Focus Network

Optimising Cyber Resilience in an AI-Driven World

Author
Andrew Milroy
Vice President and
Head of Research
Focus Network

www.focusnetwork.co

Optimising Cyber Resilience in an AI-Driven World

In a world where change is the only constant, executives have recognised the need to immerse themselves in a community of peers facing similar challenges. Focus Network's CISO Executive Society is a valuable way of understanding and of gaining fresh insights on cybersecurity best practices and of networking with peers. As an Executive Society member, CISOs gain access to a community where shared insights and experiences are invaluable.

All Executive Society members hail from organisations with a workforce exceeding 500 individuals. Additionally, they hold senior executive roles, leading the charge in steering investment and driving transformative initiatives.

In late March 2024, Focus Network held a CISO Executive Society briefing in Singapore with 25 members. The event included an interactive analyst presentation on current cybersecurity trends and a panel discussion.

During the sessions, Focus Network analysts shared research data and insights with attendees and received detailed feedback. The five key Focus Network insights derived from the research and CISO feedback are:

1. Nearly half of Singapore organisations expect their cybersecurity budgets to decrease or stay the same in 2024 — despite a much more dangerous threat environment. This can be explained by the increasing pressure on cybersecurity leaders to generate and demonstrate more value from existing investments. Additionally, CISOs are expressing concern that AI spending is starting to crowd out cybersecurity expenditure.

2. Singaporean CISOs are focused on the 3 Cs (compliance, complexity and cost issues). 63% cite compliance as their major challenge. This is particularly notable in the financial services sector where cybersecurity leaders are continually working to be aligned with changing Monetary Authority of Singapore (MAS) guidelines.

3. Generative AI is being used to help cybersecurity leaders to do more with less. It is being embedded into security operations and used to increase efficiency and productivity across a range of activities from training to threat management.

4. Cloud security is a leading initiative for the majority of Singapore cybersecurity leaders. Cloud adoption accelerated rapidly during the Covid period and security often received insufficient focus. Misconfigurations and confusion around the shared responsibility model, are common.

5. A predominantly perimeter-based 'castle and moat' approach to cybersecurity remains, for many Singaporean companies, making them immature from a cybersecurity perspective. Companies are rapidly adopting zero-trust approaches and an 'assume breach' posture. Few can claim to be continuously monitoring their assets and adapting their posture in line with the dynamic risk environment.

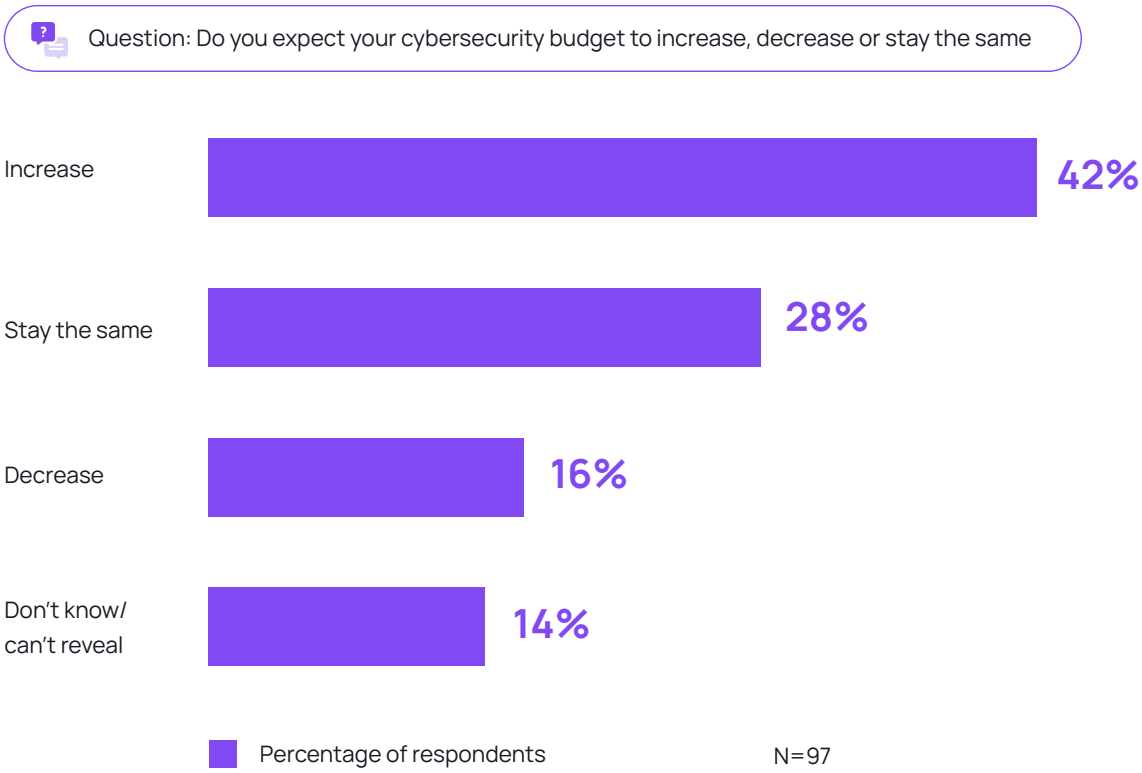
44% of Singaporean Companies Expect Cybersecurity Budgets to Decrease or Stagnate in 2024.

Singapore companies and consumers are facing an increasingly dangerous cyber threat environment. Attackers are leveraging new technologies, in particular AI, to improve the effectiveness of their TTPs. Enterprises are seeking ways of combatting emerging threats as well as ensuring that their cybersecurity postures can adequately address existing threats.

Despite the more complex threat environment, Focus Network research reveals that 44% of Singaporean organisations are expecting falling or stagnant cybersecurity budgets in 2024. Lower or stagnant budgets are being reported across other geographies, so Singapore is not unusual in this sense.

Figure 1 illustrates expected cybersecurity budget changes in Singapore in 2024.

Figure 1: Cybersecurity Budget Changes, Singapore



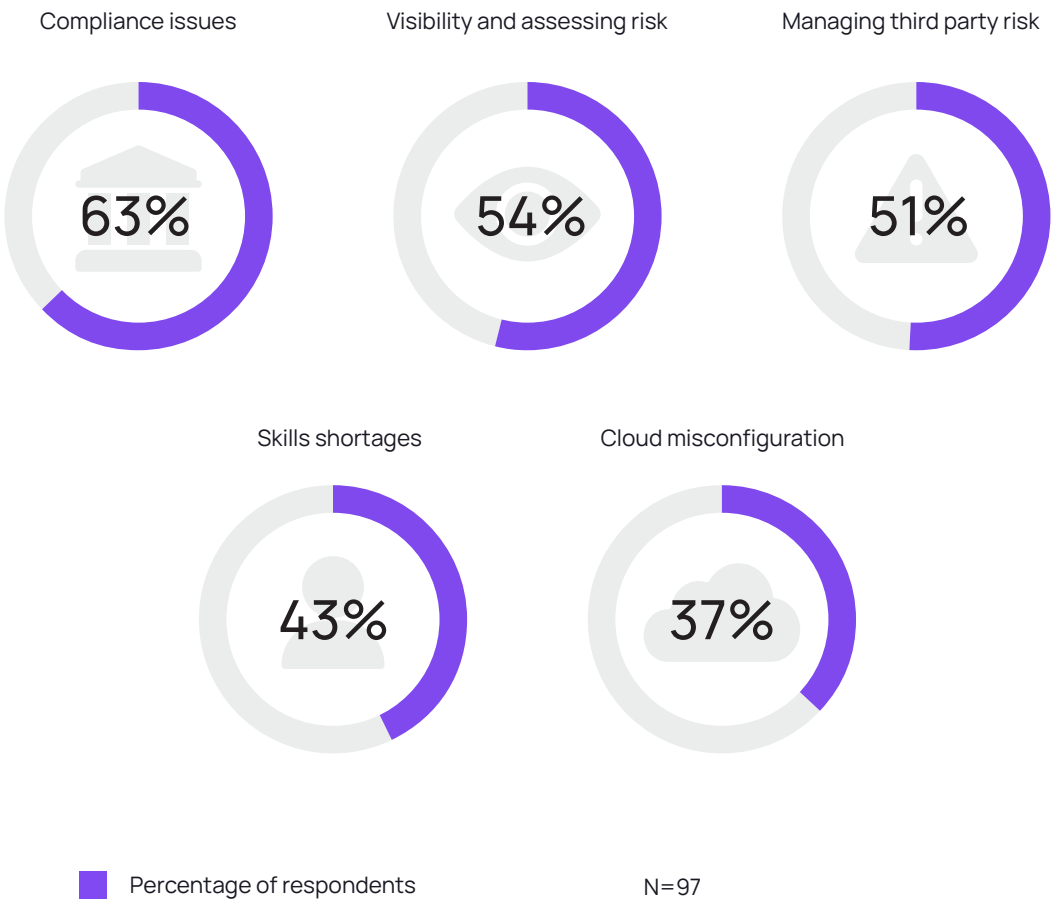
Reasons given for stagnating or declining cybersecurity budgets include, the need to demonstrate the value of cybersecurity investments to budget holders, poor communications between cybersecurity professionals and other leaders, and increased AI investments at the expense of other budgets, including cybersecurity.

63% of Cybersecurity Leaders Cite Compliance as their Biggest Challenge

The three Cs of compliance, complexity and cost, continually emerge as leading challenges for cybersecurity leaders in Singapore. Focus Network research reveals that 63% of Singapore-based cybersecurity leaders consider compliance to be their leading challenge with 54% citing visibility and assessing risk. The financial services sector is disproportionately large in Singapore and complying with changing MAS guidelines can be extremely difficult. Singaporean companies deploy an average of 41 separate cybersecurity tools, many of which are not integrated. Reducing the number of tools can lower complexity and improve visibility for cybersecurity leaders.

Figure 2 shows the leading cybersecurity challenges for Singaporean organisations. Managing third party risk, skills shortages and cloud misconfigurations are also cited as leading challenges.

Figure 2: Leading Cybersecurity Challenges, Singapore



Cloud Security is a Leading Initiative for 59% of Singapore Cybersecurity Leaders

An accelerated shift to the cloud during the Covid period was particularly noticeable in Singapore. As companies rushed to ensure that their workers could operate remotely, cloud services were adopted rapidly. Often, security was not the first consideration and traditional perimeter-based cybersecurity postures were maintained. The use of multiple cloud resources has forced Singapore companies to focus on end points to a greater extent and to take a more distributed approach to security. With cloud misconfigurations and vulnerabilities becoming common, cloud security is the leading initiative for cybersecurity leaders in Singapore.

Identity and access management (IAM) also emerges as a leading initiative. Cybersecurity leaders in Focus Network's Executive Society explained that IAM is one of the most cost-effective ways of reducing risk.

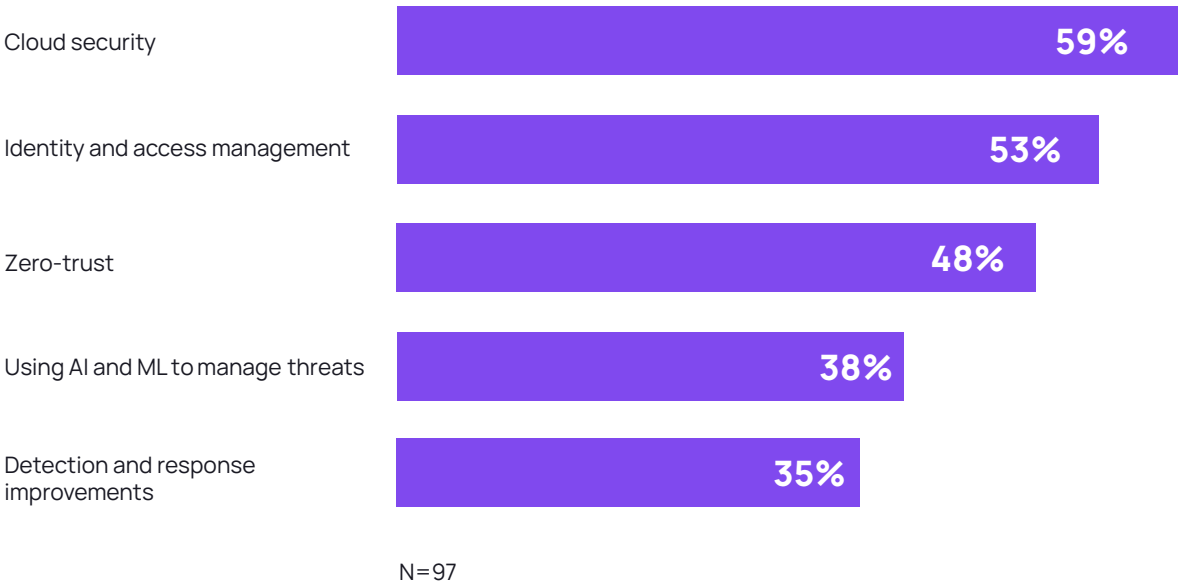
With most Singaporean companies now taking an 'assume breach' approach to cybersecurity, the implementation of zero-trust controls is becoming more critical than ever.

Greater focus on detection and response and increased use of AI and ML also emerged as major initiatives for Singaporean cybersecurity leaders. Emphasis has traditionally been placed on the first two elements of the NIST cybersecurity lifecycle (identify and protect). Commonly in Singapore, insufficient emphasis had been placed on the other three elements of the cybersecurity lifecycle (detect, respond and recover). This is changing as organisations acknowledge that they will be breached, and need to limit damage caused by breaches.

AI is now being widely used by attackers, making their threats increasingly dangerous and difficult to defend against. Building AI, particularly generative AI into defensive activities is now playing a major role in risk mitigation.

Figure 3 shows the leading cybersecurity initiatives being taken by Singaporean organisations.

Figure 3: Leading Cybersecurity Initiatives, Singapore



Generative AI Embedded in Security Operations

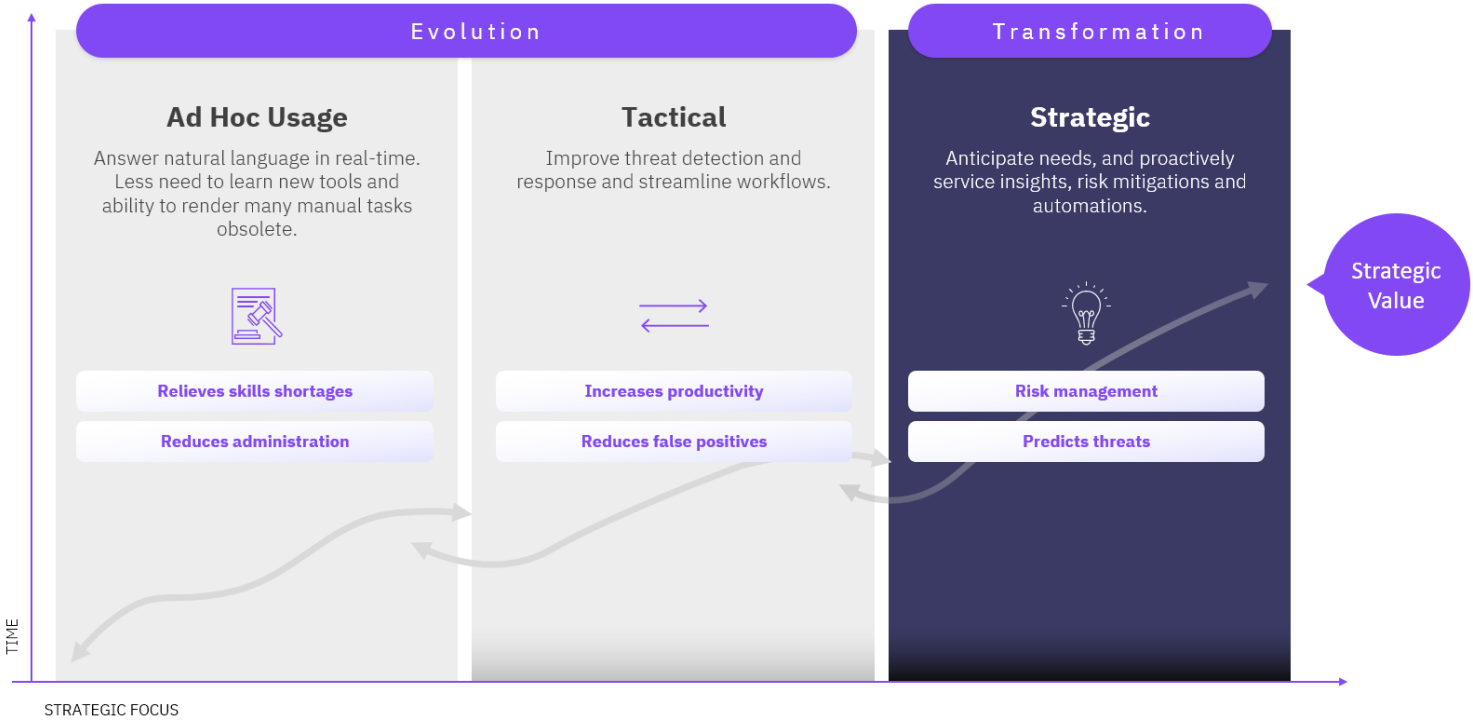
Generative AI is making security teams more efficient and productive. It can help the cybersecurity function of address increasing skills shortages as well as an expanded threat landscape.

Most organisations are using Generative AI on an ad hoc basis to relieve skills shortages and reduce administration. Focus Network's community reveals that many members, particularly financial services firms, are already embedding generative AI into their operations for tactical purposes. It is increasing productivity for these organisations as well as reducing false positives and ensuring that cybersecurity posture is aligned with the risks and risk appetite.

Increasingly, Focus Network expects generative AI to disrupt and transform the cybersecurity function. It can be expected to anticipate needs by predicting threats and proactively managing risk.

Figure 4 shows the evolution of Generative AI use in cybersecurity.

Figure 4: Use of Generative AI in Cybersecurity



Ways that Generative AI can support, drive or transform security operations include:

Threat intelligence and hunting. Massive amounts of data can be analysed simultaneously to identify vulnerabilities. Recommendations can then be made on necessary changes to cybersecurity postures.

Consolidation of data and resources on fewer dashboards. Data can be collected, aggregated and analysed from multiple sources and presented on one dashboard. This reduces complexity, and makes security operations more productive and efficient.

Contextualised monitoring, reporting and recommendations. This enables security teams to search existing code, networks and systems for vulnerabilities and offer contextualised risk management recommendations.

Patch management. Generative AI can automate the identification of required patches and updates across the enterprise.

Forensics and incident management. Generative AI can analyse attacker activity to understand their TTPs, following an incident. This information can be used to identify and mitigate exploited vulnerabilities.

Cybersecurity training. Generative AI can use synthetic data and other inputs to simulate attacks and scenarios based on the latest threat intelligence

Phishing mitigation. Generative AI can detect phishing attacks based on analysing massive volumes of data and then intervene to prevent the attacks.

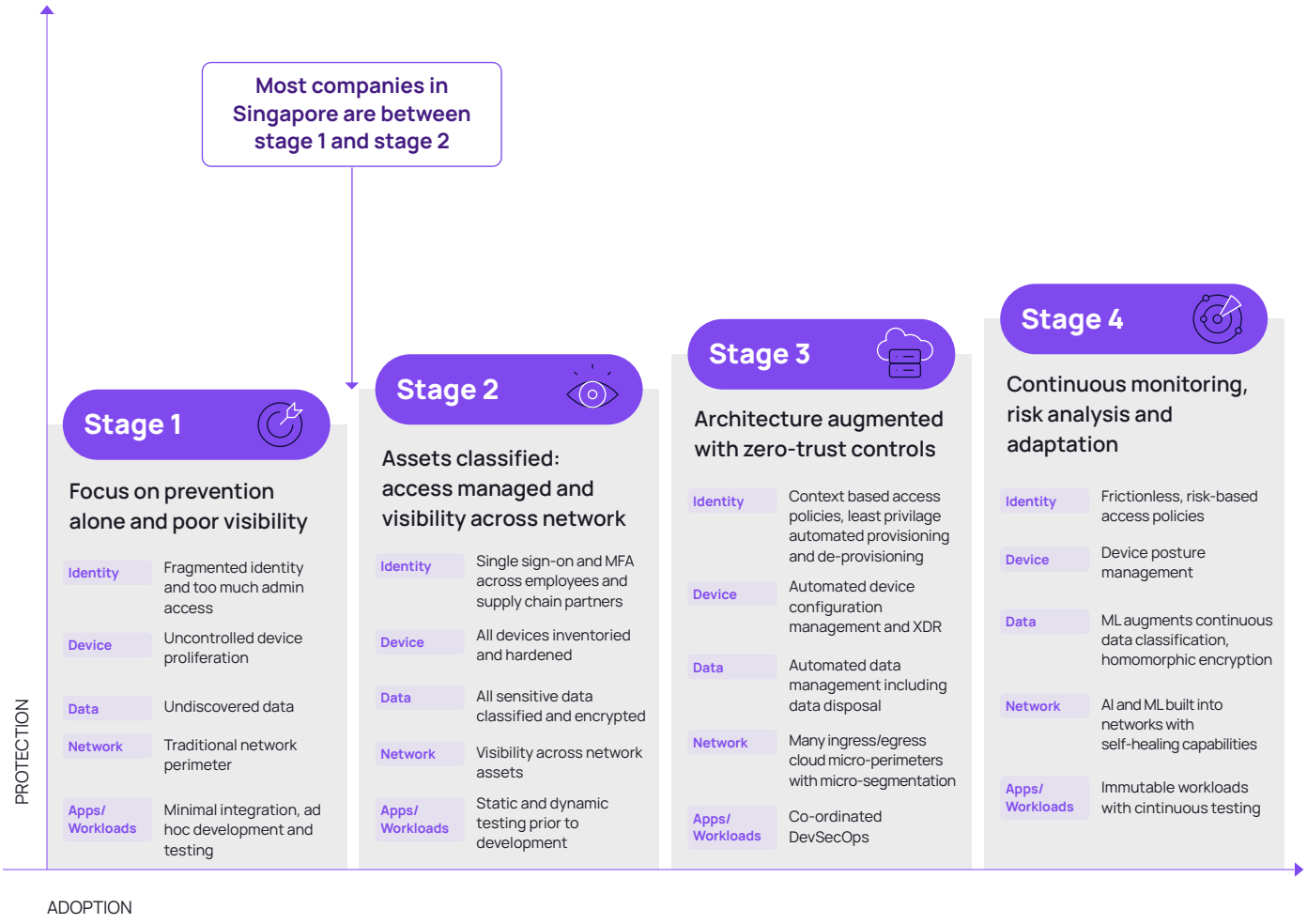
Cybersecurity Maturity in Singapore Remains Mixed

Focus Network's cybersecurity maturity curve is a useful tool for understanding where organisations lie in terms of cybersecurity and what they need to do, to manage cybersecurity risk more effectively.

Plenty of Singapore organisations remain focused on traditional preventative, perimeter-based controls, have fragmented identities and undiscovered and unclassified data. This makes them extremely vulnerable. However, data classification, more sophisticated identity and access management combined with greater visibility across networks and distributed assets is helping Singapore organisations to reduce risk.

On average, Singapore-based organisations sit between stages 1 and 2 of the cybersecurity maturity curve shown in Figure 5.

Figure 5: Cybersecurity Maturity Curve



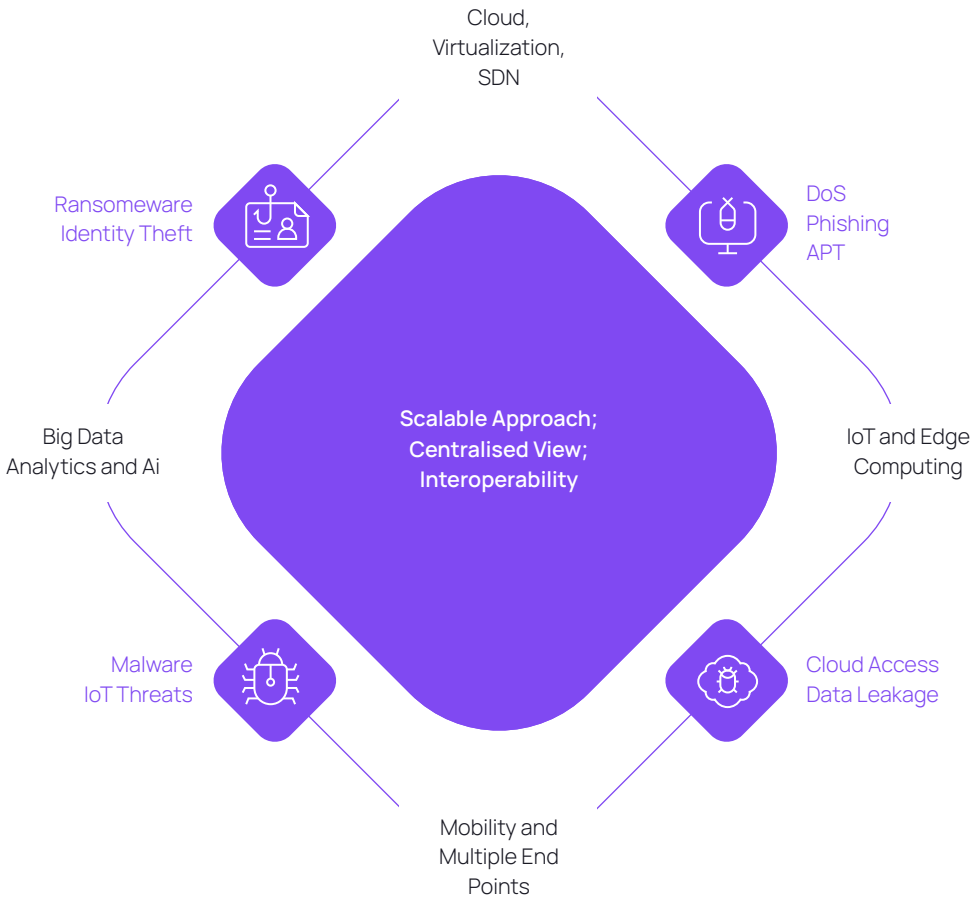
Singaporean companies need to work towards an ideal cybersecurity posture where assets are continuously monitored, postures adapt based on dynamic risk assessments and AI and ML are core to operations. Testing needs to be continuous and much more attention must be paid to secure coding.

Centralised, Scalable and Adaptable Approach is Required

Greater cyber maturity can be built by continually monitoring all data traversing all systems, networks and endpoints while adapting cybersecurity posture to address changing threats, technology mixes, regulations and risk tolerance. In this mature state, the damage caused by breaches is limited and incident response is automated. Importantly, additional controls do not impact experience – they are invisible to users.

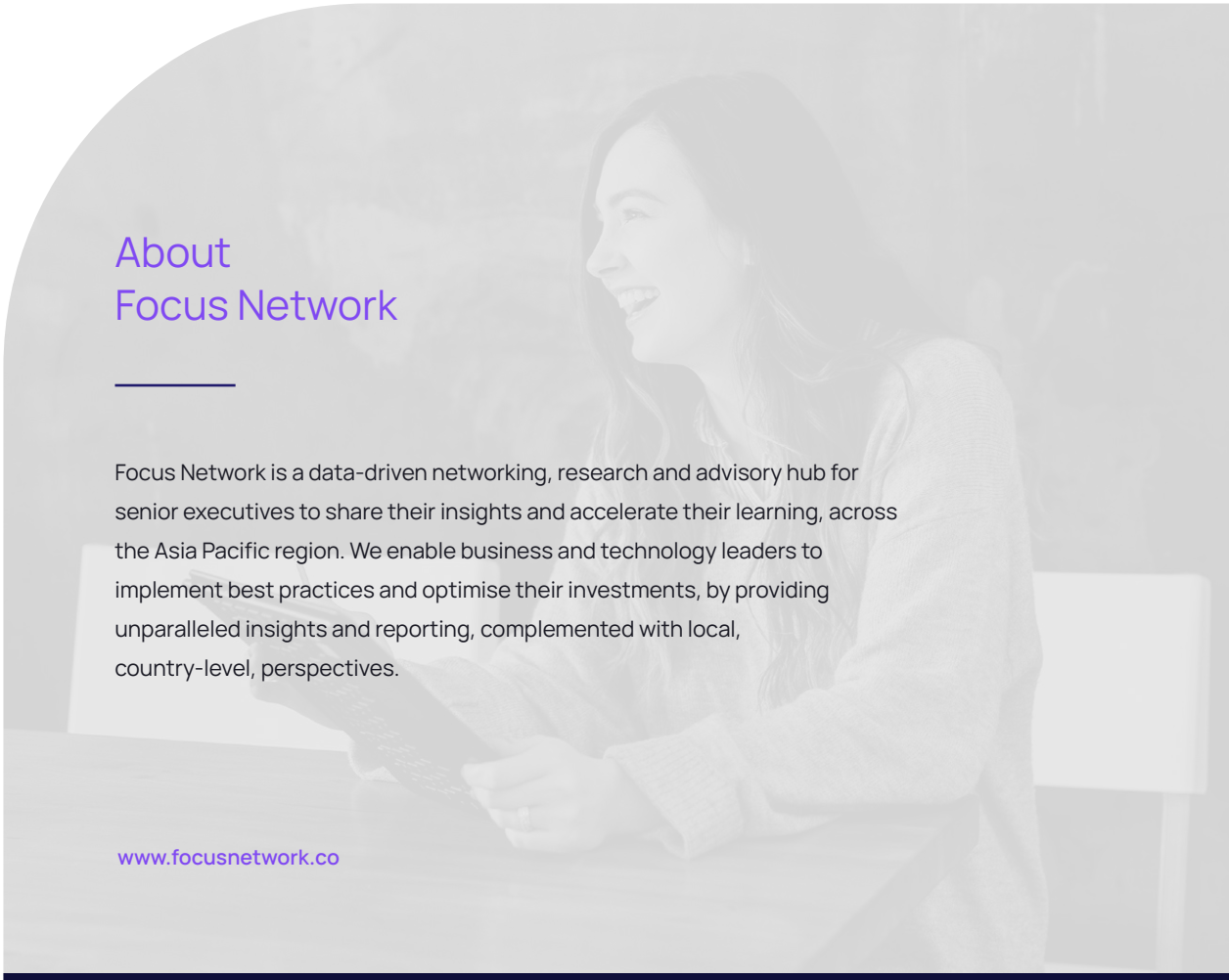
Figure 6 highlights the growing need for a centralised, and scalable approach to cybersecurity where controls are unified and visibility across distributed environments is high.

Figure 6: Growing Need for Centralised, Scalable Approach to Cybersecurity



Progressing on the cyber maturity journey is not easy. Perhaps now is the time, for companies to step back, assess their risks and risk tolerance, assess their current controls, identify the gaps and put people and processes in place that can implement an adaptable posture – aligned with acceptable risk levels and new more distributed technology environments. Cybersecurity technology investments should come after a desired set of cybersecurity policies and processes has been determined. After all, the role of technology is to implement these policies and processes. Too often, companies buy technology reactively when they encounter a threat and pay insufficient attention to policies, people and processes.

Focus Network



About Focus Network

Focus Network is a data-driven networking, research and advisory hub for senior executives to share their insights and accelerate their learning, across the Asia Pacific region. We enable business and technology leaders to implement best practices and optimise their investments, by providing unparalleled insights and reporting, complemented with local, country-level, perspectives.

www.focusnetwork.co

www.focusnetwork.co