouses and pharmaceutical supply chains are connecting ever more sensors that legacy perimeter tools aren't built to inspect.

That's because these sensors speak non-standard protocols the tools were never designed to read. A single breached endpoint, in that scenario, is enough to halt supply-chain operations across the region.

Latency makes the problem worse: backhauling cloud-bound traffic through a centralised security stack before it reaches the public cloud adds network hops and slows everything down. It also adds real consequences for customer experience and revenue in time-sensitive sectors such as manufacturing, logistics and retail.

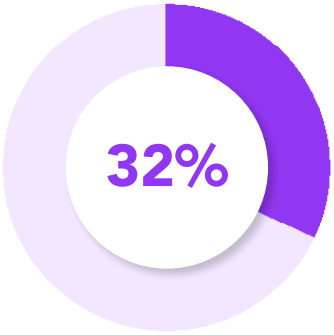
The alternative gaining ground decrypts and inspects traffic once, applying networking, secure web gateway, cloud access security broker and firewall policies simultaneously from a single console, rather than passing it through a chain of separate tools.

Vendors describe this as a create-once, enforce-everywhere model. Whatever the label, it's built to close the visibility, and consistency gaps this survey keeps turning up.

Figure 2

n= 100

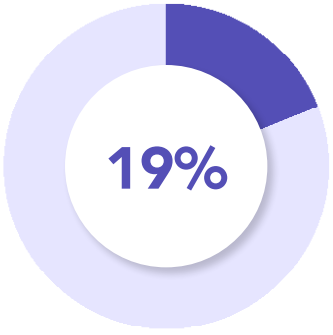
How does your IT organisation currently perceive the value of converging networking and security at the edge, such as through Secure Access Service Edge (SASE)?



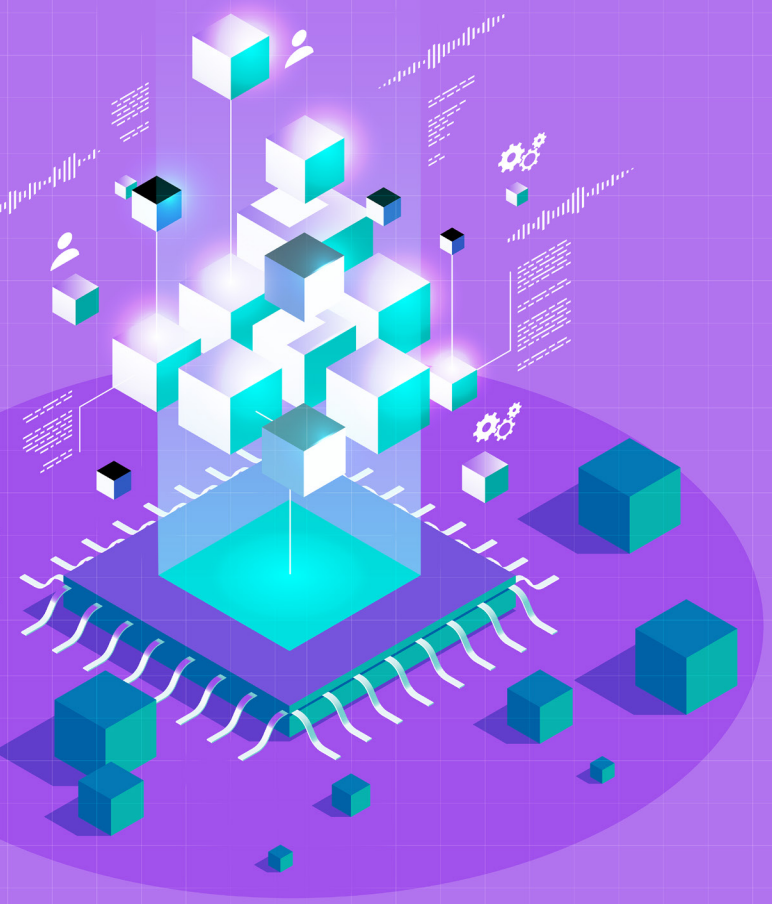
Need more information to understand its benefits better

View it as mission-critical for digital resilience and transformation

Only some stakeholders are aware of its potential



No current interest



SASE maturity is not what it seems

Secure access service edge (SASE) combines software-defined networking with cloud-native security services, such as secure web gateways, cloud access security brokers and zero trust network access, to resolve that same fragmentation. On paper, adoption looks advanced.

On the surface, adoption looks mature, with 38% of respondents saying they've already implemented SASE. But dig past the headline number, though, and the picture gets messier: 32% say they need more information before they properly understand the business case, 20% report that only a subset of internal stakeholders understands the value, and a mere 29% currently treat SASE as mission-critical to digital resilience.

That gap now has an industry label: pseudo-SASE. It means bundles of existing products relabelled and sold as a single platform while, underneath, they keep separate management planes, separate policy databases and fragmented data paths. Plenty of buyers thought they were consolidating when they signed up for one of these. What they have done is give their sprawl a new name.

The market is voting with its wallet. Gartner forecasts that by 2027 nearly two-thirds of new SD-WAN purchases will be part of a single-vendor SASE offering, up from roughly 20% in 2024, as buyers prioritise integrated policy control and vendor simplicity.

Against that backdrop, the global SASE market is on track to reach $28.5 billion by 2028, making the difference between a genuine platform and a rebadged bundle a multi-billion-dollar distinction.

Buyers seem to be catching on to the trick. IDC's data shows 31.3% now regard it as extremely important that SASE come from a single vendor, against just 5% who see consolidation as unimportant. It reflects an expectation built on the idea that a genuine platform should deliver more than the sum of its parts, and that shopping à la carte, best-of-breed style, is quietly becoming obsolete.

Getting this wrong is common. In IDC's global research, 85% of SASE buyers hit some kind of operational issue or disruption during deployment, and only 15% called their rollout clean. Forty-six per cent blamed service disruptions on policy complexity; 42% suffered outages from network misconfiguration.

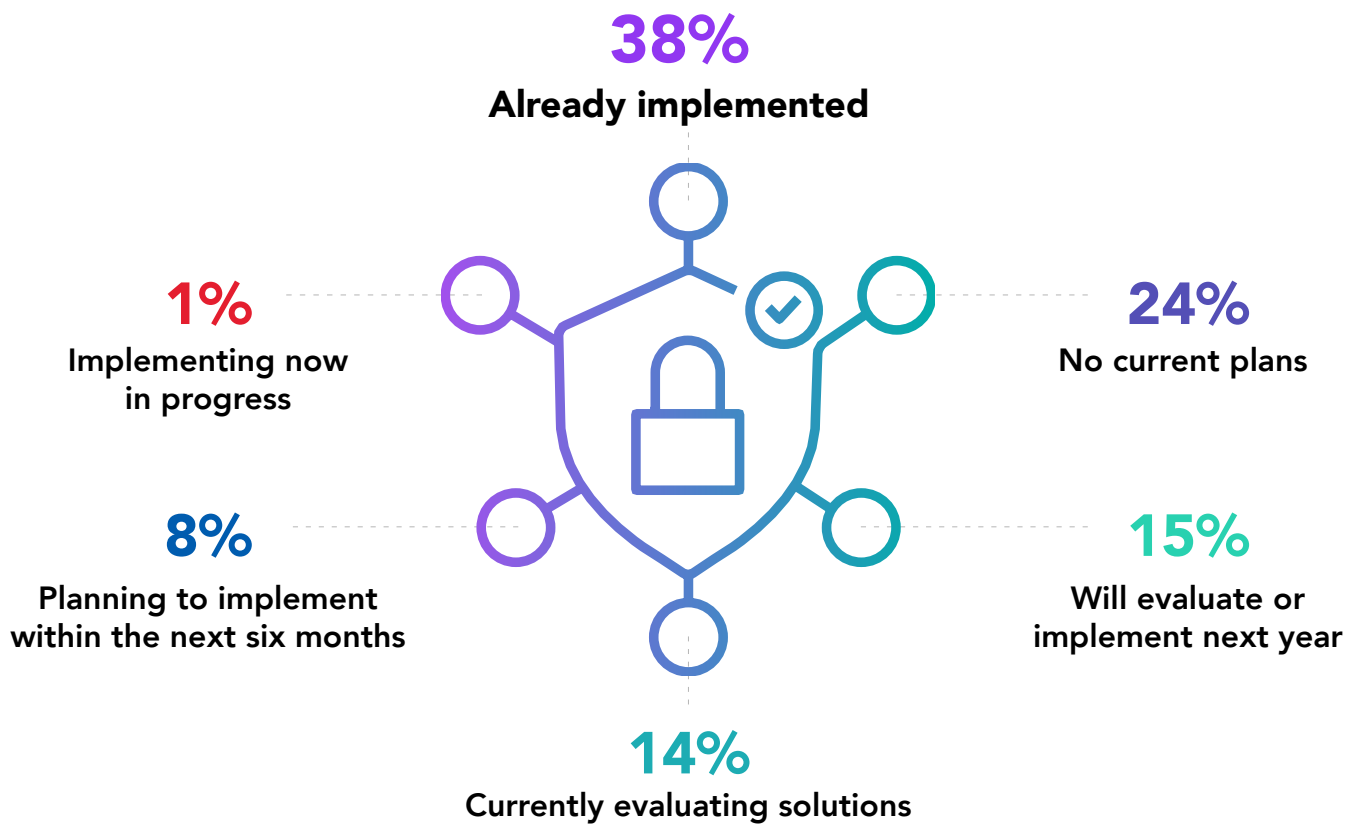
IDC's explanation is simple: Full SASE adoption usually means ripping out existing tools altogether, which disrupts established workflows and forces staff to learn an unfamiliar, monolithic product almost overnight, with security policy and network architecture complexity responsible for most of the damage recorded.

It's part of why close to a third of the region's IT leadership is still hanging back. Consolidating networking and security in-house, without a platform that was unified from day one, tends to recreate the very instability it was supposed to fix. When the rollout is done on a genuinely unified platform, the returns are measurable.

Figure 3

n= 100

? Do you plan to implement a converged networking and security solution, such as Secure Access Service Edge (SASE), and, if so, when?



Securing the connected workforce at the elastic edge

Ask regional IT leaders what they most want to fix in the next 12 months, and cost control isn't the top answer. Neither, somewhat surprisingly, is network visibility.

Gartner's 2026 enterprise networking roadmap identifies zero-trust and cloud-centric architectures as the dominant response to this shift, noting that SASE has moved from "nice to have" to a critical framework for modern cybersecurity and networking architecture.

The winner is securing connectivity for a global, hybrid workforce, ranked top by 26%, ahead of better observability (18%), simplifying operations (18%) and converging network and security functions (17%).

The ranking reflects a structural shift: the corporate perimeter, once a physical boundary defined by offices and local firewalls, now extends to remote employees, multi-cloud platforms and distributed edge devices scattered across the region.

Hardware-centric security wasn't built for this kind of perimeter, and the results show. Route remote traffic back through a central data centre via a legacy virtual private network (VPN) concentrator and you add latency and frustrate users; let distributed endpoints connect straight to cloud applications without inspection, and the friction disappears along with any real oversight of the attack surface.

The emerging answer is a zero trust architecture built directly into the network fabric, where no connection, whether from a headquarters office, a remote employee or an automated cloud process, is trusted by default.

Each one must be authenticated and authorised, every time. Delivering that consistently across a distributed workforce depends on universal zero trust network access paired with the same single-pass processing engines described earlier, now resolving decisions at points of presence close to the user rather than in a distant data centre.

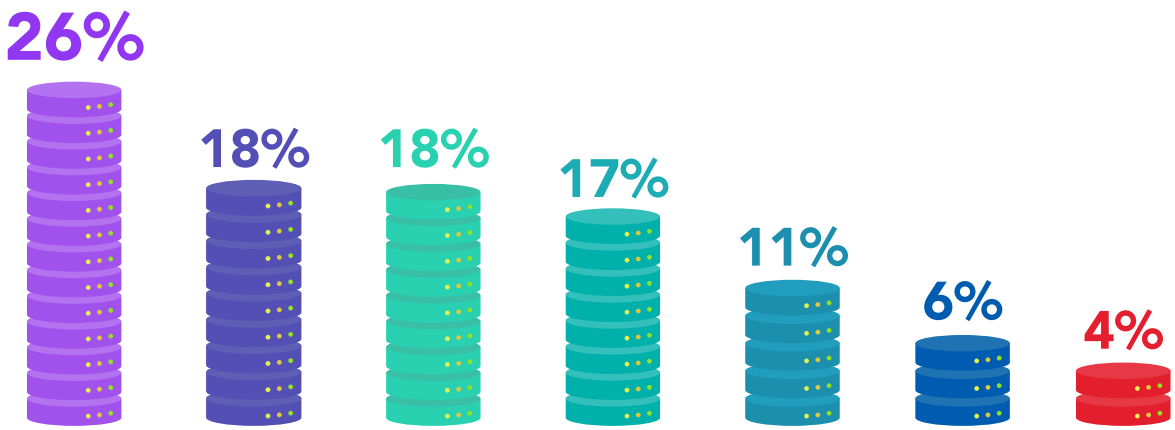
Generative AI complicates this further. As it embeds itself into everyday SaaS tools, such as Microsoft 365, Salesforce and SAP, employees are increasingly pasting proprietary code or customer data into public models nobody sanctioned, a habit now commonly known as shadow AI.

This has turned inline data-loss prevention from a nice-to-have into a practical necessity. It's also why a single-pass SASE architecture is designed to inspect and contextualise that traffic in real time, blocking leakage and prompt-injection attempts without adding the latency that would otherwise wreck the user experience.

Figure 4

n= 100

What is your top networking and network security priority for the next 12 months?



- Improving secure connectivity to the global/hybrid workforce
- Gaining better observability into network performance and security
- Simplifying operations and reducing the cost of network management
- Converging network and security operations
- Improving network, multi-cloud, SaaS, and application performance (e.g. reducing latency)
- Lessening the workload on network and security teams
- Other

From ownership to service

Enterprise IT teams increasingly aren't trying to build this themselves. Faced with rising bandwidth costs, tool sprawl and deployments that go wrong more often than not, fewer than 1% intend to keep their stack entirely on-premises for the long haul.

The logic is clear: Building and running a converged networking and security stack in-house takes specialist skills that most internal teams simply don't have. IDC's numbers back this up: 28.7% of enterprise SASE buyers already lean on managed services to implement and run their environments, and that share is climbing steadily across Asia-Pacific.

Three factors seem to be driving that decision.

1. Speed and risk reduction

A managed provider brings standardised architecture, automated policy orchestration and ongoing support. Combined, that can compress implementation timelines from nine months or more down to a matter of weeks, sidestepping many of the configuration errors that plague in-house builds.

2. Operational simplicity

A managed, unified SASE deployment consolidates network administration, policy configuration and performance monitoring into a single console, letting lean IT teams, including the 10% who describe themselves as understaffed in the Cxociety Research pulse survey, maintain consistent enforcement without juggling disparate tools.

IDC found that more than 40% of enterprise buyers plan to shift over half of their legacy network security stack to a service-based delivery model within two years

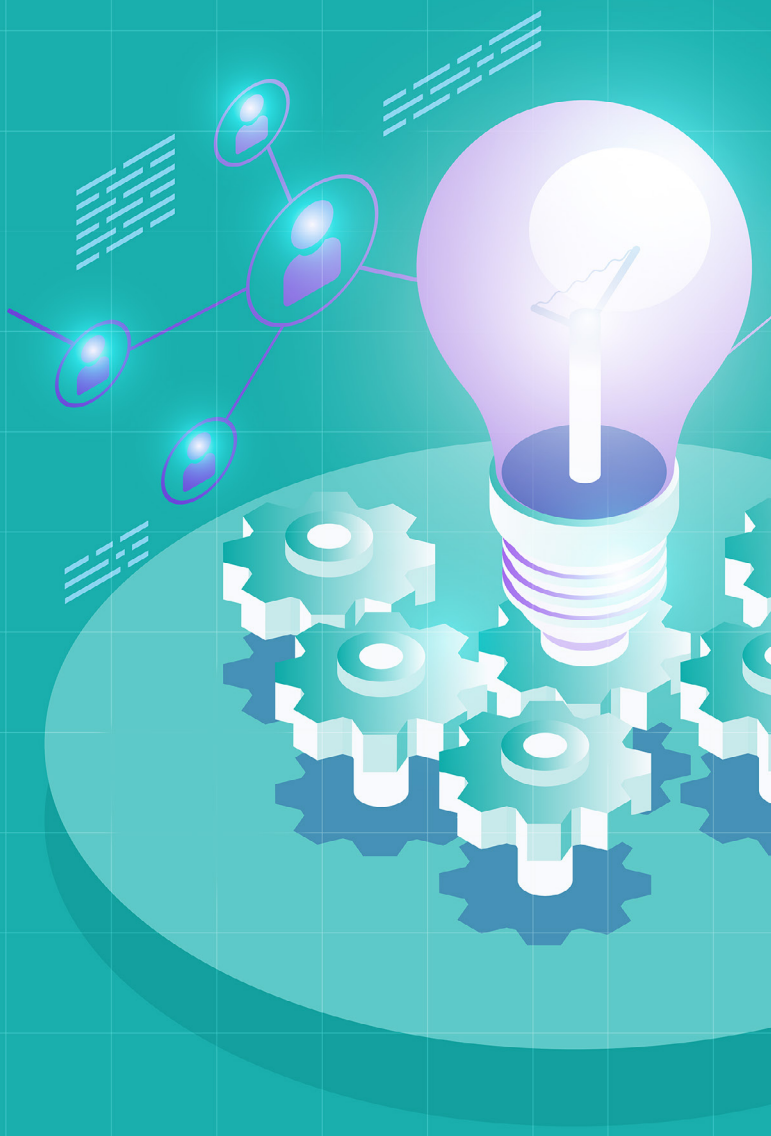
AI-driven observability turns monitoring from passive log collection into proactive remediation, correlating network telemetry with threat feeds and isolating root causes before latency becomes a business problem. IDC in its report found that 92.3% of SASE adopters report a measurable improvement in their overall security posture after deployment.

3. Financial flexibility

Traditional hardware refresh cycles demand upfront capital spending on equipment that depreciates and needs ongoing maintenance contracts. Managed SASE runs instead on an operational, consumption-based model, letting enterprises scale bandwidth and security capacity in line with actual business growth rather than a hardware refresh schedule.

Conclusion

The real constraint on resilience



None of this suggests Southeast Asia's enterprises lack ambition. IT leaders across Singapore, Malaysia, Indonesia and the wider region understand exactly what hybrid cloud, AI and automation require; what the pulse survey data expose is how much legacy infrastructure, and the security architecture built around it, are holding that ambition back.

Organisations that keep patching the old model with more point products can expect more of what this survey already shows: vendor sprawl, climbing bandwidth costs, configuration risk. Those moving towards a natively converged, unified SASE architecture, increasingly delivered as a managed service, are reporting fewer disruptions, better visibility and a real uptick in security posture.

As manufacturing, logistics, retail and pharmaceutical firms across Southeast Asia accelerate digital transformation—and as countries including Indonesia, Malaysia and Singapore expand the digital backbone to support it—the divide will not remain a technical gap. It will become a competitive fault line, separating enterprises that can fully participate in the region's next phase of growth from those increasingly left operating at its edges.

CXOCIETY PTE LTD
12 Woodlands Square, #12-85,
Woods Square, Singapore 737715
www.cxociety.com
Email: publishers@cxociety.com