WHITE PAPER

The State of Cybersecurity in the Healthcare Sector

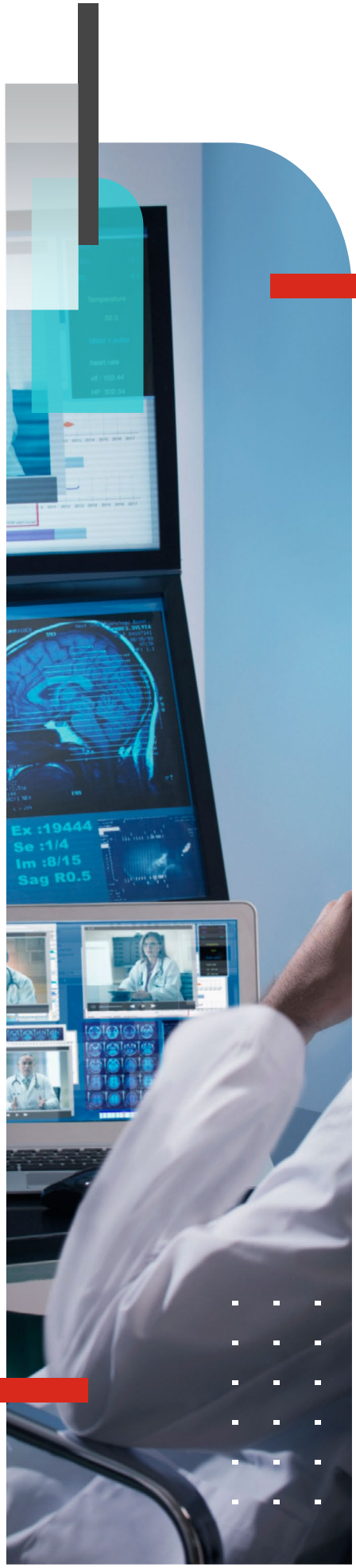
Unprecedented modernisation increasing network vulnerability

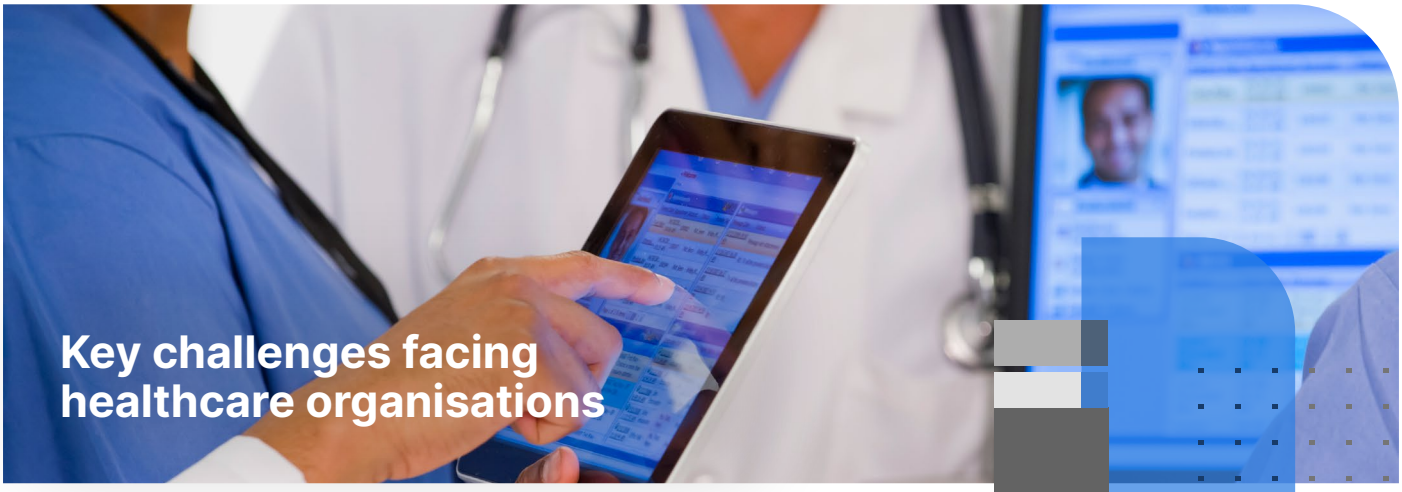
The healthcare industry remains one of the top targets for cyberattacks due to a large attack surface and significant amount of sensitive patient data. The recent introduction of the Security Legislation Amendment (Critical Infrastructure) Act has increased the pressure on healthcare organisations to develop a risk management program to detect and defend against cyberattacks. The Act requires organisations that are critical to the nation, including healthcare services, to harden their cybersecurity and report serious cyberbreaches within certain timeframes.[i]

Regulatory pressure to tighten controls and visibility around cyber risks is driving the healthcare industry to modernise infrastructure as well as its clinical networks to be able to access patient management records internally as well as externally. This has also spurred organisations to adopt network segmentation to mitigate the risks of ransomware and boost their IT security.

The industry is also embracing new innovative technology for efficient and effective patient care both in and out of the hospital or healthcare setting. The shift in mindset from hospital to hospitality has seen the industry take steps toward modernising its networks and giving patients and aged care residents fast and reliable wireless access to the external world. It also supports modern technologies such as electronic healthcare records, remote monitoring, and communication between staff.

The way the sector operates has changed significantly, with the pandemic highlighting the extent to which healthcare can be delivered remotely as well as how new technologies can modernise patient management records. With such significant changes in the past few years, healthcare organisations must improve network security controls and develop appropriate risk management strategies to mitigate cybersecurity incidents.





Key challenges facing healthcare organisations

1. Network modernisation

The landscape is changing, and more and more organisations are looking to move healthcare out of the hospital or healthcare setting and into the home. This means patients are likely to spend less time in hospitals and more time recuperating at home. To ensure that this happens as smoothly as possible, the sector is modernising its networks and upgrading patient management records so that staff can access them not only within the facilities but also outside of them.

As everything moves to the cloud, healthcare organisations must secure their networks as well as the links they're getting access to. In the past, they were dependent on legacy networking and connectivity. However, now they're implementing software-defined wide area networking (SD-WAN) to simplify network infrastructure by integrating networking and security requirements, empowering application resilience, providing network visibility, and centralising management functions. The decision to use SD-WAN is based on three major factors: cost; risk; and performance.

Organisations want to reduce the costs of legacy multiprotocol label switching (MPLS) by transitioning to SD-WAN to enable a more efficient and scalable means of networking as well as reduce risk and complexity by extending consistent security across the network.

Organisations want to reduce the costs of legacy multiprotocol label switching (MPLS) by transitioning to SD-WAN to enable a more efficient and scalable means of networking as well as reduce risk and complexity by extending consistent security across the network.

Organisations are also looking to add a wireless layer into their network. Previously, they had two separate networks: wired and wireless. Now, they're meshing the two networks together and implementing SD-WAN to automate and direct traffic from an end-user directly to a data centre thereby eliminating backhauling traffic.

SD-WAN also improves cloud application performance by prioritising business critical applications related to care delivery and internal processes. While moving to the cloud enhances the ability for healthcare providers to access patient data, it also imposes inherent risks if the appropriate security measures aren't enforced. Healthcare organisations need to be able to secure systems and applications within the cloud with specialised cloud security controls to meet stringent yet necessary regulations and compliance requirements.

2. Cybersecurity skills shortage

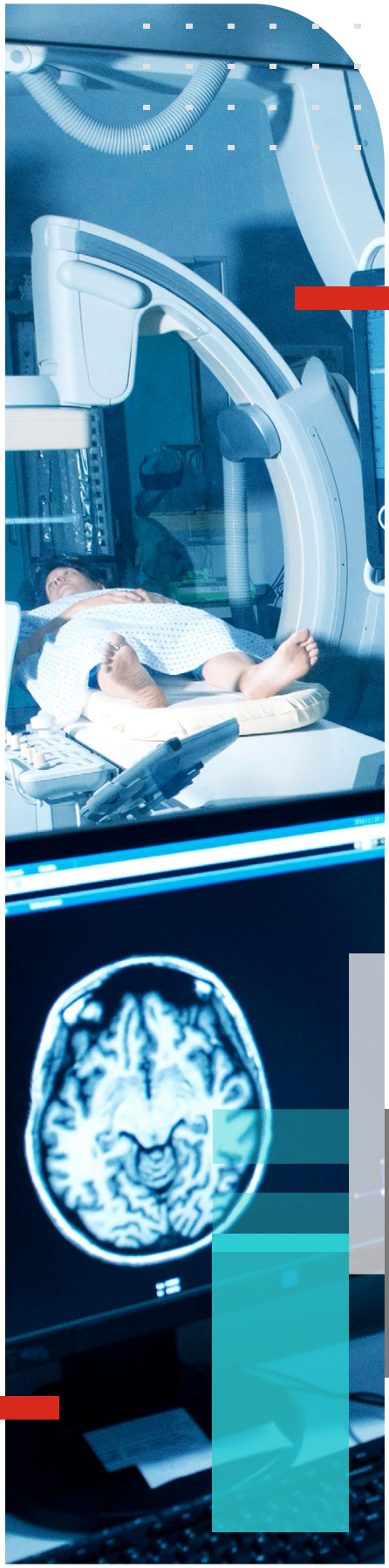
The severe shortage of highly skilled cybersecurity professionals continues to be one of the key issues healthcare providers face. There is still an urgent need to close the current cybersecurity skills gap to ensure healthcare critical assets are protected as well as the staff and the patients. Small, or non-existent, cybersecurity teams are tasked with responding to evolving threats in a complex environment without strong visibility across the entire security infrastructure coupled with an overall lack of awareness. Because of this, many healthcare organisations targeted in ransomware attacks aren't aware they're being infiltrated until years later. When they find out, they often don't know what data is stolen, what the attackers have done with it, or how it's being used.

Meanwhile, healthcare organisations continue to invest in cutting edge technology that isn't secured effectively, leaving healthcare providers and patients vulnerable to cyberattacks. To combat these challenges, more healthcare providers are looking at integration and automation to help address the skill shortages while also looking at transforming their business models. This will go a long way in helping healthcare providers stay ahead of emerging and developing threats, enforcing device compliance, and reducing the attack surface.

3. Endpoint complexity and cost

Cybersecurity initiatives are costly and the healthcare sector is already operating on razor-thin margins with very few resources allocated to IT security. While budgetary restraints aren't new to the sector, challenges from the past few years have stretched budgets tighter than ever before, particularly due to disruptions to elective surgeries, the costs associated with personal protective equipment and testing kits, as well as the need to plug COVID-19 enforced workforce gaps. The problem is further exacerbated by the fact that government regulation is putting healthcare organisations under immense pressure to regularly implement new technologies, which often delay network security attempts. New technologies improve patient care and facilitate communication between healthcare providers; however, they also increase endpoint complexity, which leaves sensitive data at risk.

Despite the costs associated with meeting critical infrastructure security requirements, healthcare organisations must better prepare and protect themselves with more sophisticated security measures. Failing to do so will open them up to further attacks from threat actors and risk delay and disruption of healthcare operations, potentially placing patients' lives at risk.



4. Managing third-party risks

While private healthcare facilities are owned and operated by the private sector, public healthcare facilities such as hospitals are largely owned and managed by the state and territory governments. This means that they don't run their own building infrastructure. While they are solely responsible for the operational aspects of the business including IT and medical systems that hold patient and corporate data, the building infrastructure is the sole responsibility of the facility manager who oversees the facilities' maintenance as well as the catering, ward support, and security. As a result, healthcare organisations in the public sector must look at their third-party providers to ensure they can't be infiltrated by their channels and unwittingly jeopardise the security of sensitive patient information.

Healthcare organisations can reduce risk by pivoting to an agile and data-driven risk management strategy that extends zero trust principles for secure third-party risk management. Fortunately, some of the major hospitals in the country are now modernising their buildings and everything inside the building including the network and applications. This will enable modern management of every endpoint and reduce the risk of cyberattacks through those third-party channels.

Healthcare organisations in the public sector must look at their third-party providers to ensure they can't be infiltrated by their channels and unwittingly jeopardise the security of sensitive patient information.

The value of a security fabric for healthcare organisations

With the adoption of the security fabric approach, healthcare organisations can reduce complexity and cost, while increasing cybersecurity preparedness. A security fabric approach offers a broad set of integrated, automated solutions for comprehensive network protection without disrupting business operations. By moving from a fragmented data security stack to a single unified data security fabric, healthcare organisations can reduce network complexity and cost while delivering secure patient outcomes. The security fabric can also secure legacy medical technology that is notoriously difficult to secure including ageing scanners, smart sensors, and endpoint devices (tablets, laptops, smartphones) that nurses and carers use to assist patients. With the security fabric, healthcare organisations will be able to isolate, gain visibility, and secure what has traditionally been unable to be secured.

How the healthcare sector stacks up in terms of cybersecurity preparedness

As the healthcare industry continues to implement new wireless technologies to give better and faster access to staff and patients, the sector opens itself up to new cyber risks that, if left undetected, could threaten patient care and private data. In October 2021, private hospital group Macquarie Health Corporation, was involved in a ransomware attack by a group known as Hive. The cybercriminals exposed sensitive data from over 6,700 patients and leaked it onto the dark web. While Macquarie Health was able to take its systems offline, the company continued to experience significant impacts from the attack, despite the disruption not impacting patient care.[ii]

The Fortinet *Networking and Cybersecurity Adoption Index 2022* explored the cybersecurity readiness of more than 150 enterprise decision-makers across Australia and New Zealand. The index rated the overall preparedness for cybersecurity threats on a scale of zero to 100. Organisations in both Australia and New Zealand reached an overall score of 75 in all areas, with the processes component falling short of the ideal mark.

The index found that most organisations are, for the most part, doing a reasonable job of ensuring cyber resilience. However, many of the specific actions needed to genuinely be prepared are not given the attention they need to withstand and recover from a cyberattack. Organisations continue to attract high levels of cyberattacks despite most decision-makers understanding the detrimental effects of an inadequate risk management system in managing cybersecurity risks.

Below are the key findings of the Fortinet *Networking and Cybersecurity Adoption Index 2022.*

i https://www.legislation.gov.au/Details/C2021A00124

ii https://machealth.com.au/2021/10/macquarie-health-corporation-it-service-disruption/

WHITEPAPER

The Fortinet Networking and Cybersecurity Adoption Index 2022

Introduction

A volatile economy, the war in Ukraine, rising inflation, and more have contributed to an unstable threat environment in 2022.

The Australian Cyber Security Centre (ACSC) issued an advisory alert in April 2022 urging Australian organisations to adopt an enhanced cybersecurity posture and mentioned the escalating threat environment.[i]

Similarly, the New Zealand National Cyber Security Centre (NCSC) issued a warning for New Zealand organisations to strengthen their cybersecurity preparedness in light of the attack on Ukraine.[ii]

NCSC data shows that there was a 15% increase in incidents affecting nationally significant organisations in the 2020/21 year compared to the previous period, with 28% showing links to suspected state-sponsored actors and 27% that were likely criminal and financially motivated.[iii]

The ACSC has noted an increase in ransomware targeting Australian critical infrastructure entities, with ransomware being recognised globally as one of the top threats facing organisations.[iv] The *Fortinet Global Threat Landscape Report* showed that ransomware had increased 10.7 times between 2020 and 2021. While the frequency of these attacks eased off slightly in the second half of 2021, they remained sophisticated, aggressive, and high impact. For example, double extortion threats have now become the norm. These attacks steal data and threaten to leak it to extort ransoms, in addition to locking the data so it can't be used unless the company pays the ransom.[v]

Australian and New Zealand organisations face ongoing cyberthreats with the potential to cause significant harm to the organisation and to individuals. Coping with the ever-evolving threat landscape requires organisations to combine people, processes, and platforms in an ongoing cycle of improvement to strengthen the organisation's cyber resilience.

This can be challenging as organisations continue to grapple with the ongoing cybersecurity skills shortage, as well as a shortage of subject matter experts in this space. This means that organisations must ensure their most talented and skilled people are focused on the most important threats rather than on managing multiple point solutions, which can be costly and inefficient. It also means that now more than ever, security awareness training should be undertaken by organisations to create a cyber aware workforce to further enhance cyber resilience.

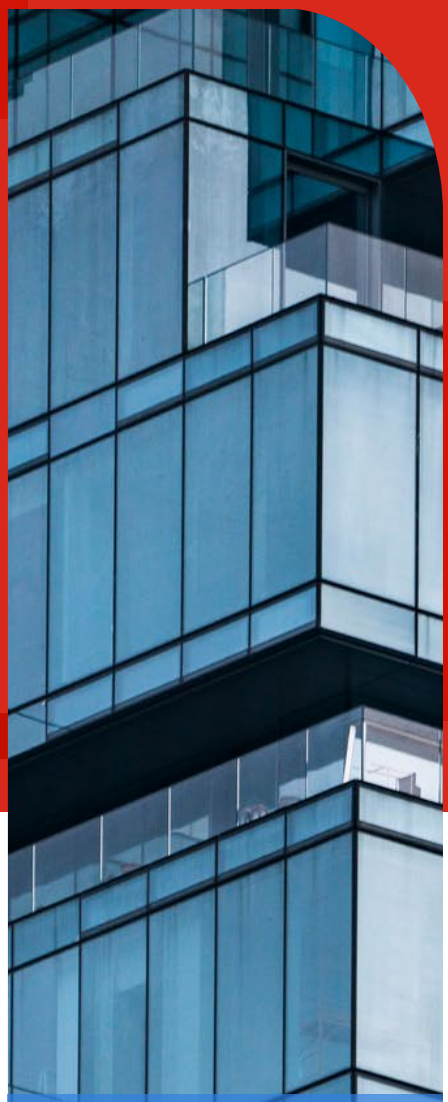
This concept has crystallised in an approach that Gartner has called the 'cybersecurity mesh architecture'.[vi] This approach brings fragmented infrastructure and deployments under a single, unifying banner that makes it easy and straightforward to deploy new technologies and services securely. Fortinet exemplifies this approach with its Fortinet Security Fabric, which delivers a broad, integrated, and automated cybersecurity mesh platform to help organisations reduce complexity and increase security.

Fortinet exemplifies the cybersecurity mesh architecture approach with its Fortinet Security Fabric.

The mesh approach sees a portfolio of secure networking technologies come together to interoperate seamlessly with each other and those from other vendors. The mesh can therefore identify and share threat intelligence, correlate data, and automatically respond to threats as a single, coordinated system. This presents a significant opportunity for organisations to strengthen their cyber resilience even in the face of growing threats.

Fortinet has collaborated with CoreData Research to investigate how enterprises across Australia and New Zealand are addressing the evolving cyberthreat landscape. The *Fortinet Networking and Cybersecurity Index 2022* canvassed the opinions of 150 enterprise decision-makers across Australia and New Zealand in early 2022. This report examines the results of the index.

The impact of people, processes, and platforms



People, processes, and platforms create the three pillars of cyber resilience. These three pillars can present both a risk and an opportunity depending on how well-resourced they are and how they are deployed. The Fortinet Networking and Cybersecurity Index 2022 scored Australia and New Zealand on a scale of zero to 100, with scores higher than 75 indicating a robust, organisation-wide cybersecurity strategy. Scores lower than 75 indicate that some work is yet to be done in key areas.

The score is comprised of 15 questions that are weighted evenly. The scores for people, process, and platform are combined and averaged to create the overall score for each section, with the section scores averaged to create the overall score.

Overall, the index revealed a score of 75, which means that organisations are, for the most part, doing a reasonable job of ensuring cyber resilience. However, organisations were let down on the process side, indicating significant room for improvement.

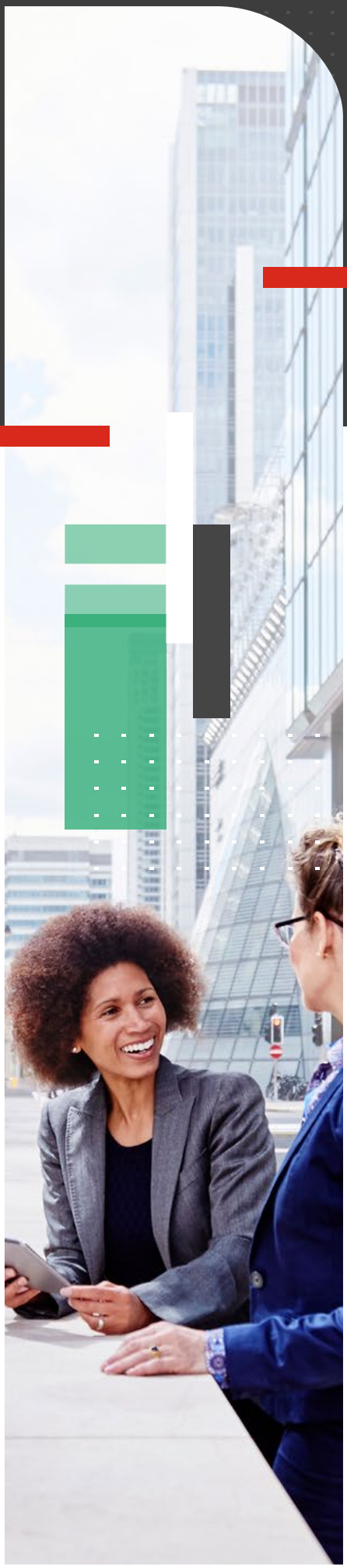
75
Overall score

77 People score

72 Process score

77 Platform score

People



The index scores revealed that there are some areas on the people side where organisations could be seen to excel. In terms of preparation of the incident management team to deal with breaches and cyber exploit threats, the score was 85. Organisations' physical security to protect data assets and IT infrastructure scored 83. This is a very good score; however, organisations must be aware of the risk posed by remote, isolated systems that can be quite exposed. This is especially true in sectors such as mining, energy, and transport, which are considered critical infrastructure sectors according to the Australian government's new legislation. This means these organisations must do more to ensure strong cyber resilience across the board.

The competency of staff to protect data assets and IT infrastructure scored 81 and resourcing of staff to protect data assets and IT infrastructure was slightly lower at 78.

This means that organisations are generally doing a good job of preparing and resourcing the organisation for cyber resilience. However, there is still some room for improvement. For example, the provision of IT security programs for employees scored the lowest at 60.

This is a significant concern for organisations because it suggests that they may not be investing as much time and energy into training staff members as they could. While general preparedness seems relatively high, this is likely to trend downwards if not supported long-term by effective and comprehensive training programs.

It's essential for organisations to consider adding training and awareness programs for all employees into their frameworks and policies, creating a common language around cyber resilience that can help maintain high preparedness scores into the future.

This is also important because, while cyber savvy members of the organisation may consider themselves well-prepared for a cyberbreach, there is a less-visible cohort of employees that are less cyber aware. These users create a potential security risk for organisations. By participating in basic cybersecurity awareness training, these users could increase their resilience and help reduce the risk of a successful attack on the organisation.

It's important to note that internal phishing systems, designed to protect the organisation, are generally seen as negative and ineffective. Training staff members to more accurately identify and respond to phishing attempts is essential.

85

Preparation of incident management team to deal with breaches and cyber exploit threats

83

Organisations' physical security to protect data assets and IT infrastructure

81

Competency of staff to protect data assets and IT infrastructure

78

Resourcing of staff to protect data assets and IT infrastructure

60

Provision of IT security programs for employees

Preparation of incident management team to deal with breaches and cyber exploit threats

The index revealed that 53% of respondents considered themselves highly prepared, while 34% considered themselves reasonably prepared to deal with breaches and cyber exploit threats. A further 13% considered themselves somewhat prepared.

Competency of staff to protect data assets and IT infrastructure

43% of respondents said their staff were highly competent to protect data assets and IT infrastructure, 41% said their staff were reasonably competent, and 15% said their staff were somewhat competent.

53%
of respondents considered themselves highly prepared

43%
of respondents said their staff were highly competent

Resourcing of staff to protect data assets and IT infrastructure

Only 41% of organisations considered themselves highly resourced while 37% considered themselves reasonably resourced. 15% considered themselves somewhat resourced while 5% considered themselves minimally resourced. This is concerning because it suggests that organisations are potentially not doing enough to protect data assets and IT infrastructure, possibly opening them up to cyber risks that could be financially and reputationally damaging.

41%
of organisations considered themselves highly resourced

Breaking this down across established businesses versus businesses in development shows that businesses in development are much more highly resourced. 63% of development businesses said they were highly resourced compared with 31% of established businesses. This could be due to an increased focus on cybersecurity for new businesses that have a greenfield approach and a dedicated cybersecurity budget. Businesses that are ramping up could face additional cybersecurity threats as they grow, so strong resourcing is important at this stage of a business's development.

23% of development businesses said they were reasonably resourced compared with 37% of established businesses. This is likely because of the much higher number of respondents who said they were highly resourced. 3% of development businesses said they were somewhat resourced compared with 29% of established businesses.

Development businesses were more likely to say they were minimally resourced or not resourced at all with 13% in this category versus 2% for established businesses.

Regardless of resourcing, organisations must have specific plans for incident response, business continuity, and disaster recovery. These plans should be realistic and incorporate specifics including a lack of resources so that the business has visibility into potential weak spots. These plans should be tested regularly, which can help improve preparedness regardless of the outcome.

Organisations' physical security to protect data assets and IT infrastructure

Almost half (47%) of respondents said they had considerable physical security measures in place and 40% said they had reasonable measures in place. 12% had some measures in place.

Provision of IT security programs for employees

63% of organisations provide training for employees, 62% provide ongoing support, and 61% focus on awareness. Meanwhile, 59% provide onboarding orientation and 56% focus on cyber hygiene practices.

58% of staff members consider themselves very well trained and 37% consider themselves somewhat well trained. Just 5% consider themselves somewhat poorly trained.

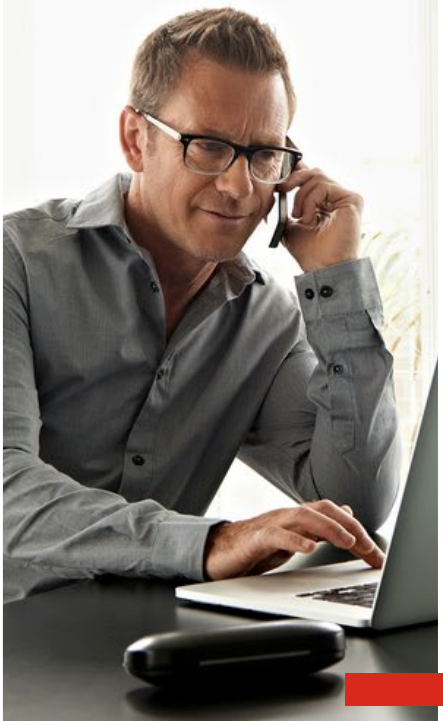
The average number of staff members certified in tools such as the Fortinet Network Security Expert (NSE) program, Cisco Certified Network Associate (CCNA), or Microsoft Certified Systems Engineer (MCSE) was 20. The average number of certifications (e.g., SANS or IC2) in the organisation was 10. Organisations can benefit from leveraging certification training from providers, which can significantly increase the skills and capabilities of IT teams. Some of this training can be completed online at no cost apart from the IT professional's time, so it can deliver real value for organisations and individuals alike.

63%
of organisations provide training for employees

Processes

85

Organisations' cultural commitment to IT security



The overall process score was 72, indicating that more work is required to improve processes. Organisations' cultural commitment to IT security scored highest at 85. The effectiveness of IT security decision-making and the resourcing of an organisation's budget to protect digital and data assets and IT infrastructure both scored relatively well at 79.

However, organisations across Australia and New Zealand only scored 62 when it came to having procedures and processes currently in place and a very low 54 regarding implementation of IT security procedures and processes.

This is at odds with the people scores, which were high when it came to organisations' ability to deal with breaches and threats and the competency of staff to protect data assets and IT infrastructure.

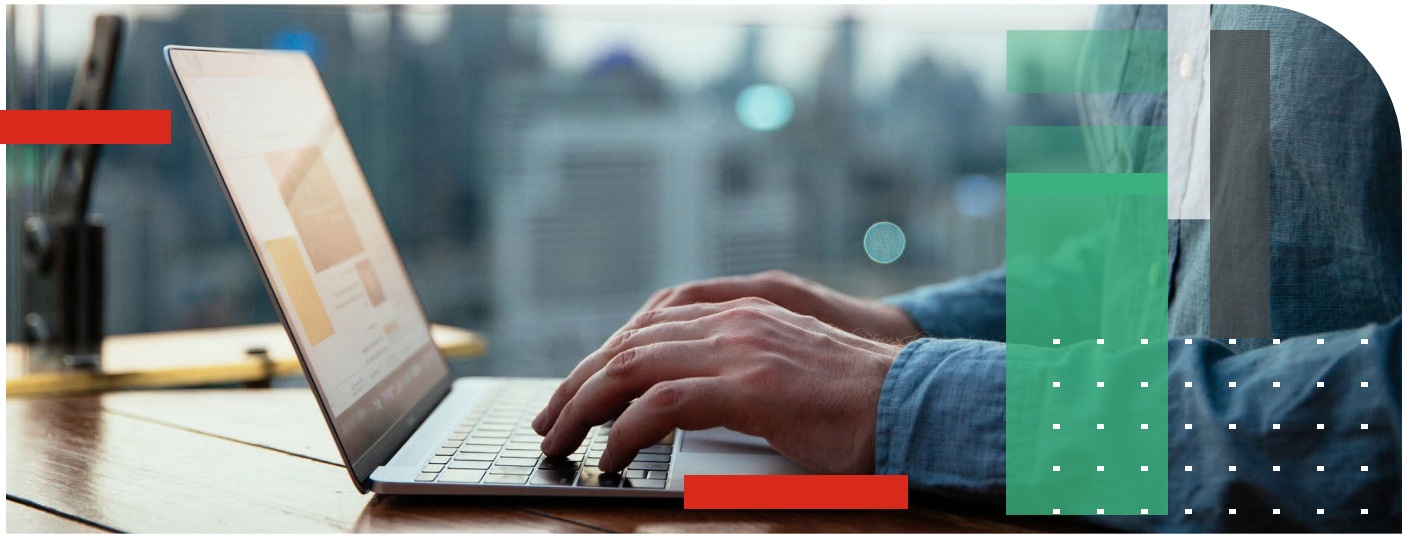
Furthermore, the relatively low focus on procedures and policies suggests that the maturity level for these organisations may not be as high as it could be. Having security in place without processes to make that security effective across the business means that organisations could be missing an opportunity for increased resilience.

79
Effectiveness of IT security decision-making in organisations

79
Resourcing of an organisation's budget to protect digital and data assets and IT infrastructure

62
Procedures and processes currently in place

54
Implementation of IT security procedures and processes



Effectiveness of IT security decision-making

41% of organisations said they made decisions highly effectively and 36% said they made decisions reasonably effectively. 21% rated their decision-making effectiveness as somewhat effective.

However, when this is compared with organisations' commitment to audits and drills (which sits at 57%), there is concern that this decision-making is not being tested and validated.

Resourcing of organisations' budget to protect digital and data assets and IT infrastructure

44% of organisations considered themselves highly resourced while 29% considered themselves reasonably resourced. 23% considered themselves somewhat resourced.

Organisations' cultural commitment to IT security

More than half (51%) considered themselves highly committed to IT security and 40% considered themselves reasonably committed. 9% were somewhat committed, with no respondents reporting being minimally committed or not committed at all.

While commitment is high, many organisations may be struggling to determine where to start with cyber resilience, because disciplined adherence to best practices is low at 49%. Chief information security officers (CISOs) could benefit from attending a roundtable with their peers to learn more about implementation and how to proceed for best results.

41%
of organisations said they made decisions highly effectively

44%
of organisations considered themselves highly resourced

51%
considered themselves highly committed to IT security

Procedures and processes currently in place

Of the procedures and processes currently in place, 69% of organisations use IT security performance metrics, 63% have IT security governance frameworks, while 61% conduct periodic scheduled reviews, assessments, and gap analyses.

Just 59% of organisations have an enterprise risk management and implementation plan. However, the perception remains that organisations are well-prepared for a cyber incident. This is unlikely to be true without a strategic and proven plan in place. Understanding what organisations think they have in place to protect against cyberbreaches versus what is actually in place is essential to mitigating risk effectively. Furthermore, this is a requirement for critical infrastructure operators as part of the new CI legislation.

57% of organisations have a regular schedule of auditing and drill regimes. Auditing can seem like an expensive and time-consuming process, which makes many organisations reluctant to commit. However, there are various low-cost, cloud-based automated tools that can help simplify the audit process. This can, in turn, assist organisations to ensure they have the right tools in place to address the organisation's risk.

Achieved in implementing IT security procedures and processes

65% of respondents said they had achieved effective incident response processes and data breach readiness. 53% said they had aligned security and business objectives and a further 53% said they had clear role responsibilities and accountability throughout the organisation.

Less than half (49%) said they had achieved disciplined adherence to established best practices and 48% said they had achieved transparency around risk vulnerability.

This is at odds with organisations' assertion that they are highly prepared and well-resourced to protect the organisation against cyberattacks. With only 53% agreeing that there are clearly defined roles and responsibilities, this indicates that many companies may struggle when it comes to accountability. Automated cyber resilience solutions can assist in this area by taking that responsibility away from individuals to some extent and delivering processes and transparency.

Furthermore, developing and testing incident response, business continuity, and disaster recovery plans should form part of the organisation's process. The more specific these plans are, and the more often they are tested, the more prepared an organisation will be for an emergency situation.

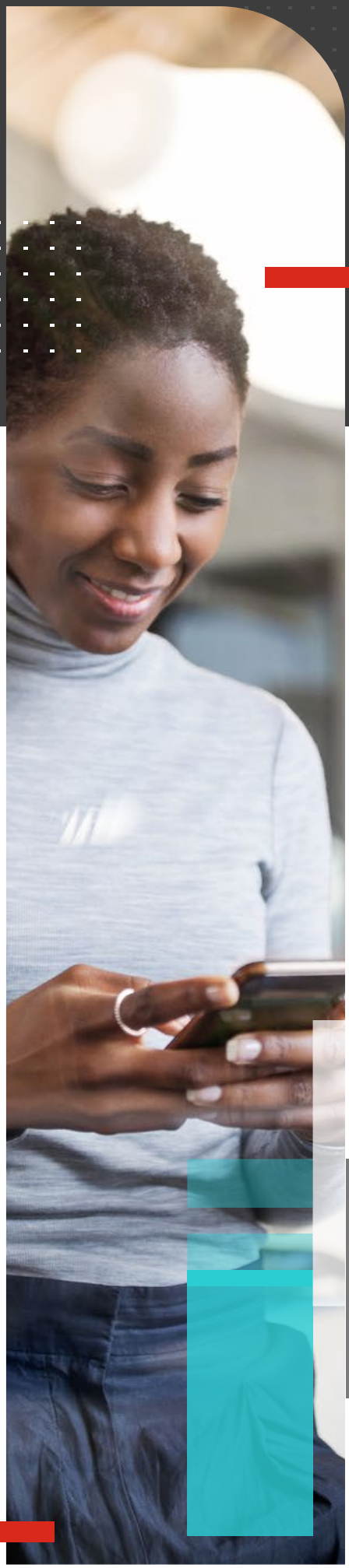
59%

of organisations have an enterprise risk management and implementation plan

65%

said they had achieved effective incident response processes and data breach readiness

Platforms



Platforms received an overall score of 77. Frequency of suitability review of software-defined wide area networking (SD-WAN) providers scored high at 86. Frequency of network security testing also scored high at 85 and frequency of suitability review of antivirus and firewall solution providers likewise scored high at 83. Confidence that networking and cloud security technologies can protect data assets and IT infrastructure was also high with a score of 80.

However, the overall score was brought down by a low score of 57 when it came to up-to-date platforms. This indicates that, despite frequently reviewing their providers, organisations aren't necessarily upgrading as regularly as they could be. This could be due to the complexity of keeping systems up to date. However, when considering a layered security approach, it's crucial to have the platforms available to respond promptly. This requires up-to-date systems. When systems are not updated regularly, a layered security approach can help create a positive security model regardless.

While frequency of network security testing (with a score of 85) is important, having up-to-date platforms is arguably even more essential, yet it sits at a low score of 57. This should be reversed, with organisations focusing on deploying the most up-to-date platforms, then testing those platforms to ensure they're working as anticipated.

This is particularly important in light of research that shows threat actors are exploiting older vulnerabilities versus newer ones.[vii] By simply deploying newer platforms, many of these risks can be mitigated. The cybersecurity mesh approach assists with integration and increases internal capabilities.

86
Frequency of suitability review of SD-WAN providers

85
Frequency of network security testing

Another issue around maintaining out-of-date solutions is the lack of a cohesive approach to cyber resilience. This means that, as people identify new challenges, organisations tend to look for brand-new solutions that can solve that challenge specifically. This leads to a proliferation of point solutions that increase complexity and cost. The alternative is to seek a cybersecurity mesh architecture that pulls together disparate products into a single, overarching fabric that reduces blind spots and delivers seamless coverage across the entire environment. The cybersecurity mesh approach assists with integration and increases internal capabilities.

83
Frequency of suitability review of antivirus and firewall solution providers

80
Confidence that networking and cloud security technologies can protect data assets and IT infrastructure

57
Up-to-date platforms

Frequency of network security testing

55% of organisations test network security monthly and 34% test quarterly. 7% test twice a year and 4% test annually.

Confidence networking and cloud security technologies can protect current data assets and IT infrastructure

Confidence in networking and cloud security technologies is high across the board. 43% of organisations are highly confident and 37% are reasonably confident that networking and cloud security technologies can protect current data assets and IT infrastructure. This could be because organisations are more security-aware when moving to the cloud, or they may feel that it is easier to implement logical security controls in the cloud.

16% are only somewhat confident. This number is high given that most problems with security technologies are either patched before issues arise, or are related to misconfiguration. Organisations can have more confidence in their security technology.

Frequency of suitability review of antivirus and firewall solution providers

57% of organisations review the suitability of their antivirus and firewall solution providers annually, 21% review every few years, and 20% review 'as the need arises'. Others review their provider suitability sporadically or rarely.

43%
of organisations are highly confident

Frequency of suitability review of SD-WAN provider

52% of organisations are reviewing the suitability of their SD-WAN provider annually, 19% every few years, and 23% 'as the need arises'. As networks have become more complex, SD-WAN provides a way to manage this complexity more effectively. It has also blurred the lines of what security really is. There is a knowledge gap that may make organisations less confident when it comes to cloud security. While people are confidently moving to the cloud, simply moving to the cloud does not indicate confidence in security.

It's important to understand that the value of SD-WAN is that it blends networking with security. This is important for the future, where all solutions should be built on a foundation of security. Not all SD-WAN solutions are the same in terms of security, making it essential for organisations to do due diligence to ensure that they're working with a truly secure SD-WAN offering.

52%

of organisations review the suitability of their SD-WAN provider annually

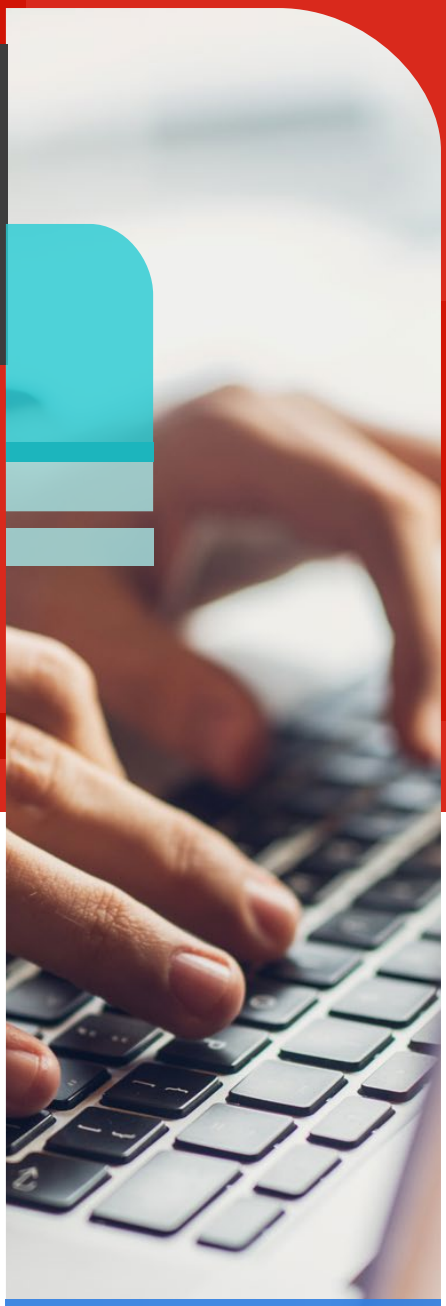
Up-to-date platforms

65% of organisations conduct regular maintenance of software updates and security patches. This is concerning, especially in light of the Australian Cyber Security Centre's Essential 8 recommendations, which advise that patch applications are one of the essential baseline cybersecurity controls that must be in place.[viii] Ideally, this number should be closer to 100%.

61% have their endpoint security, identity, and privileged account management protocols up to date. 60% have up-to-date and suitable antivirus and firewall solutions for the organisation's needs. Just 51% have maturity, compliance, and certification assessments up to date. Only 45% have up-to-date intrusion detection and threat intelligence operating models up to date.

These scores are significantly low and, again, this is at odds with organisations' assertion that they are well-resourced when it comes to cyber resilience. **Organisations should look to make their platforms more efficient and effective.** They can do this by choosing a cybersecurity mesh architecture approach, which combines various cybersecurity tools into an overarching and highly integrated solution.

Key results



Challenges

Detecting and remediating breaches

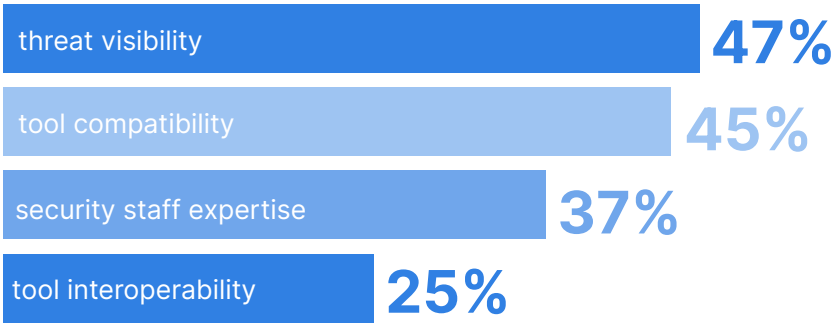
When it comes to detecting and remediating breaches, organisations face significant challenges. Less than half (49%) of the organisations surveyed could detect a breach in less than 30 days, indicating that most organisations could be at risk of advanced, persistent threats that go unchecked for longer than 30 days. In fact, 23% of businesses take between two and three months to detect a security breach, during which time significant damage could be done to the organisation.

Ideally, organisations should be able to detect and remediate a breach much sooner. Using artificial intelligence (AI)-powered tools, Fortinet's Virtual Security Analyst™ can achieve a 99.9% detection rate with detection in less than one second.[ix] This can dramatically reduce the time to detection and remediation without putting undue pressure on existing security teams or requiring additional headcount.

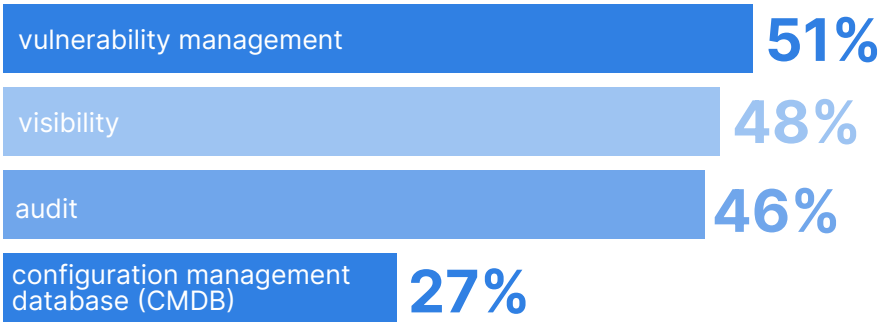
49%
of organisations could detect a breach in less than 30 days

23%
of businesses take between two and three months to detect a security breach

The barriers to gaining visibility and reducing threat detection time were:



The gaps in enterprise risk management were identified as:

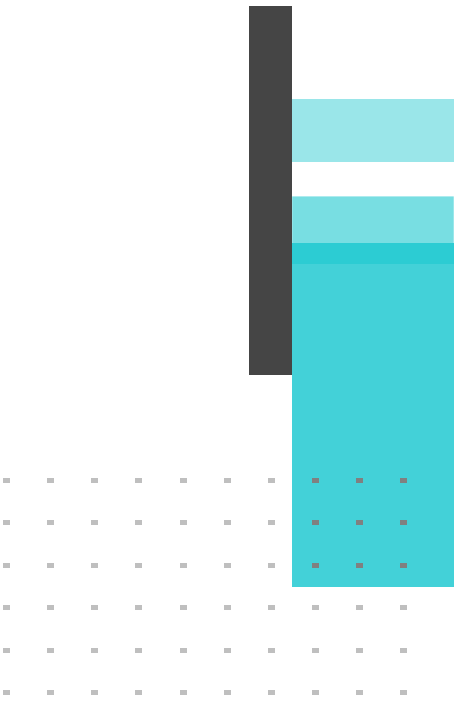


By using a cybersecurity mesh architecture approach, organisations can improve these numbers significantly. A mesh solution will catch and quarantine malware as soon as it comes in, reducing the detection timeframe from 30 days to instantaneous. This is essential given the nature of the current threats such as ransomware, which can do enormous damage in very little time.

A mesh solution reduces the detection timeframe from 30 days to instantaneous

The faster an organisation can detect and remediate a threat, the higher it sits on the maturity scale. Increasing the organisation's maturity can reduce operational risk substantially, which in turn lowers costs and improves an organisation's ability to remain productive because it is less likely to be materially affected by cyberbreaches.

84% of respondents were able to trigger a response that can remediate cyberattacks across domains. However, with a mesh approach, the threat itself would not be able to spread across domains in the first place, rendering this ability irrelevant.



Siloed IT security tools

One of the key issues facing organisations is the proliferation of discrete, siloed IT security tools with some organisations using as many as 45 different tools and most using more than five.

This creates significant complexity, can reduce visibility into the overall effectiveness of the organisation's security posture, and can increase the costs associated with managing so many tools.

Often, these tools may overlook vulnerable legacy systems. These are systems that sit in a backroom completing important tasks yet rarely attract attention. In some cases, these systems may form part of the organisation's operational technology (OT), which cannot be easily secured using traditional IT security methods. Deploying a cybersecurity mesh architecture can help organisations be more operationally effective because the mesh approach ensures these legacy systems are protected.

Vulnerabilities

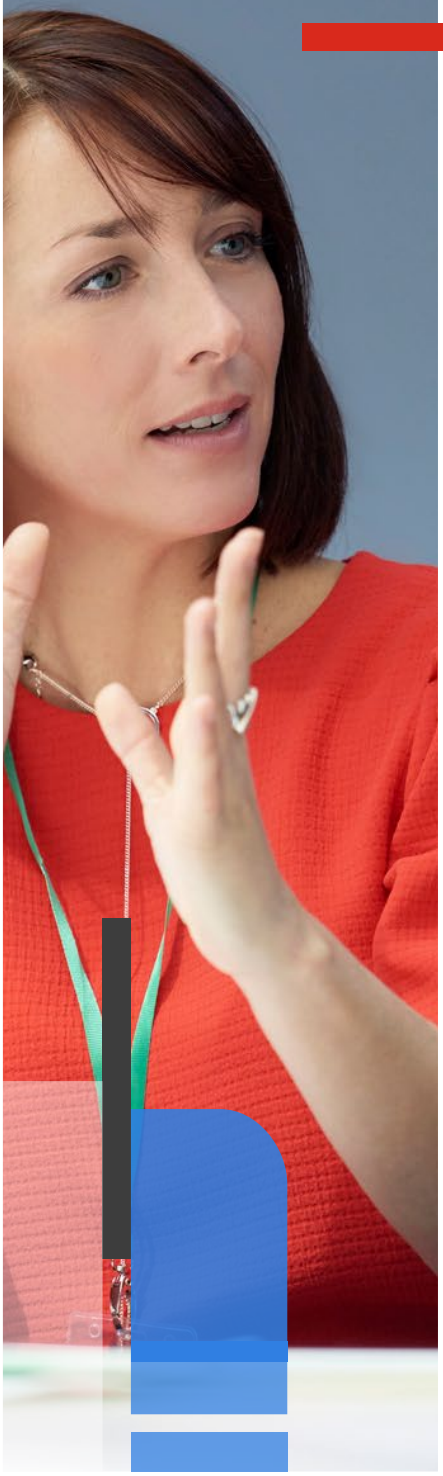
Remote working remains a key vulnerability for organisations with 97% of respondents working remotely to at least some degree and 64% of IT decision-makers expecting this trend to increase in the next 12 months.

The greatest security threat source according to IT decision-makers is advanced persistent cybercrime, which was rated as number one by 19% of respondents.

This was followed by malicious employee action (17%); operational technology and core to the edge (17%); destructive ransomware (16%); competitor espionage (13%); unwitting employee action (11%); and state-based actors (7%).

Malicious actors are becoming ever more sophisticated. Today's threat actors are achieving exploits and attacks that are on par with those traditionally associated with nation state actors. This demonstrates that threat actors are highly trained and experienced, with tools and tradecraft designed to defeat advanced security defences. Additionally, threat actors are engaging in multi-pronged campaigns, where a victim may experience any combination of ransomware, data and personally identifiable information theft, extortion, or all three.

One of the key issues facing organisations is the proliferation of discrete, siloed IT security tools



Opportunities

Cybersecurity mesh

21% of organisations are planning to engage a managed security provider in the next 12 months while 77% already have a managed security provider in place.

Decision-making

When it comes to making decisions regarding new enterprise technology, 70% of organisations rely on their IT supplier. 51% rely on industry associations, 45% lean on their colleagues for advice, and 45% review vendor websites. 41% get their information from the media and just 27% get their information from resellers.

Digital transformation

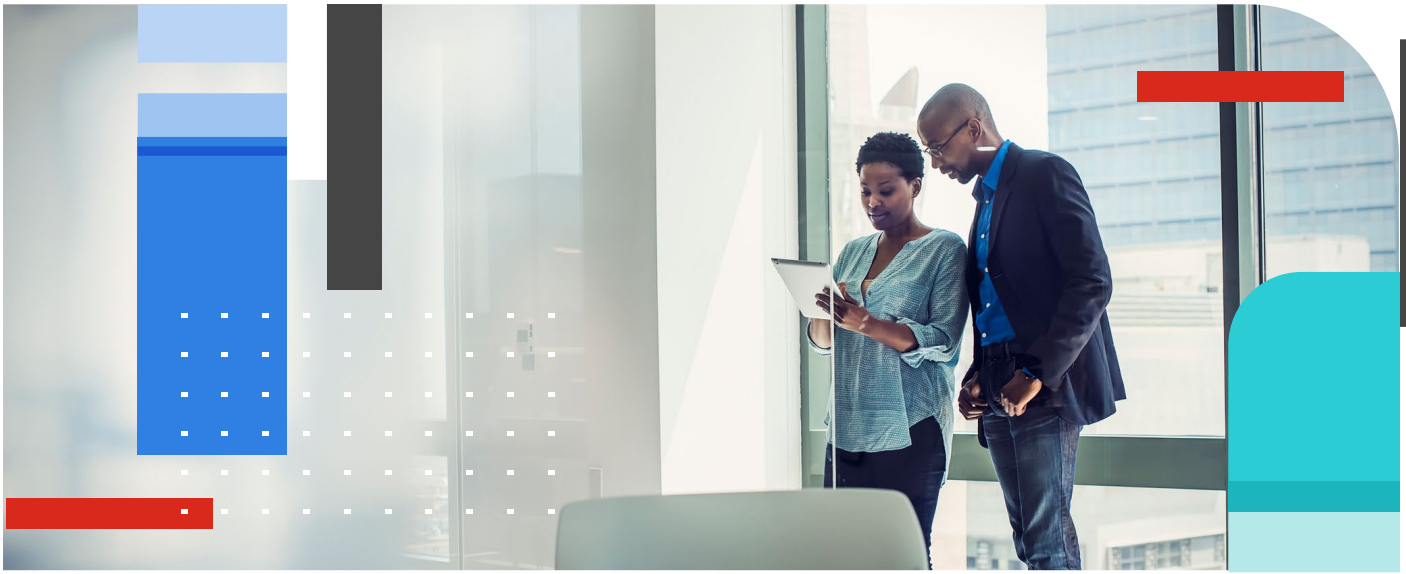
There has been significant ongoing hype around digital transformation and the index results suggest the hype is warranted. 57% of organisations have undertaken change management or digital transformation to address IT security in the last 12 months and a further 31% had done so prior to the last 12 months.

71% of organisations plan to undertake change management/digital transformation in the next 12 months while a further 23% plan to do so without an immediate deadline.

Transformation could be made difficult by a lack of access to IT security specialists that can support general industry and business requirements. 50% of respondents said there were enough IT security specialists; however, it can be difficult to find good ones. 42% said there were plenty of IT security specialists. 7% said there were not enough IT security specialists.

57%

of organisations have undertaken change management or digital transformation to address IT security in the last 12 months



Critical infrastructure

71% of organisations considered themselves to be classed as critical infrastructure under new legislation. The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* requires critical infrastructure (CI) operators to strengthen their cyber resilience measures and be able to show that they've done so. This includes demonstrating that they have developed and maintained a CI risk management program and have a way to report serious cybersecurity incidents.

The latest iteration of the Act focuses on addressing the impact of cybersecurity incidents on a broader range of sectors and assets, according to law firm Gilbert + Tobin's analysis. Critical assets covered under the Act include: broadcasting; domain name; data storage and processing; hospitals; energy market operators; water and sewerage; electricity; gas and liquid fuel; and financial market infrastructure (critical payment systems).[x]

This means that more organisations are affected by the Act than first thought. Preparing to comply with the Act brings financial implications. The Australian government is attempting to help defray those costs with generous rebates for companies with a turnover of less than $50 million. Those businesses will be able to claim 120% of the cost of new technologies and training courses as deductions. So, for every $100 these organisations spend on technology and training, they can deduct $120 from their taxable revenue.[xi]

Organisations that aren't certain whether they're considered CI operators under the Act should check sooner rather than later to confirm their obligations.

71%

of organisations considered themselves to be classed as critical infrastructure

Investment and adoption

Zero trust

Zero trust remains a hot topic, with 42% of organisations planning to implement zero trust security in the next 18 months and 37% having already implemented it. 13% are aware of zero trust yet have no immediate plans while 5% are aware of zero trust but don't know how to implement it. This could provide an opportunity for managed security service providers (MSSPs) to step in to assist these organisations.

When discussing zero trust, it's important to have a clear definition in mind. For example, zero trust network access (ZTNA) refers to ensuring that users on a network are using devices that are security-compliant and are only accessing authorised resources. Zero trust edge refers to a process that connects internet traffic to remote sites, often through a secure access services edge (SASE) tool.

Analyst firm Forrester's *Now Tech Report* in December 2021 featured all-in-one zero trust edge solutions. The report described the future of next-generation networking infrastructure as the bringing together of networking and security in any combination of cloud, software, and hardware interweaving users, data, and resources securely using zero trust principles.[xii]

Investment plans

Organisations are planning significant investments in the next 12 to 18 months across various technologies. For example:

38% plan to invest in leading-edge security technologies using automation and artificial intelligence tools

38% plan to invest in next-generation firewalls

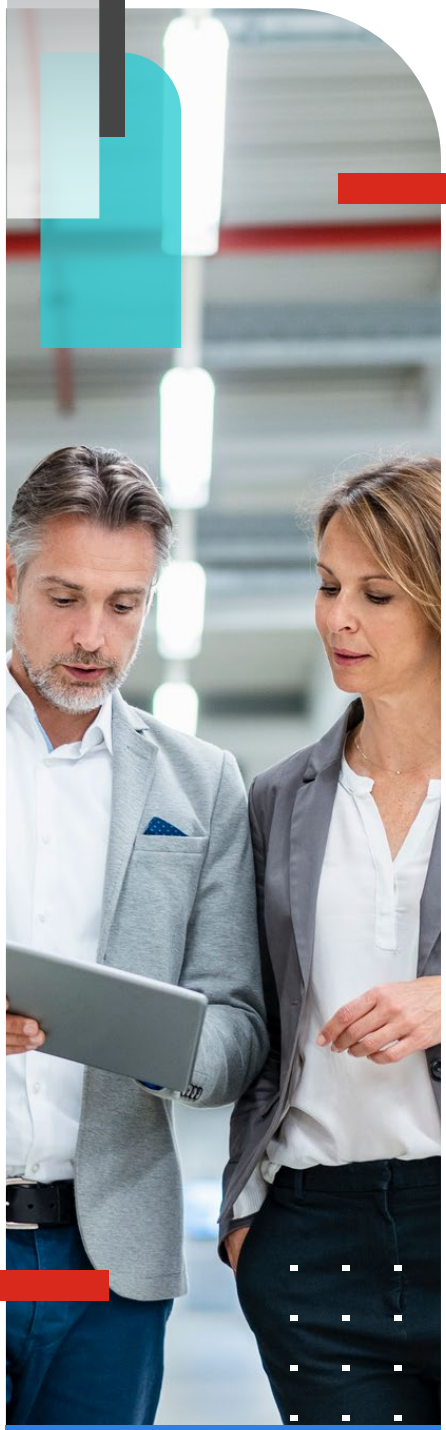
29% plan to invest in SD-WAN

31% plan to invest in 5G

27% plan to invest in operational technology

23% plan to invest in cloud technology

A substantial percentage of organisations are considering these technologies with no immediate plans to invest.



42%

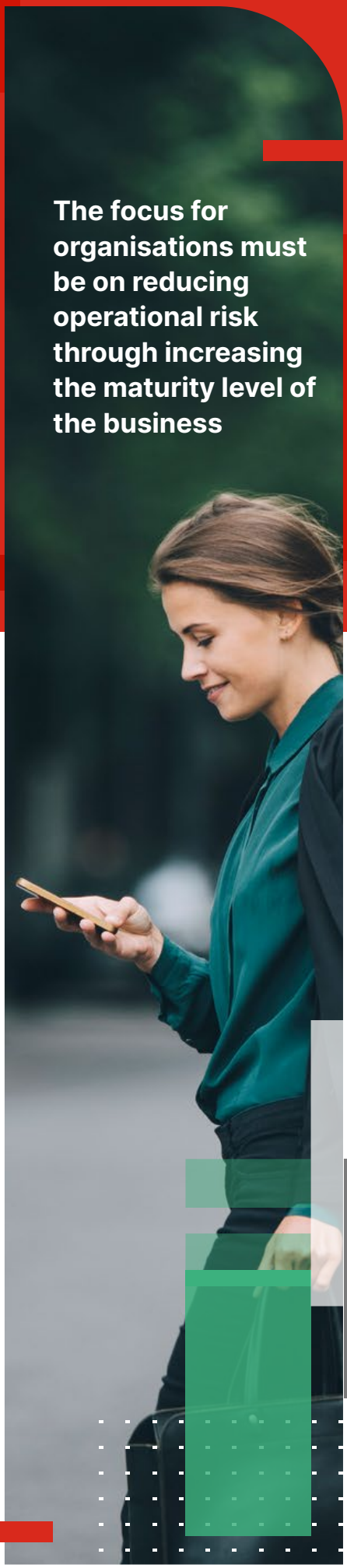
of organisations plan to implement zero trust security in the next 18 months

Barriers

The main barriers to upgrading cybersecurity systems and processes are:

36%	time and effort to learn to use digital platforms effectively
35%	cost
35%	limited technical capabilities of staff
34%	hassle and complication of replacing old systems
29%	deciding on suitable digital solutions for the business's needs
29%	limited recognition of importance for the business
24%	lack of direction for how to go about it
21%	not enough time to get around to it

The way forward: securing people and devices everywhere



The results of the *Fortinet Networking and Cybersecurity Adoption Index 2022* suggest that while organisations tend to consider themselves well-prepared in general, many of the specific actions required to genuinely be prepared are not being given the attention they need.

The focus for organisations must be on reducing operational risk through increasing the cyber maturity level of the business. Organisations can get quick wins in this area with relatively minor investments. For example, moving to multifactor authentication, endpoint detection and response tools, segmentation and micro-segmentation, and risk-based authentication can deliver significant benefits and help increase an organisation's maturity.

Many businesses are focusing on components of this maturity curve; however, few seem to be focusing explicitly on building maturity. By doing so using zero trust, cloud, artificial intelligence-based tools, and a cybersecurity mesh architecture approach, organisations can significantly improve their cyber resilience and futureproof their networks. Businesses should also examine the legacy components within their security architecture and look to build for the future.

CISOs and CIOs must look to educate their boards to understand the importance of building maturity to face the ongoing onslaught of cyberthreats. With the cybersecurity mesh approach, which Fortinet exemplifies with its Security Fabric, organisations can break down silos, reduce complexity and cost, and gain increased visibility and control over their networks.

With a complete solution for the entire network edge, the Fortinet Security Fabric isn't just a cybersecurity provider; it is a networking solutions provider. From SD-WAN to zero trust and next-generation firewalls, Fortinet integrates security across the entire organisation and helps drive increased maturity for stronger cyber resilience.

As organisations continue to operate in an increasingly digital landscape, the cyberthreats facing those organisations will also continue to grow. Businesses need to be able to innovate and transform at pace without compromising security. Embracing the cybersecurity mesh architecture approach will lower risks, complexity, and costs while increasing flexibility, agility, and adaptability.

---

[i] https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture

[ii] https://www.ncsc.govt.nz/newsroom/gsa-2022-2940/

[iii] https://www.ncsc.govt.nz/newsroom/ncsc-cyber-threat-report-shows-rise-in-malicious-attacks-on-new-zealand/

[iv] https://www.cyber.gov.au/acsc/view-all-content/alerts/increased-global-ransomware-threats

[v] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-q1-2022-threat-landscape.pdf

[vi] https://www.gartner.com/en/doc/756665-cybersecurity-mesh

[vii] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-q1-2022-threat-landscape.pdf

[viii] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq#:~:text=The%20mitigation%20strategies%20that%20constitute,factor%20authentication%20and%20regular%20backups.

[ix] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiai.pdf

[x] https://www.gtlaw.com.au/knowledge/curtain-falls-final-reforms-australias-critical-infrastructure-laws

[xi] https://www.theguardian.com/australia-news/2022/mar/29/australia-federal-budget-2022-small-business-technology-training-boost

[xii] https://www.fortinet.com/resources/cyberglossary/zero-trust-edge

FORTINET

www.fortinet.com