State of Secure Networking in Australia: 2024-25

What's inside

Overview

The State of Secure Networking in Australia: 2024-25 report, commissioned by Telstra and Cisco, and proprietary of Moxie Research, offers insights into strategic priorities, business challenges and areas of best practice for small to enterprise-sized organisations.

Research centred on understanding the approach to enhanced employee experience and strengthened security defences in the context of network environments, highlighting the strategies and solutions required to succeed.

The in-depth assessment is based on an outlook of the next 6-12 months, to capture the short- to medium-term objectives of organisations specific to future investment plans, areas of implementation and revised outsourcing requirements.

Methodology

Research was conducted between June to July 2024 and survey respondents included: C-Suite, Executives, Directors and Managers. Company sizes represented within this research includes: Small Business, Mid Market and Enterprise segments. Additional interviews were also conducted across various segments for quantitative insights.

Survey respondents: 351

Location: Australia

Personas*

The following breakdown represents the executives from end-user organisations we surveyed with decision-making capabilities.

- CIO: 31%
- CTO: 22%
- CDO: 9%
- CISO / CSO: 11%
- President: 4%
- Vice President (VP): 2%
- IT Director: 23%
- IT Manager: 27%

*Total is more than 100% as some executives hold multiple positions.

Breakdown by company size (employee headcount)

- 1-200: 26%
- 201-500: 19%
- 501-1000: 33%
- 1001-5000: 17%
- +5000: 5%

Industry Sectors**

- Education: 9%
- Financial Services (Banking, Insurance): 18%
- Government: 6%
- Health: 9%
- Manufacturing: 15%
- Media / Entertainment: 3%
- Mining: 3%
- Oil and Gas: 7%
- Professional Services: 17%
- Real Estate: 6%
- Retail: 10%
- Telco: 4%
- Transport: 4%
- Travel / LeisureUtilities: 4%

**Total is more than 100% as some organisations operate in multiple industries.

01 Executive Summary

Australian businesses are overwhelmed with technological choice yet troubled by rising internal and external threats – a market rich in products yet poor in solutions.

In this era of extreme expectations, notably in the context of rising artificial intelligence (AI) and machine learning (ML) enthusiasm, organisations are being distracted by hype in the pursuit of blind innovation.

While an ‘innovate at all costs’ mindset is progressive, as economic realities and industry dynamics come to the surface, a more pragmatic picture is emerging in businesses across the nation.

Industry trends suggest that transformation is the goal, with its definition shaped by two leading priority statements:

1. Enhancing employee experience
2. Strengthening security defences

Inside Australian businesses, a pressing need exists to evolve future of work[1] strategies in response to changing employee demands[2]. This is a key battleground in which high-performing talent can be won or lost.

Externally, an already volatile threat landscape[3] is worsening with the Australian market now a clear and consistent target[4] for bad actors.

Breaches are becoming more local, more high profile and more frequent. Whether combined or in isolation, these three factors are dominating executive agendas and shaping business priorities in the short- and medium-term.

Building on an in-market partnership[5] of almost 20 years, Telstra and Cisco are here to help organisations transform in Australia.

Employee Experience

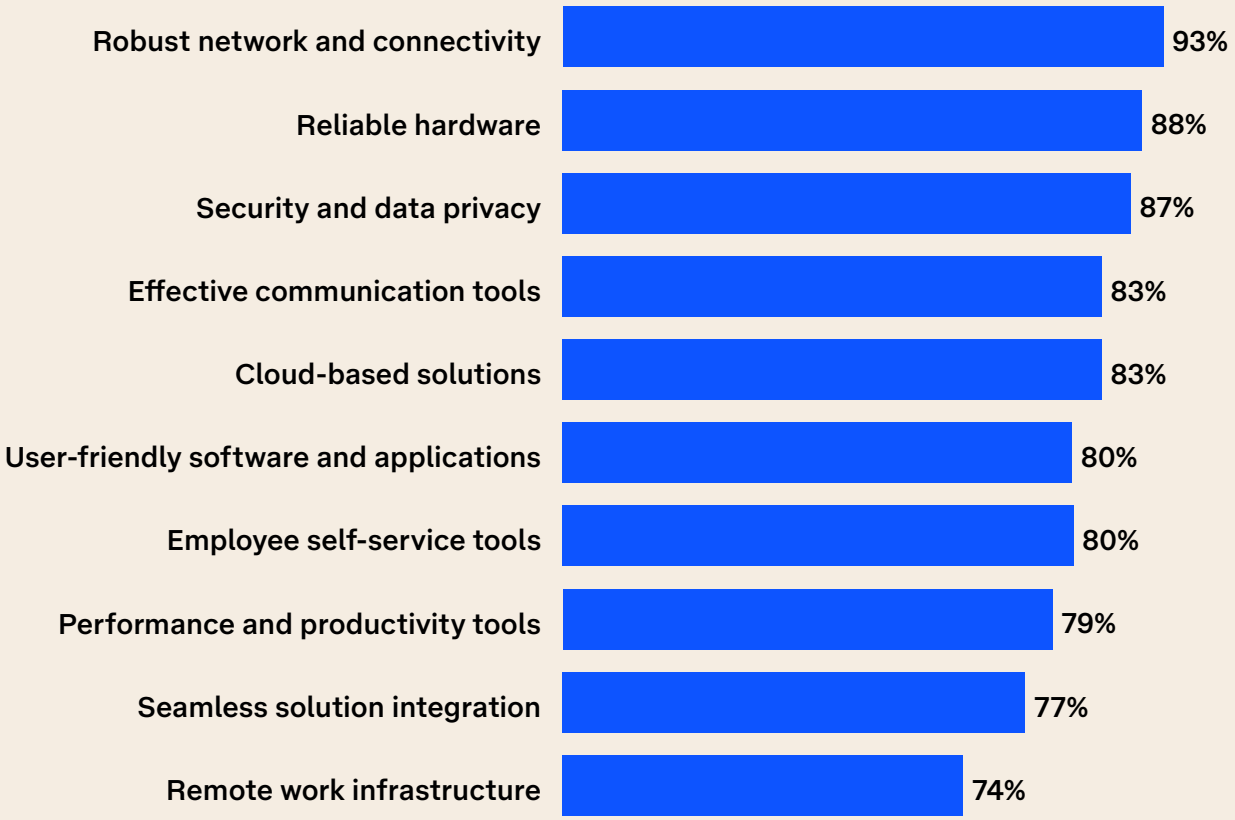
The workforce of today[6] is now more disparate and digital than ever before and hybrid work environments require productivity tools to work smoothly across multiple locations.

Reliable network connectivity and high-speed performance is now considered foundational for a positive employee experience, irrespective of company size. To effectively enhance employee experience levels, 93% of organisations surveyed noted robust network and connectivity as ‘very important’, supported by strong security and data privacy (87%) solutions and frameworks.

1. https://www.webex.com/products/collaboration-ai.html
2. https://www.randstad.com.au/hr-news/workforce-management/what-aussies-want-from-their-bosses-2024/
3. https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/
4. https://ia.acs.org.au/article/2024/ato-cops-4-7m-cyber-attacks-every-month.html
5. https://www.telstrainternational.com/en/telstra-partner-program/alliance-partner-program/telstra-cisco-partnership
6. https://www.telstra.com.au/business-enterprise/news-research/research/technology-evolution-is-powering-employee-and-customer-satisfaction

Question: How important are the following technology considerations in enhancing employee experience within your organisation?

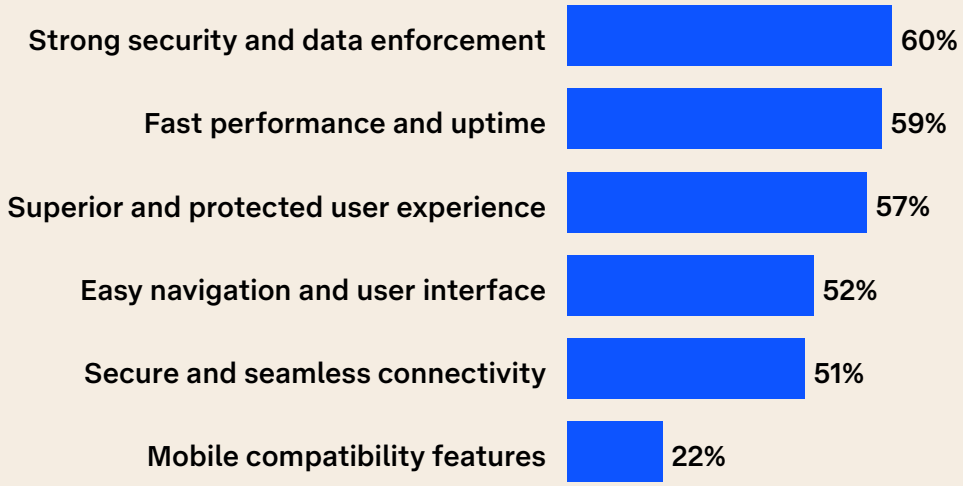
Percentage of businesses that responded ‘Very Important’.



The majority of Australian companies surveyed identified fast performance and uptime (59%) as a critical solution feature in work-related applications, in addition to superior and protected user experience (57%) and secure and seamless connectivity everywhere (51%).

Aligned to a resilient network is demand for strong security and data enforcement (60%) within offerings, in recognition that businesses must strike a balance between enhancing employee experience while bolstering security defences.

Question: Which solutions features are most critical in work-related applications?



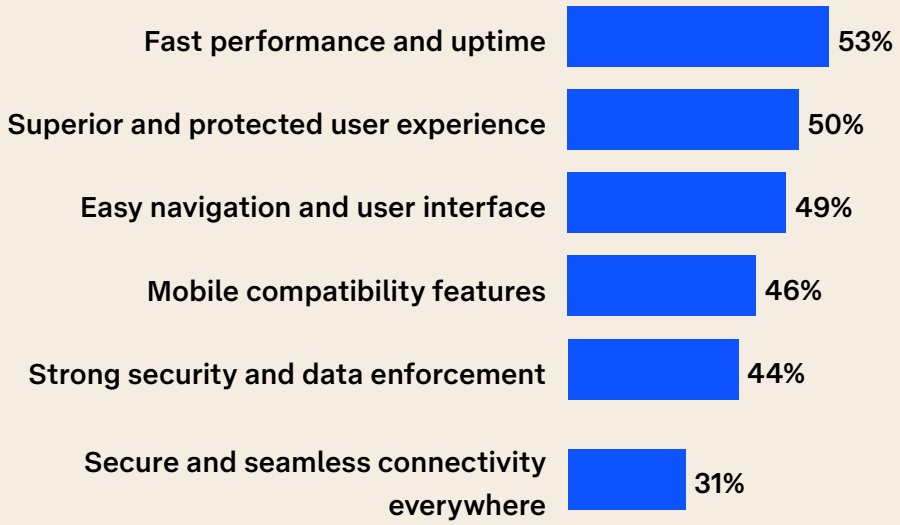
In Australia, the percentage of organisations with ‘Average’ or ‘Weak’ networking infrastructure that currently supports mobile and remote workforces is concerning.

Despite acknowledging the ingredients required to respond to an increasingly digital workforce[7], organisations remain hindered by an inability to modernise infrastructure environments. A disconnect exists between the priority of experience and the reality of out-dated technology.

7. https://www.telstra.com.au/business-enterprise/news-research/research/technology-evolution-is-powering-employee-and-customer-satisfaction

Question: Rate how well your networking infrastructure supports mobile and remote workforces from a technology standpoint.

Percentage of businesses that responded ‘Average’ or ‘Weak’.



The change in user experience

The rise of AI-powered video platforms[8] is also helping to redefine employee expectations and user experience. For example, audio, language and video intelligence features help remove noise, offer real-time translations and utilise immersive sharing.

Businesses are prioritising improved in-office hybrid work environments to create more consistent and frictionless employee and guest experiences[9], while also more effectively utilising workspace.

The optimised office requires improved network performance to support advanced collaboration technologies, underpinned by enhanced security and access across more locations for employees. This is creating heightened platform demand for Cisco Meraki[10] and Cisco Catalyst[11] switches, wireless and sensor products, as well as the utilisation of Cisco Duo[12] and Cisco Umbrella[13] offerings, delivered via a Telstra team of Cisco-accredited professionals in Australia.

8. https://www.webex.com/products/collaboration-ai.html.
9. https://blogs.cisco.com/government/ai-and-hybrid-work-for-a-frictionless-experience-and-citizen-engagement
10. https://meraki.cisco.com/
11. https://www.cisco.com/site/au/en/products/networking/switches/index.html
12. https://duo.com/
13. https://umbrella.cisco.com/

As reported by Cisco, business benefits include 60% lower zero-trust total cost of ownership (TCO) for improved and more effective security and 65% lower cost of connectivity for reduced OpEx investment. Plus, 59% faster on-boarding of services to deliver faster time to value. Through this platform approach, organisations are also achieving extended benefits from a quality and comfort perspective.

Cisco further reported that environmental wellness is a critical factor in employee experience strategies, with businesses reducing energy costs by 22% and TCO by 25%. Better staffing is another upside with 65% of job candidates preferring organisations with robust environmental policies.

Strengthening Security

According to the Annual Cyber Threat Report 2022–23[14], developed by the Australian Signals Directorate (ASD), both state and non-state actors continue to show the intent and capability to compromise Australia's networks. As reported, during the 2022-23 financial year, the ASD notified 158 entities of ransomware activity on their corporate networks, representing an approximate increase of 7% compared to 148 during the previous year.

The Australian Protective Domain Name System blocked over 67 million malicious domain requests (up 176%) while the Domain Takedown Service blocked more than 127,000 attacks against Australian servers (up 336%)[15].

No organisation is immune with almost 94,000 cyber crime reports recorded (up 23%) within the 12-month period across small, medium and large businesses.

14. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy
15. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

According to Moxie Research, the three most common types of cyber attacks targeting the network in Australian businesses are malware (56%), phishing (50%) and ransomware (32%).

Based on the businesses surveyed, the potential consequence of a successful cyber security breach on the network is the loss of sensitive data (56%). This is followed by reputational damage (47%), financial loss (45%) and operational downtime (45%).

Question: What would be the potential consequences of a successful cyber security breach on the network in your organisation?

Rank	Technology	
1	Loss of sensitive data	56%
2	Reputational damage	47%
3	Operational downtime	45%
4	Financial loss	45%
5	Intellectual property (IT) theft	34%
6	Regulatory non-compliance	33%
7	Legal liabilities	32%
8	Customer dissatisfaction	20%

Notably, the cost of being unprepared can be substantial. In the 2024 Cisco Cybersecurity Readiness Index[16], 53% of Australian businesses reported that they recently experienced a cyber security incident outlining the expense at a minimum of $300,000 in USD.

16. https://news-blogs.cisco.com/apjc/2024/04/10/cri2024/

It’s unsurprising that the primary investment drivers in secure networking technologies centre around the need for improved security. Businesses surveyed, reported the following (in order of priority) as key factors when investing and selecting a secure networking solution.

1. Data Protection and privacy
2. Risk management
3. Cost savings
4. Regulatory compliance
5. Competitive advantage
6. Business continuity
7. Employee productivity
8. Threat landscape response.

Security is at the heart of the Telstra and Cisco's joint go-to-market strategy, with both prioritising a robust network infrastructure to protect company data.

As one of Australia's largest critical infrastructure providers, Telstra constantly evolves core network management capabilities to deliver high levels of security, resilience and data sovereignty.

Cisco platforms, leveraged by Telstra's technologies, applications, networks and solutions, act as one to deliver 60% time savings on security issue resolutions and 59% time savings on configuration compliance checks.

A Cisco Validated Framework is employed to enable technical solution clarity along with the availability of just-in-time design and deployment documentation to deliver integrated multi-layered security from the core to the edge.

With AI-powered zero-trust network access policies, every connection point is fortified with zero-trust security to better protect people, places and things. Agile, secure networking infrastructure minimises risk, closes security gaps and defends against evolving threats, enabling comprehensive protection.

Through Cisco solutions, Australian organisations are deploying common security policy that spans all network domains, including offices, industrial facilities, remote users, data centres and public clouds.

Supporting this is consistent enforcement so that connections between a user and an application is protected. Such enforcement includes through native firewall capabilities distributed throughout the secure networking infrastructure.

02 Business Barriers

As a digitally advanced nation, corporate consensus exists that Australia is not exempt from the threat of cyber attacks and data breaches, but the ability of businesses to mitigate such risk effectively remains highly questionable.

According to the 2024 Cisco Cybersecurity Readiness Index[17], less than 1% of Australian organisations are at the ‘Mature’ stage of readiness in responding to modern cyber security risks. Declining in maturity, 18% are at the ‘Progressive’ stage, 62% are ‘Formative’ and 19% are ‘Beginners’.

17. https://news-blogs.cisco.com/apjc/2024/04/10/cri2024/

Network Challenges

According to Moxie Research, 54% of businesses surveyed would consider their own third-party risk management capabilities to be ‘Average’ or ‘Weak’, when asked to rate the cyber security capabilities of their internal network.

This is compounded further by a lack of investment in secure networking technologies (51%) and a failure to implement stringent governance, risk and compliance (GRC) protocols (47%).

Businesses also reported a lack of executive leadership and board involvement (52%) and an inability to keep pace with regulatory compliance (43%) in specific industry sectors.

Whether in isolation or combined, such negative assessments of network cyber capabilities suggests that it’s commonplace for fragile frameworks to surround the corporate network among companies in Australia.

This extends into the technical environments also, with businesses noting the most pressing challenges facing organisations seeking to secure the network centred around (in order of relevance) data protection and privacy (47%), cloud security (43%) and network visibility (33%).

Data protection, within network environments, faces several complex challenges, including unauthorised access and issues related to managing user permissions, implementing multi-factor authentication (MFA) and secure network access points.

Protecting data stored in the cloud presents additional challenges, whether due to a lack of stringent standards or a failure to secure information passed between multi-cloud locations.

This is worsened by ongoing visibility obstacles preventing organisations from assessing and controlling all activities on a network. A new level of troubleshooting and monitoring is required as full-stack observability[18] emerges as a key organisational consideration.

18. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m06/cisco-and-splunk-launch-integrated-full-stack-observability-experience-for-the-enterprise.html

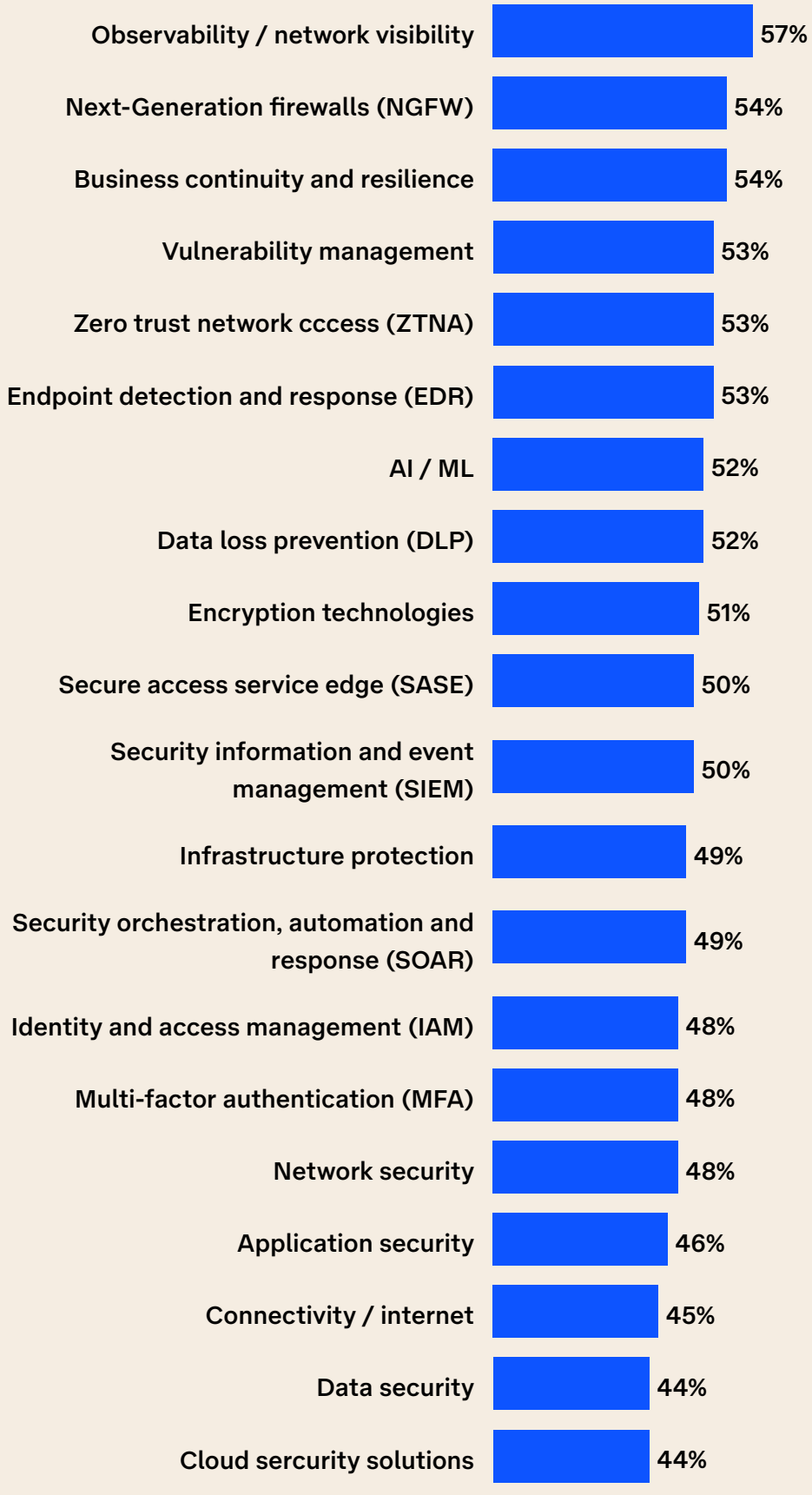
Question: Rank the top technology challenges your organisation faces when securing network environments?

Rank	Technology	
1	Data protection and privacy	47%
2	Cloud security	43%
3	Network visibility	33%
4	Incident detection and response	28%
5	Zero trust security	27%
6	Legacy systems	27%

On page 19 is a comprehensive self-assessment from Australian organisations surveyed highlighting the areas of improvement required to bolster cyber security capabilities in their network.

Question: From a technology standpoint, rate the cyber security capabilities of your network?

Percentage of businesses that responded ‘Average or Weak’.



Product Overload

In many instances, the desire by organisations to urgently strengthen security environments has resulted in an overload of point solutions.

While the exact number is unknown, it is estimated that there are more than 3,900 cyber security vendors[19] within the Australian market today, each armed with competitive pricing and compelling narratives.

According to the 2024 Cisco Cybersecurity Readiness Index[20], 66% of Australian organisations have deployed 10 or more point solutions in their security stacks. And, for almost a quarter of those businesses (22%), the number is far higher at 30 or more.

Yet this approach is creating new obstacles linked to increased complexity and integration which in turn is exposing gaps within network environments. This is reflected in Moxie Research findings, with 85% respondents in strong agreement that having multiple security vendor products will create additional risk and exposure.

Beyond that, inconsistent policies and procedures serve only to create added operational challenges, as identified by 81% of businesses surveyed.

Even though price isn't a primary factor in securing network environments, the unnecessary spike in costs from running siloed products cannot be ignored. For 87% of organisations surveyed, an increase in project costs is driving a company-wide need for product consolidation.

In response, companies noted that they are prioritising investments in integrated platforms to better connect the cyber dots internally as performance and scale become mission-critical.

The value of adopting a platform approach to address IT complexity, enhance user experience and strengthen cyber security is now evident in Australia.

Too many disconnected tools create complexity and inefficient operations, worsened by increased business risk and a distinct lack of agility and innovation.

19. https://it-harvest.com/
20. https://news-blogs.cisco.com/apjc/2024/04/10/cri2024/

As highly distributed users connect to highly distributed applications, data and resources, only modernised network security solutions can protect organisations against cyber threats.

Cisco and Telstra have a long history in driving innovation in networking with both prioritising a robust network infrastructure to protect company data.

As one of Australia's largest critical infrastructure providers, Telstra constantly evolves core network management capabilities to deliver high levels of security, resilience and data sovereignty.

Cisco platforms, leveraged by Telstra's technologies, applications, networks and solutions, act as one to deliver 60% time savings on security issue resolutions and 59% time savings on configuration compliance checks.

Through Cisco solutions, Australian organisations are deploying common security policy that spans all network domains, including offices, industrial facilities, remote users, data centres and public clouds.

Supporting this is consistent enforcement so that connections between a user and an application is protected.

Through the power of Telstra and Cisco, simplify, streamline and secure your network, and improve your business performance.

03

Tech Transformation

The product overload problem statement is adding credibility to a platform approach anchored in a need to remove inefficiencies and complexities. And businesses still grappling with point solutions now acknowledge the power of a network platform in delivering more consistent architecture.

So much so that 72% of IT leaders surveyed in the 2024 Global Networking Trends Report[21] expect to have a platform architecture in place across one or more networking domains within the next two years.

In Australia, consolidation and centralisation is happening across campus, branch, WAN, data centre and multi-cloud domains.

According to IDC[22], a network platform is an integrated system that combines hardware, software, policy and open APIs with an intuitive user interface, advanced telemetry and automation. Desired corporate outcomes include faster innovation, improved performance, strengthened security and cost savings.

21. https://www.cisco.com/c/en/us/solutions/enterprise-networks/global-networking-trends.html
22. https://blogs.cisco.com/networking/achieving-operational-simplicity-with-a-network-platform-approach

Secure networking solutions from Cisco[23] use common policy and distributed enforcement to connect campus and branch locations—irrespective of application, environment or network.

Unifying fragmented IT and end-user experiences in the pursuit of a platform strategy to better secure networking infrastructure requires:

- Top-tier SD-WAN and cloud security platforms
- Exte nsive security integrations across SD-WAN and cloud
- Flexibility through unified and integrated SASE options.

Guidance outlined via IDC Analyst Connection[24] (in partnership with Cisco) recommends an extensibility assessment as the first step to get started when building a comprehensive network platform strategy. This type of assessment gives organisations an understanding of a understand a platform's ability to: unify management, visibility and assurance across networking domains over time. This is in addition to its ability to add new services and integrate across other IT systems through open APIs.

From a business perspective, ensuring the platform can support the company's IT strategy is critical across on-premises, cloud and hybrid management. Then it's about aligning IT capabilities with business needs across all departments in your organisation, deploying a platform that can effectively break down these silos, all through a unified approach.

23. https://www.cisco.com/site/us/en/solutions/transform-infrastructure/secure-networking-overview.html
24. https://www.cisco.com/c/dam/en/us/solutions/transform-infrastructure/idc-network-platform-approach-paper.pdf

AI Advantage

When assessing business and technology priorities, IT business leaders surveyed continue to evaluate the promise and potential of AI.

Key to ongoing success is the ability for businesses to move this technology from industry buzzword to business use case status. Based on Moxie Research insights and industry understanding, this process is already underway.

Businesses surveyed noted that AI ranks as the leading solution deployment priority for 43% of organisations during the next 6-12 months. To drive such widespread adoption, IT executives (specifically CIOs) have identified that they are adopting two core roles within the business.

Firstly, for 67% of IT executives, they are assuming the position of a ‘strategist persona’ to collaborate more closely with the wider company to align IT strategies to key business objectives. Secondly, 42% of IT executives are embracing an ‘innovator persona’ to spearhead transformative change within the business as a leading figure of disruption.

Specific to generative AI (GenAI), 76% of businesses surveyed believe this will have a ‘Positive Impact’ on profitability, as well as customer satisfaction (67%) and employee productivity (65%). Further noting other key benefits including gains in revenue (64%) and market share (58%).

Such strong AI sentiment is also evident in the network, with IT leaders utilising the technology to enhance applications, automate operations, enforce policy, strengthen security and assure digital resilience.

According to the 2024 Global Networking Trends Report[25], more than 95% of IT leaders surveyed, noted that their current IT teams are not equipped to deliver the innovations required to help steer business strategy, satisfy customers and optimise operations. Further, the report noted that primary motivators for businesses using AI include the following use cases: to simplify operations, automate complex tasks and accelerate the remediation of performance issues.

25. https://www.cisco.com/c/en/us/solutions/enterprise-networks/global-networking-trends.html

Looking ahead, 60% of businesses surveyed expect to have AI-enabled predictive network automation in place within the next two years. And during this time period, organisations surveyed are also looking to ensure AI-enabled innovation will extend to SASE cloud architecture (54%) and endpoint recognition and policy management (51%).

The common consensus among companies is that future success will centre on automation powered by AI. And using AI to achieve efficiency from an operational standpoint, will allow businesses to redirect IT investment into revenue-generating projects. According to Gartner, overall, IT spend in Australia continues to experience sustained single-digit growth year-on-year from $124 billion in 2023 at an annual increase of 6.4% to $133 billion in 2024, up 7.8% (value in AUD)[26].

26. https://www.gartner.com/en/newsroom/press-releases/2023-09-12-gartner-forecasts-it-spending-in-australia-to-grow-in-2024

04

Strategic Guidance

Specific to security and risk management, business appetite for investment is holding higher at double-digit growth numbers. In Australia, spending on this segment alone totalled $6.6 billion in 2023 and $7.3 billion in 2024, increasing 12.4% and 11.5% year-on-year respectively[27].

Healthy appetite for protection, modernisation and transformation is forecast to remain in 2025, according to Gartner[28]. Dovetailed with Australian data extracted from the 2024 Cisco Cybersecurity Readiness Index[29], nearly half of companies (42%) are planning to significantly upgrade IT infrastructure environments within the next 12-24 months.

Almost every business leader surveyed (97%) expect to increase budget for cyber security initiatives during the year ahead, with the majority (85%) preparing for an increase of 10% or more. Further, most plan to upgrade existing solutions (59%), deploy new solutions (54%) and invest in AI-driven technologies (43%).

27. https://www.gartner.com/en/newsroom/press-releases/2023-09-12-gartner-forecasts-it-spending-in-australia-to-grow-in-2024
28. https://www.gartner.com/en/newsroom/press-releases/2023-09-12-gartner-forecasts-it-spending-in-australia-to-grow-in-2024
29. https://news-blogs.cisco.com/apjc/2024/04/10/cri2024/

Strengthening businesses through secure networking

"The threat landscape will always evolve which is why visibility is crucial for organisations. Creating strong security posture as an organisation – and passing that discipline onto users – is fundamental in responding to the rise in cyber attacks across Australia.

We're seeing increased demand for network and security solutions because this is now a boardroom conversation. Bringing these two core offerings together will also help overcome product overload, which is a top priority for companies now focusing on a platform approach.

Businesses continue to remain at different stages of maturity however and our role at Cisco is to support organisations on that journey, alongside our strategic partner channel with Telstra."

Rodney Hamill
Managing Director, Partner and Routes to Market Sales (Australia and New Zealand), Cisco

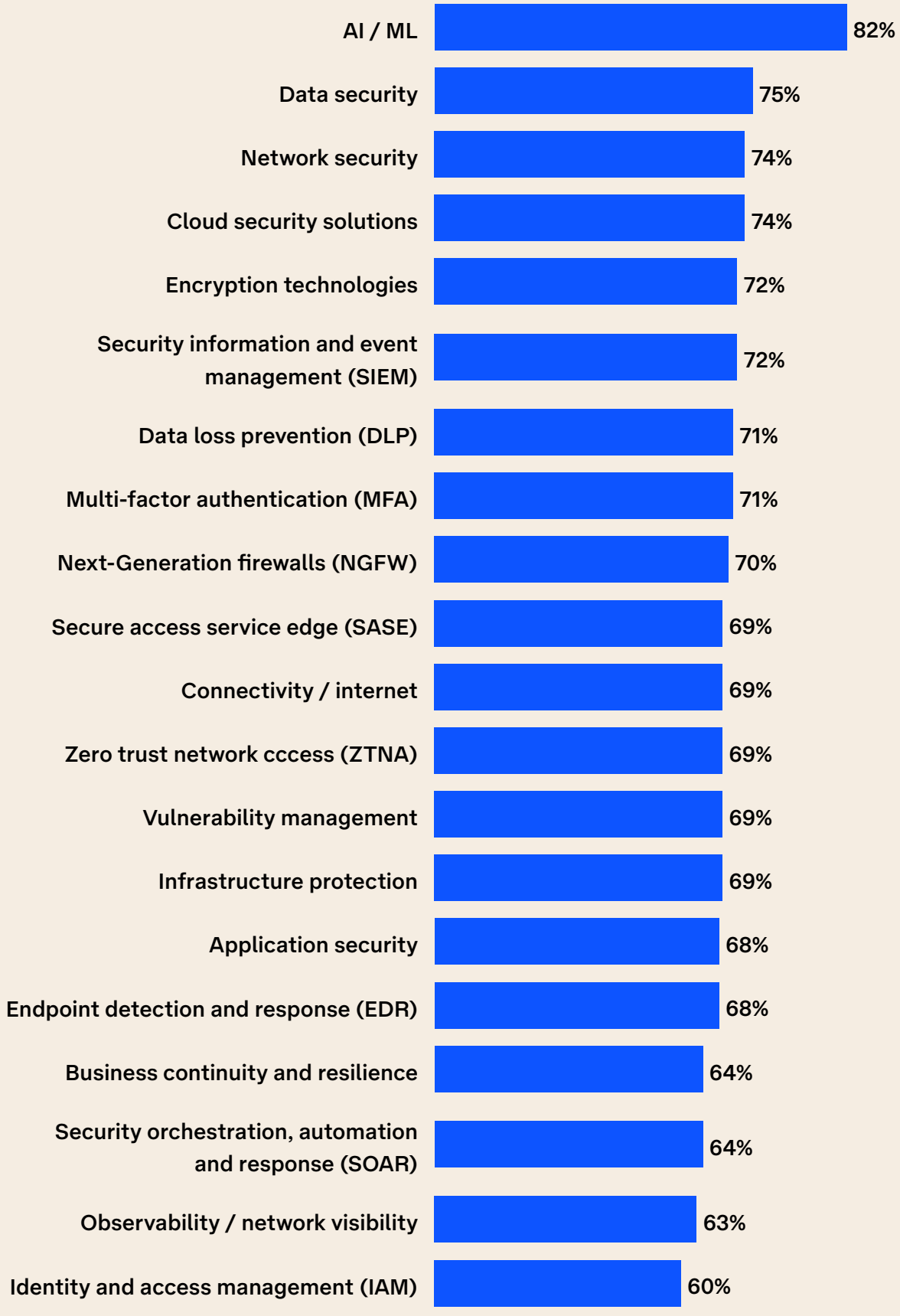
Drilling into imminent investment in secure networking technologies, findings from Moxie Research endorse the view that enhancing employee experience and strengthening security defences are driving purchasing decisions.

In a hybrid world, organisations are prioritising visibility and control over encrypted traffic to prevent unprecedented attacks and respond to sophisticated threats across networks, clouds, applications, users and endpoints.

Notably, AI and ML are viewed as critical in strengthening networking resiliency and security through intelligent operations and integrations.

Question: Which secure networking technologies are you planning to invest in within the next 12 months?

Percentage of businesses that responded ‘Increased Investment’.



Secure networking solutions embedded with advanced AI and ML techniques have the capability to empower IT operations teams with actionable intelligence based on historical and real-time network performance data and enhanced by predictive models that improve over time.

With increased networking solution investment on the agenda, businesses are seeking to define smarter segmentation policies, create custom alerts to detect unauthorised access and ensure compliance.

Visibility and threat detection across on-premise networks and all major public cloud platforms is once again of paramount importance, evident through a commitment to increase spending on data, network and cloud solutions.

The rise of SASE[30] is also showing no signs of slowing down in Australia, primarily motivated by an organisational desire to streamline and simplify the delivery of critical network and security services via the cloud.

According to Gartner[31], such demand for SASE solutions triggered an 11.5% swing in data centre spending locally, posting 5.1% growth at $4.3 billion in 2023 compared to a decline of 6.4% in 2022 (at $4.1 billion).

Ecosystem Value

Business leaders surveyed noted improved network visibility (52%) and reduced security incidents (50%) as the leading metrics for organisations when measuring the return on investment (ROI) of secure networking technologies. This is aligned to the logic that to stop a breach of the network, businesses must first be able to identify and examine any incoming threats. Benefits must extend beyond top-line requirements however, specifically in the areas of improved regulatory compliance (42%) and enhanced user productivity (41%).

The upgrade of ageing legacy systems (36%) will be an inevitable but welcomed secondary result, alongside augmented threat detection and response capabilities (35%).

Interestingly, only 31% of businesses surveyed consider cost savings and budget benefits as a primary ROI metric. Again, the priority remains centred on securing the organisation while empowering employees within it.

30. https://moxie-insights.com/market/australian-spending-pendulum-swings-back-in-data-centre-direction/
31. https://www.gartner.com/en/newsroom/press-releases/2023-09-12-gartner-forecasts-it-spending-in-australia-to-grow-in-2024

With the unifying of network and security takes centre stage, businesses are turning to technology ecosystems to overcome implementation obstacles. When deploying secure networking solutions, the biggest barriers to effective utilisation are:

1. Lack of skilled personnel
2. Rapidly evolving threats
3. Complexity of integration
4. Lack of a strategic outsourcing partner.

This highlights the importance of finding trusted advisors to partner with when executing secure networking strategies.

Seventy-two percent of businesses surveyed, are committed to outsourcing more projects to strategic partners in the area of cyber security. With reliance on third-party expertise expected to accelerate during the next 6-12 months (inclusive of the roll-out of tailored managed security services).

In order of significance, the most important factors for organisations when selecting a secure networking technology partner include:

1. Deep cyber and networking skills in specific industry sector
2. Collaborative approach and flexible contracts
3. Deep skills in cyber and networking solutions
4. Easy to engage / do business with
5. Ability to provide end-to-end cyber and networking solutions.

Partnering to succeed in secure networking

"A huge amount of opportunity exists in the secure networking market for Australian organisations to capitalise on.

There's a plethora of choice for businesses in terms of what technology they use, how they approach strategy and who they receive advice from. The Telstra and Cisco ecosystem is strongly positioned to have those types of conversations especially through our accredited Partner network, who have strong and trusted relationships across our customer base.

Our channel houses a specialised network of partners who possess the skills and expertise required to build market-leading secure networking blueprints.

Capabilities extend beyond core networking, IT and mobility environments into new areas of priority and focus for organisations – enhancing employee experience and strengthening security defences.

Our partners are taking a lead role in guiding organisations on this secure networking journey."

Peggy Renders
Chief Customer Officer,
Telstra Enterprise

05 Key Takeaways

1. Adopt a platform approach

Ensure all solutions in your security stack are integrated and optimised for maximum impact, removing reliance on isolated point products.

2. Embrace AI features

Empower your IT operations teams with actionable intelligence and predictive models that can improve threat detection and response.

3. Gain network visibility

Better understand the threat landscape across network, cloud, infrastructure and data environments. Leverage full-stack observability features to increase visibility and control to prevent attacks and respond in real-time through advanced analytics.

4. Prioritise robust connectivity

Focus on fast performance and uptime to avoid compromising on employee experience to enable secure and smooth connectivity when using work-related applications.

5. Leverage strategic expertise

Collaborate with skilled partners to utilise deep solution and sector knowledge while overcoming a lack of skilled personnel in-house.

For more information on how Telstra and Cisco can help your business, please contact us today.

13 22 53 business.care@team.telstra.com