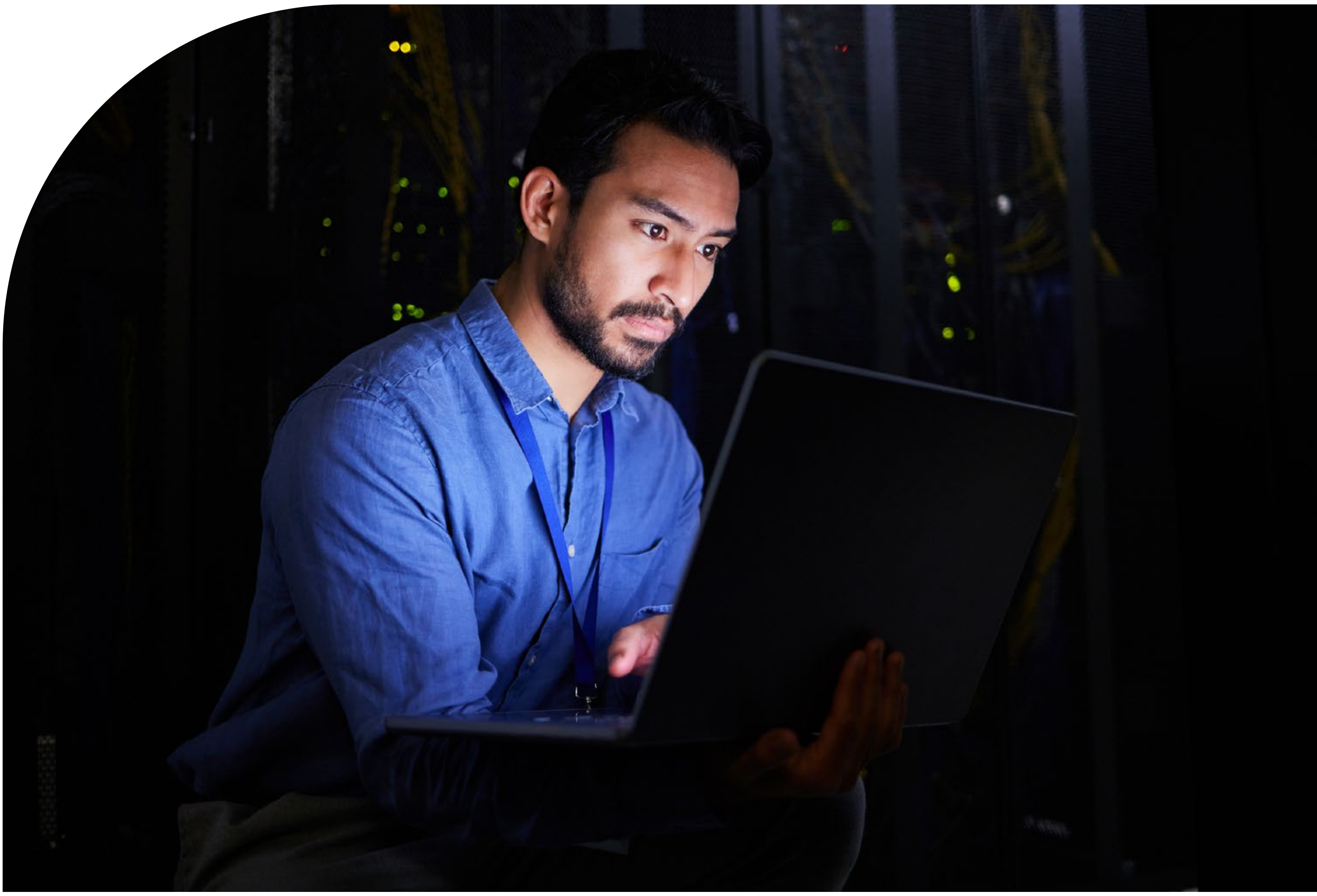
Maximising the Value of Cybersecurity Investments

Andrew Milroy
Vice President and
Head of Research,
Focus Network

October 2023

www.focusnetwork.co

Table of Contents



Executive Summary

Increased economic uncertainty is placing growing pressure on cybersecurity budgets. Despite an increase in the frequency and impact of attacks, combatting them is becoming progressively more challenging, with declining or stagnant cybersecurity budgets.

Companies often respond to threats in a reactive manner — adding additional cybersecurity processes and tools, to address newly discovered attack types and vectors. This approach is not working. It is making the situation worse. According to Focus Network, Australian companies have, on average, 36 cybersecurity tools, creating a huge amount of complexity. These tools often operate in silos requiring different skill sets to manage them.

Increasingly cybersecurity leaders need to demonstrate a return on cybersecurity investments and increase productivity. This requires a reduction in the number of tools and a focus on efficiency by:

Reducing the workloads on security operations centres by decreasing the number of alerts and false positives. This can be achieved by focussing on security incidents over alerts by correlating and contextualising large numbers of alerts into fewer incidents and campaigns.

Lowering the amount of time and the number of tools required for basic cybersecurity hygiene such as vulnerability management, secure configuration assessment, patch management.

Reducing remediation times, detection times, and missed detections.

In addition to increasing efficiency and reducing complexity, CISOs need to demonstrate their success, to gain support across their organisations. Obtaining this support and keeping budgets in line with cybersecurity risk, requires them to communicate much more effectively with the rest of the business and provide them with metrics that make sense to them, and relate to the business, as a whole.

This white paper will focus on the need to maximise security investments and highlight:

- The constraints on cybersecurity investments.
- The need to increase productivity with a renewed focus on cyber hygiene, security process automation and consolidation.
- Alignment of security outcomes with business outcomes and goals.
- Key metrics for maximising the value of cybersecurity investments.

Cybersecurity Investment Constraints

In the face of economic turmoil, businesses are facing the dual challenges of stagnating cybersecurity budgets and escalating, and increasingly complex threats. For years, cybersecurity budgets increased. Today, budget is the leading constraint to cybersecurity investments. Indeed, nearly 80% of Australian cybersecurity leaders cite budget and cost issues as their major cybersecurity investment constraint with just over 60% indicating that their cybersecurity budgets will be flat, or decline over the next year.

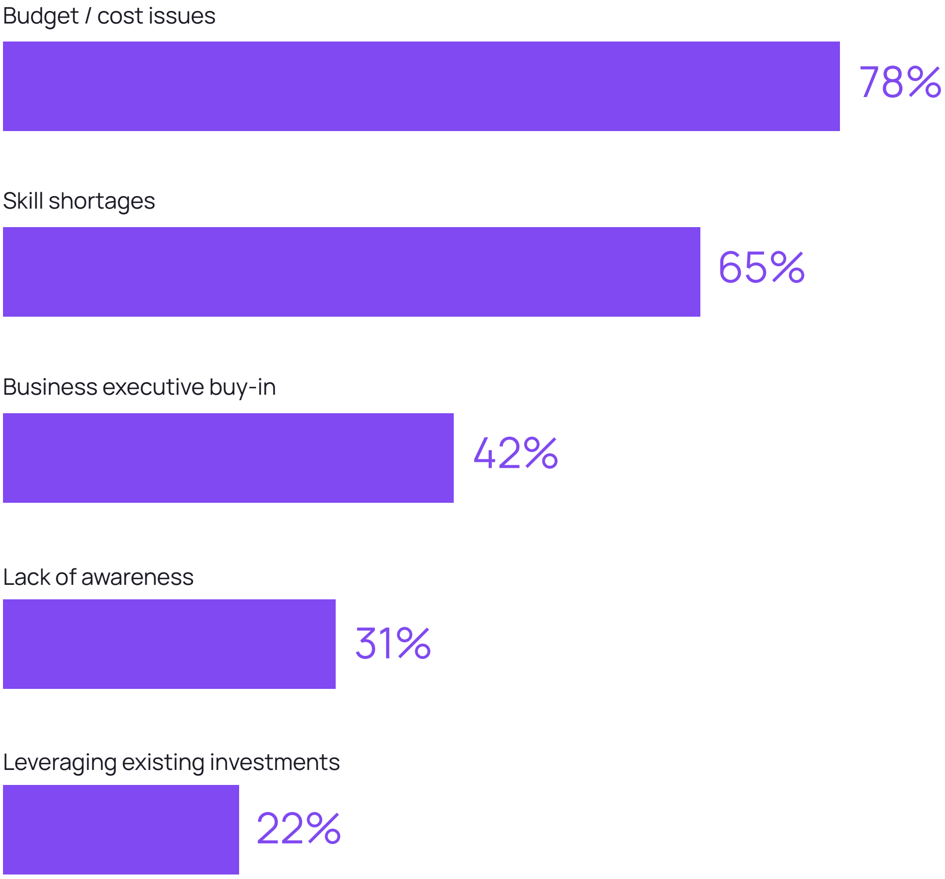
Cybersecurity skills shortages remain acute in Australia — making the implementation and management of cybersecurity processes and tools, a major challenge. Gaining executive buy-in is also problematic as business leaders and the C-suite increasingly need to understand the business value of cybersecurity investments — and request metrics which illustrate the benefits of cybersecurity controls.

A lack of awareness of the frequency and potential impact of cybersecurity breaches on organisations makes it difficult to allocate adequate resources to cybersecurity controls. Metrics which illustrate the importance of cybersecurity — and the impact of controls — need to be shared widely within the organisation.

Substantial investments have already been made in cybersecurity and, for many, the returns have not been visible or commensurate. At the same time, there is increasing pressure to extract more benefit from existing cybersecurity investments.

Figure 1 illustrates the leading cybersecurity investment constraints for Australian organisations. Respondents gave multiple responses.

Leading Cybersecurity Investment Constraints



N=320
Australian Cybersecurity Survey, 2023

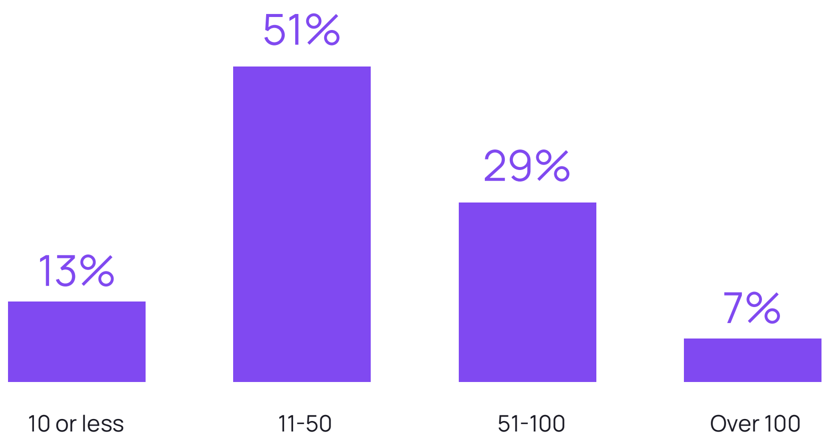
Increasing Productivity with Focus on Cyber Hygiene, Security Process Automation and Consolidation

Australian companies have typically made substantial investments in cybersecurity, over several years, and are now under pressure to show an increase in returns and tangible business value/ outcomes for those investments. One major issue is the number of cybersecurity tools being used today. On average, Australian companies are using 36 separate cybersecurity tools which creates additional complexity and new vulnerabilities. 87% of Australian organisation have more than ten separate cybersecurity tools. This cybersecurity tool sprawl makes increases in operational efficiency and effectiveness, particularly challenging.

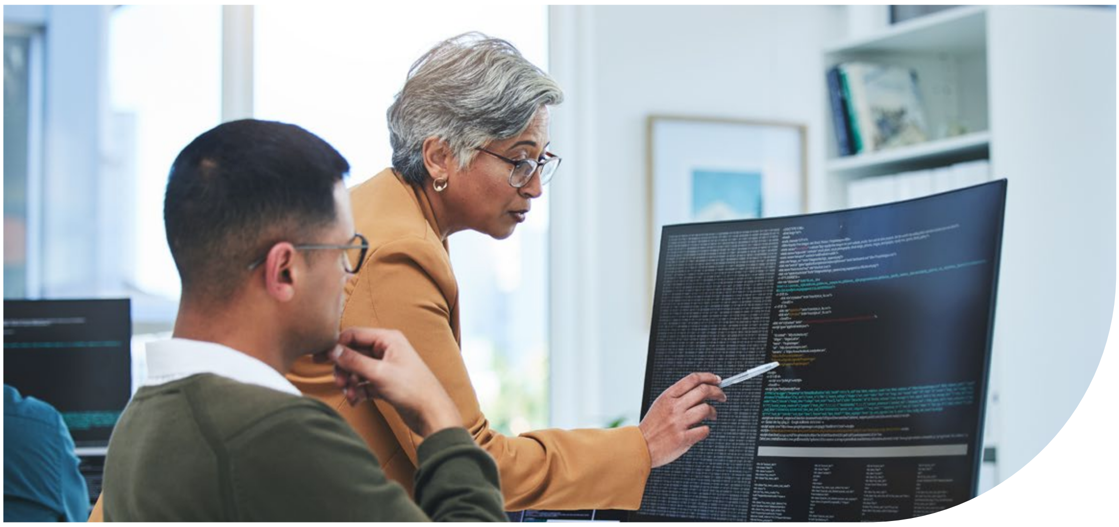
Too many cybersecurity tools are also a major challenge for companies because data sits in silos and is not effectively integrated. Visibility across assets is impaired by multiple dashboards sharing differing metrics and manual correlation or stitching of data points which is also prone to human errors.

Figure 2 shows the number of cybersecurity tools used by Australian organisations.

Figure 2: Number of Cybersecurity Tools Used



N=320
Australian Cybersecurity Survey, 2023



Australian companies are addressing these challenges by streamlining their cybersecurity policies and procedures and consolidating their cybersecurity platforms. 37% of Australian companies cite reducing complexity and improving visibility as leading cybersecurity initiatives over the next year.

Increased automation, particularly around threat detection and response is also a key cybersecurity initiative over the next year, with 35% of Australian organisations intending to place more emphasis on automated detection and response. Alert fatigue, and slow labour-intensive, security operations, are driving greater automation, as companies seek to detect attacks and respond to attacks more rapidly, while reducing false positives and missed detections.

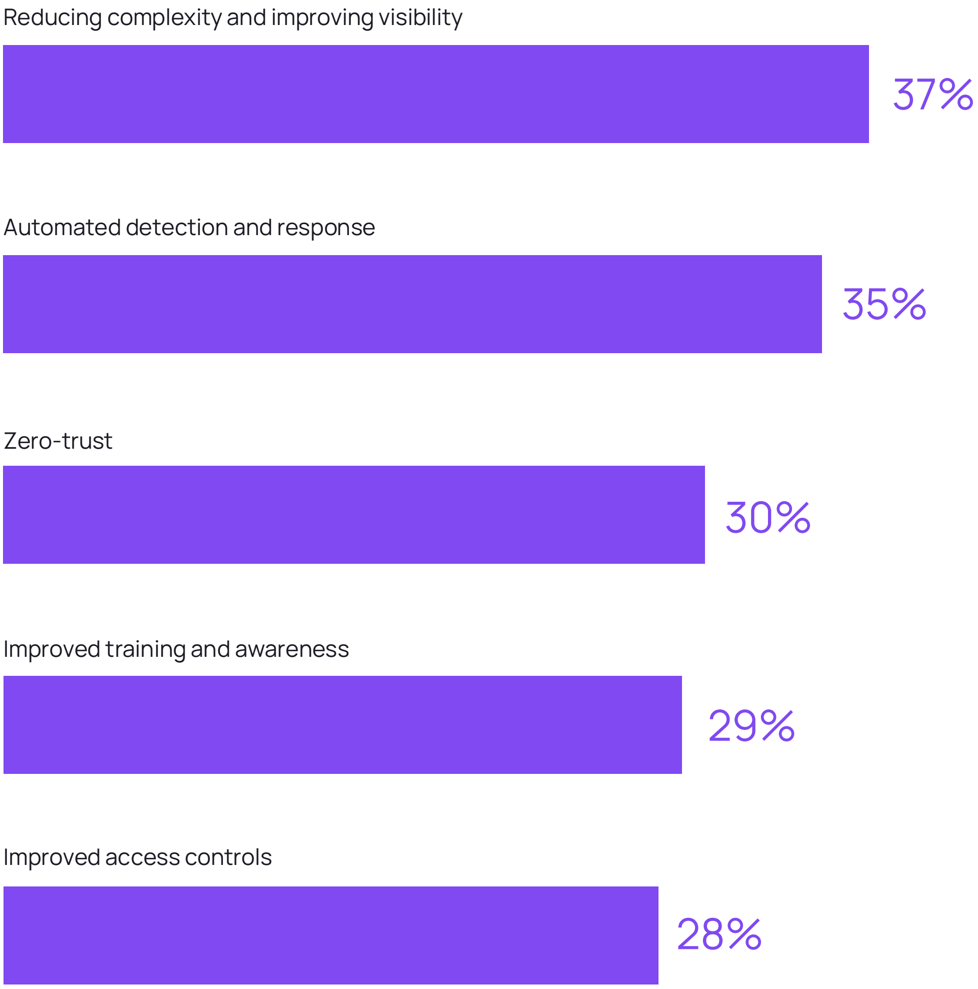
The concept of taking a zero-trust approach to cybersecurity is not new. It has been used heavily in the marketing material of leading cybersecurity vendors for several years as well as being promoted by regulators and advisory bodies. Australian companies are now widely implementing zero-trust policies and tools. It is a leading initiative for 30% of Australian organisations. They are taking an 'assume breach' approach and placing controls in place that treat all system and network traffic as potentially malicious.

Renewed emphasis is being placed on ensuring that cybersecurity policies are linked to risk appetite and that basic cyber hygiene such as patch management, vulnerability scanning, access management and training are addressed. Increased cybersecurity spending is not equal to decreased cybersecurity risk. Basic cyber hygiene must be followed if cybersecurity technology is to be effective in delivering value. Breaches caused by low cybersecurity awareness are increasing, despite efforts to improve training programs and awareness. Renewed focus needs to be placed on training and awareness. Nearly 30% of Australian companies plan to invest more in improved training and awareness over the next year.

Improper or unauthorised access to resources is a major cause of breaches in Australia. Data buckets, APIs and other cloud resources are, too often, exposed. 28% of Australian organisations consider access controls to be a leading area for investment in the next year.

Figure 3 illustrates the leading cybersecurity initiatives for Australian organisations over the next year. Respondents gave multiple responses.

Leading Cybersecurity Initiatives



N=320
Australian Cybersecurity Survey, 2023

Aligning Security Outcomes with Business Outcomes and Goals

There are many external challenges facing Australian organisations as they address cyber risk, but a critical one is internal—the lack of alignment between CISOs and the rest of the C-suite.

As cyberattacks grow in sophistication and scale, the business impact from a security incident is increasing enormously. In today's environment, a security threat is a business threat.

That's why it's critical that cybersecurity outcomes are aligned to business outcomes and goals. This can mitigate the risks that obstruct organisational success and measure the true business impact of security investments. This enables companies to build cybersecurity programs that don't just protect businesses, but also grow them.

Business leaders are increasingly factoring cybersecurity risk into their overall risk calculations and are partnering with CISOs to assess risk and vulnerabilities — and to ensure that risk mitigation activities are adequately resourced.

CISOs need to collaborate widely with the C-suite and other business leaders. This can be achieved by:

- Framing conversations around risk, especially assessing risks and defining and explaining controls that mitigate risk.
- Outlining cybersecurity risk management priorities with emphasis on the impact and likelihood of breaches, and risk prioritisation.
- Using data to assess risk and propose solutions. Hard metrics on improvements in detection and response times are particularly useful as are compliance metrics and any data that reveals the cost of breaches.
- Developing a cybersecurity strategy and set of objectives to ensure that business and cybersecurity goals are aligned.
- Assessing the cost of implementing a cybersecurity strategy.

Effective cybersecurity postures reduce risk and complexity, increase the value of the firm as well as the value of the brand, increase speed to market, and provide competitive differentiation. It is therefore, not surprising that business leaders increasingly seek cybersecurity metrics which are aligned to business outcomes and goals.

Key Metrics for Maximising the Value of Cybersecurity Investment

Calculating the total cost of ownership (TCO) of cybersecurity investments has been common practice for many years. Business value is more challenging to measure and varies widely by risk appetite, organisation type and jurisdiction.

Key business value metrics include the following, that are caused by cybersecurity investments:

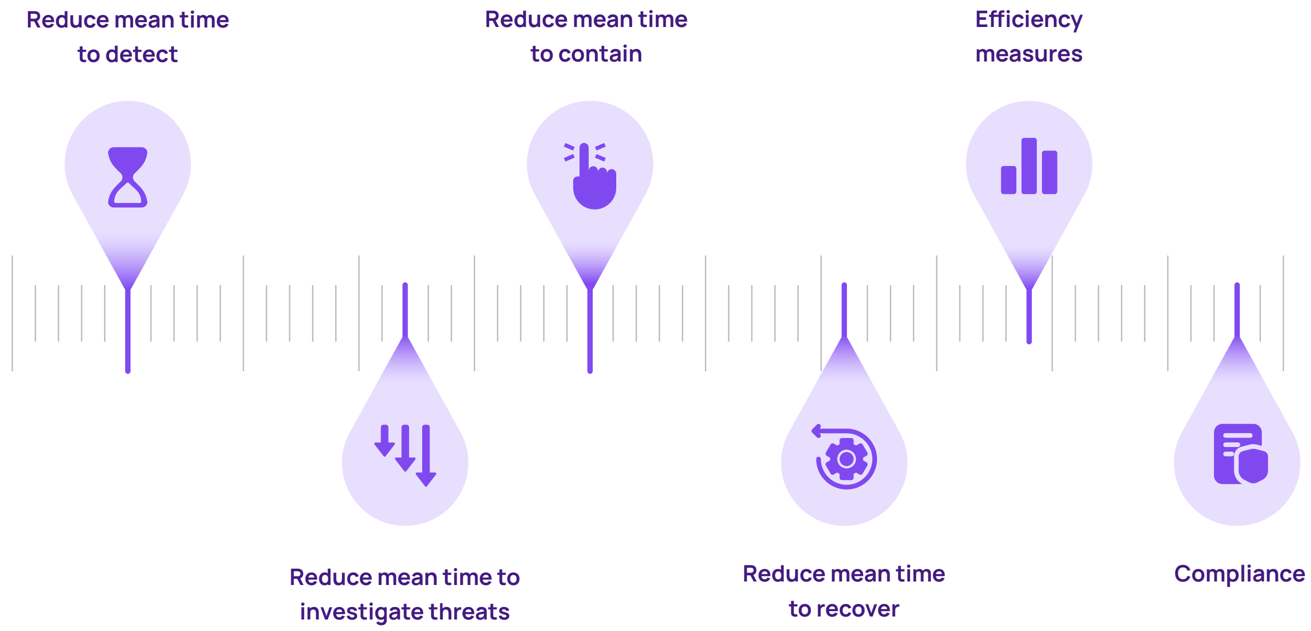
- ✓ Reduced risk leading to an increase in the value of the firm.
- ✓ Reduction in interruptions to business operations.
- ✓ Increased brand equity driven by improved reputation.
- ✓ Compliance leading to lower potential costs from fines.

These factors can enable organisations to calculate the return of their security investments. Importantly, organisations must always recognise that too much emphasis on security technology alone can lower returns on security investment. Organisations need to ensure that they have the necessary people and processes in place — to deliver higher returns on security investment. Technology alone will not reduce cybersecurity risk.

Measurements which impact risk are particularly valuable to the business. From a cybersecurity perspective there are several metrics that can be shared with the rest of the business, that reduce risk. These metrics should also be shared with industry benchmarks to help the business to make sense of the data.

Figure 4 illustrates key metrics that CISOs can share with the business to help reduce risk.

Key Cybersecurity Metrics


Reduce mean time to detect
Reduce mean time to investigate threats
Reduce mean time to contain
Reduce mean time to recover
Efficiency measures
Compliance

Conclusion

With most cybersecurity budgets expected to be stagnating over the next year — despite the rapid growth in threats — CISOs will increasingly focus on doing more with less.

In the coming year, CISOs will assess existing cybersecurity investments and seek to reduce complexity, consolidate their cybersecurity platform, increase automation and ensure that basic cyber hygiene processes are productive, and being enforced.

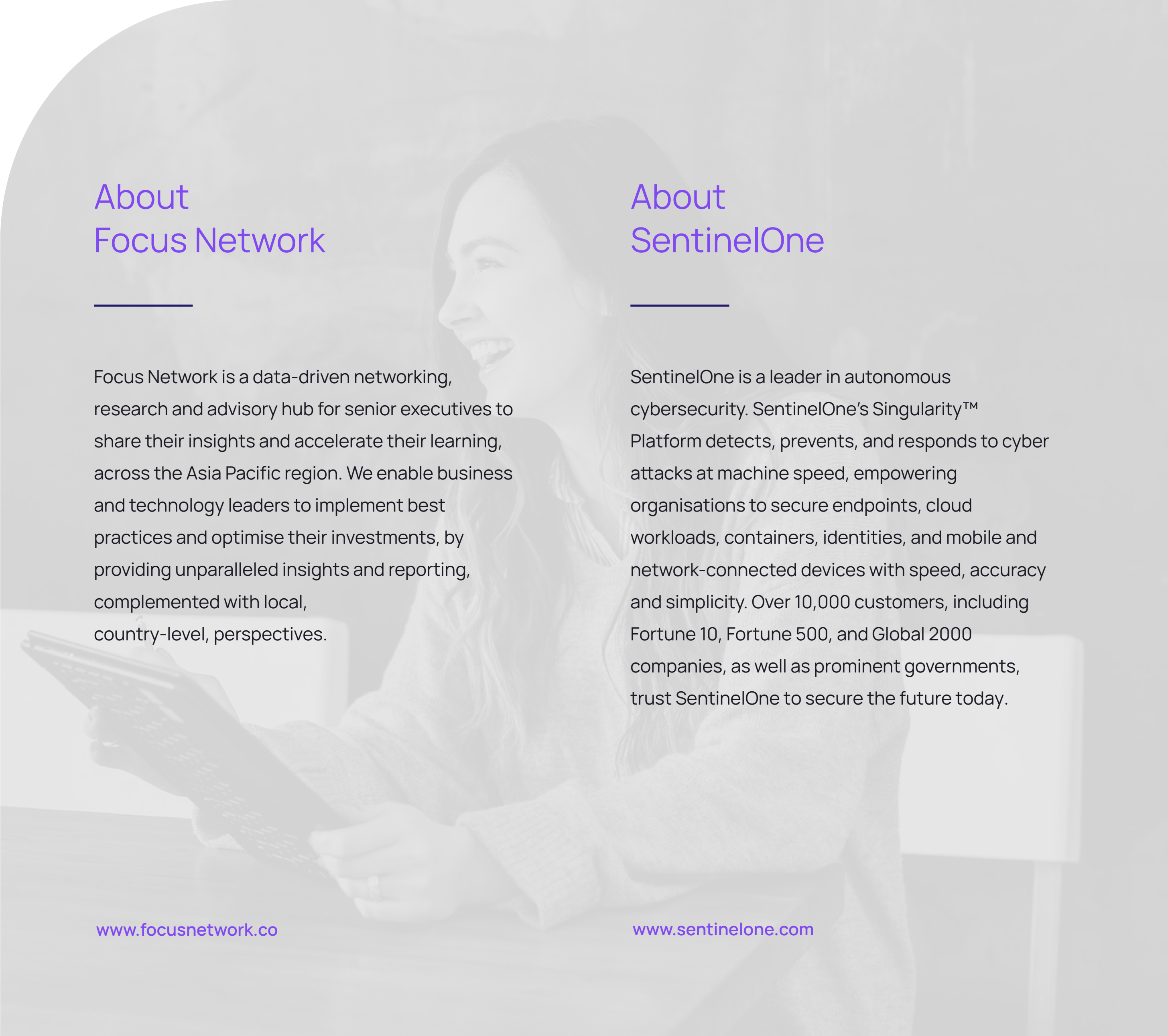
Australian organisations have an average of 36 cybersecurity tools to manage. For many CISOs, their primary focus will be inward with emphasis on reducing the number of tools that they use and the associated complexity.

These issues can be addressed by decreasing the number of alerts and false positives, lowering the amount of time and the number of tools required for basic cybersecurity hygiene such as patch management. Crucially, reducing remediation times, detection times, and missed detections increases productivity and reduces complexity, dramatically.

From a cyber hygiene perspective, there will be more emphasis on basic processes such as regular health checks for technologies, increased focus on the efficacy of training and awareness programs, vulnerability scanning and configuration management. Polices and processes will also be evaluated – to ensure that they are aligned with risk appetite and are effective.

Skills shortages and budget constraints are also driving increased automation. CISOs are focusing to a greater extent on standardisation across technologies and processes – to enable more efficient and sustainable automation.

Metrics that demonstrate value to the business are now becoming essential tools for CISOs – to justify cybersecurity spending and demonstrate their value. Risk resilience metrics such as reductions in mean time to detect and respond to an attack are critical, as they demonstrate business value clearly.



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

About SentinelOne

SentinelOne is a leader in autonomous cybersecurity. SentinelOne's Singularity™ Platform detects, prevents, and responds to cyber attacks at machine speed, empowering organisations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with speed, accuracy and simplicity. Over 10,000 customers, including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments, trust SentinelOne to secure the future today.

www.sentinelone.com

Disclaimer
Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Focus Network nor any person engaged or employed by Focus Network accepts any liability for any errors, omissions or other inaccuracies.

Readers should independently verify any facts and figures as no liability can be accepted in this regard - readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Focus Network.

Focus
Network

www.focusnetwork.co