vmware®

Australia

Australia Security Insights Report

Extended enterprise under threat

2021

Introduction

This research was conducted to understand the challenges and issues facing Australian businesses when it comes to escalating cyberattacks. It identifies trends in hacking and malicious attacks, and the financial and reputational impact breaches had in what has been an unprecedented year. It examines Australian organisations' plans for securing new technology, adopting a cloud-first security strategy, and dealing with the complexity of the current cybersecurity management environment.

Read this report to discover how senior cybersecurity professionals plan to adapt to the security challenges of the distributed workplace and evolve defences to make security intrinsic to infrastructure and operations.

Management Summary:

Foreword

INSIGHTS FROM THE AUSTRALIA CYBERSECURITY LANDSCAPE

Rick McElroy, Principal Cybersecurity Strategist, VMware Security Business Unit

Everything is different, and yet the same.

The cybersecurity professionals who contributed to the fourth edition of our Australia Security Insights Report are in a very different position than when they answered the 2020 survey. After a year that saw the largest and fastest transformation in work patterns in history, security teams now preside over an ecosystem that is more distributed and heterogeneous than ever before.

Digital transformation programmes advanced rapidly as the cyberattack surface expanded to include living rooms, kitchens, home networks, and personal devices. The remote workforce behaves very differently to the office workforce, accessing the network at unpredictable hours as they strive to stay productive while caring for their families and following government restrictions. As a result, network traffic has changed beyond recognition. Defenders must adapt monitoring systems and trigger points, or risk leaving opportunity for threat actors to use atypical patterns to mask infiltration attempts.

Against this rapidly changing backdrop, some things remain the same:
One industry that has not been disrupted by COVID-19 is cybercrime.

The frequency of attacks is high, sophistication continues to evolve, and breaches are the inevitable result.

Three-quarters (72 percent) of the 251 respondents to our survey said the number of attacks they faced increased in the past year. Of those, 89 percent said attacks increased as a result of more employees working from home. 80 percent said these attacks had become more sophisticated.

The result? Respondents who had a cyberattack reported **2.3 breaches on average per year**, an increase from the 2 breaches reported on average in the last report. These were not minor incidents. In eight out of 10 cases, the breach was a material incident requiring reporting to regulators or the involvement of an incident response (IR) team.

Clearly, security teams are under pressure, and there is little complacency: 59 percent of the CISOs surveyed fear that their organisation will experience a material breach in the coming year.

CISOs can't see into the corners

Cyberattack volumes have grown, but the rapid pivot to remote working means businesses are still not seeing the full picture. Erratic employee behaviour, personal devices, and home network use reduce visibility, creating blind spots and dark corners where attacks go undetected. Consequently:

89%

said attacks increased as a result of home working

2.3

breaches on average have been reported per organisation, per year

79%

said they had suffered a material breach

Ransomware, Third-Party Apps, and Process Weakness Are the Leading Breach Causes

When asked what is causing breaches, the three most common vectors build a picture of external threats and internal weaknesses. Ransomware is the most common culprit, followed closely by third-party apps and then by process weaknesses. Out-of-date security was the fourth most common breach cause.

The rapid pivot to work from anywhere has exposed organisations that had lapsed in security hygiene and failed to implement multifactor authentication.

In addition to these threats, the rapid escalation in ransomware has added unwelcome tension. Multistage campaigns involving penetration, persistence, data theft, and extortion are ramping up pressure as attackers capitalise on the disruption faced by remote workers. In most ransomware attacks, email continues to be used as the most common attack vector to gain initial access.

Ransomware resurgence

Ransomware returns as a top breach cause as attackers launch sophisticated and lucrative multistage campaigns.

26% of all breaches were caused by ransomware.

Apprehension Around App Development and Consumption

Third-party apps remain one of the most concerning causes of breaches since our last report, according to our surveyed CISOs. So, it's not surprising that security teams are focusing on sharpening their approach to consuming and developing them.

Almost half of respondents (57 percent) agree[1] they need better visibility over data and apps to prevent attacks. An overwhelming 60 percent agree that better contextual security is needed to track data security through the application lifecycle. The impact of COVID-19 is recognised as 56 percent agree they need to view security differently than they did in the past due to an expanded attack surface.

Apps topped the list as the most vulnerable point on the data journey. 37 percent of respondents said that apps were the most vulnerable breach point in the data journey at their organisation.

Workloads are rising significantly as a source of perceived vulnerability.

18 percent of respondents said workloads were the most vulnerable breach point in the data journey at their organisation, noting this wasn't the case 12 months ago.

[1] Agree is strongly agree and somewhat agree options combined.

A further 2.4 percent said they had been the most vulnerable point for more than 12 months. Teams are recognising that traditional antivirus fails to secure server workloads, and misconfigurations are a significant breach risk. This often arises due to a knowledge gap between security teams and infrastructure teams whereby security teams don't know how production workloads are expected to behave, and infrastructure teams aren't experienced in recognising attacker behaviour. This year, we anticipate organisations will be looking to address these gaps and strengthen defences for workloads in the cloud.

On the topic of cloud, our research finds an inexorable shift is underway. Almost all the CISOs we surveyed either already follow a cloud-first security strategy or plan to do so very soon. This is a considerable shift and shows that organisations are accelerating their cloud security roadmap in response to the challenges of COVID-19. It may be a road they were already travelling, but they are putting their foot on the gas in recognition of the imperative for comprehensive cloud-first security for a cloud-first world.

We hope that you find our fourth **VMware Australia Security Insights Report** revealing and informative.

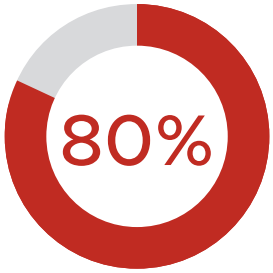
Key Findings

Attack frequency and breach risk remain high

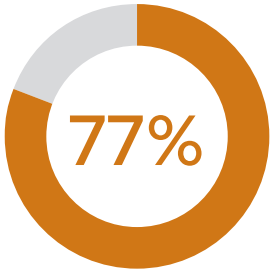
The frequency of attacks is high, their sophistication continues to grow, and breaches are the inevitable result.

72% said attack volumes had increased in the past 12 months. The average reported increase among them was 36 percent.

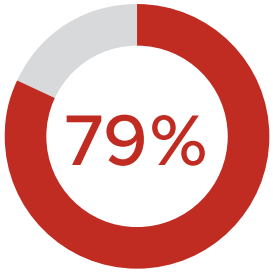
89% of those who had a cyberattack said attacks increased due to more people working from home.



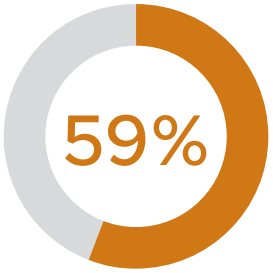
of those who had a cyberattack said attacks were more sophisticated.



have suffered a breach in the past 12 months, with those who have been breached experiencing an average of 2.3 breaches during that time period.



said the breaches they suffered were material.



fear a material breach in the next 12 months.

Ransomware, third-party apps, and process weakness top CISO concerns

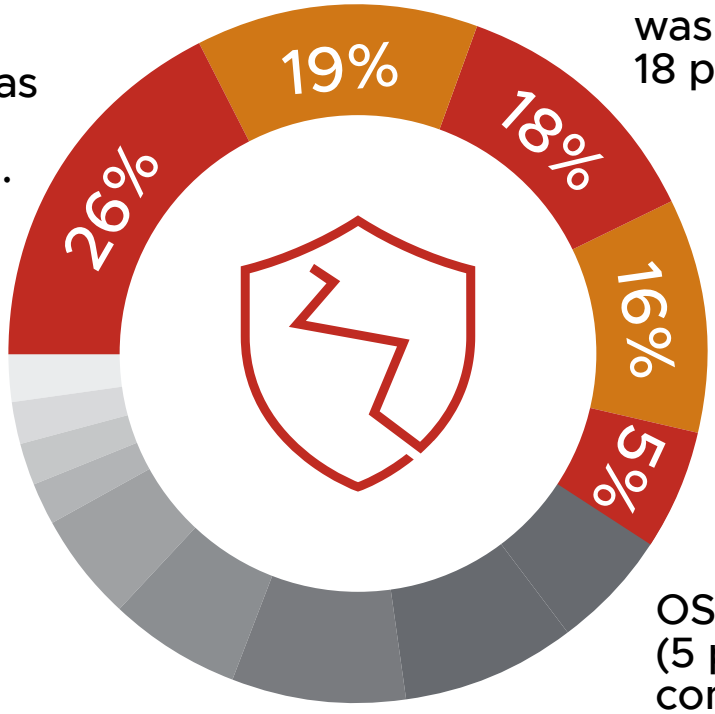
The top vectors that cause breaches build a picture of external threats and internal weaknesses.

Top breach causes for those who had a cyberattack:

Third-party apps were second with 19 percent.

Process weakness was third with 18 percent.

Ransomware was the top cause with 26 percent.



Out-of-date security technology was fourth with 16 percent.

OS vulnerability (5 percent) completes the top five.

Apps and workloads topped the list as the most vulnerable point on the data journey, but they are by no means the only areas of concern.

Expanding attack surfaces have leaders rethinking their traditional approach to security

The good news is that there is recognition of a fundamental shift in security for a highly connected, remote work-supporting, digital age.

56% agree they need to view security differently than they have previously as the attack surface has expanded.

60% agree they need better contextual security in place to track data through the lifecycle.

57% agree they need better visibility over data and apps to pre-empt attacks.

Simplification, consolidation and a switch to cloud-first are in the plan for 2021

Surveyed CISOs appear to be following a path of technology consolidation and the adoption of a more intrinsic approach to security. 47 percent said they are increasing their security budget to achieve these aims.

46% have adapted their security technology to mitigate the risk.

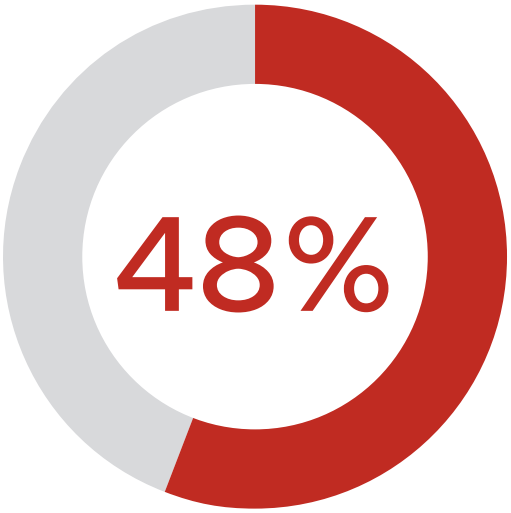
46% are building more security into their infrastructure and apps, and reducing the number of point solutions.

46% have updated their security policy and approach to mitigate risk.

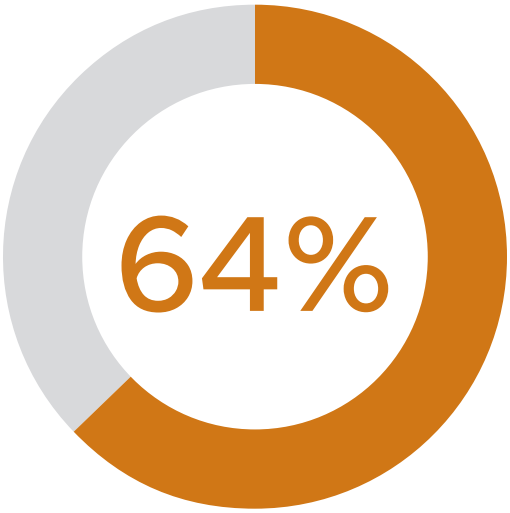
98% have shifted or plan to shift to a cloud-first security strategy.

AI is the next frontier for business innovation, but are security concerns stifling progress?

The next frontier for business innovation is AI as businesses seek an edge to drive more competitive customer services and digital experiences.



Yet, almost half of Australian respondents (48 percent) agree security concerns are holding them back from embracing AI/machine learning (ML)-based apps to improve such services.



64 percent of respondents agree that their ability to innovate depends on their building and getting apps into the hands of employees and customers more securely.

AI is the next frontier for business innovation, but are security concerns stifling progress?

Many respondents are concerned that they're unable to respond to the digital opportunity.

45% agree there is too much complexity in the security solutions industry to make them change their security policy, even though they know today's IT security is not working.

54% agree their board/senior leadership team feels increasingly worried when they bring new apps to market because of the growing threat and damage data breaches/attacks have.

57% agree they would like to use more AI/ML in their apps to improve security and services.

57% agree they need better visibility over data and apps to pre-empt attacks.

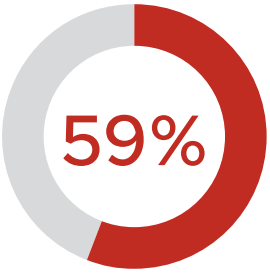
Securing brand and reputation—does it command more urgency for change?

Brand and reputation remain the holy grail for businesses, and it is easily lost. However, the reputational impact of security breaches outstrips financial impact.

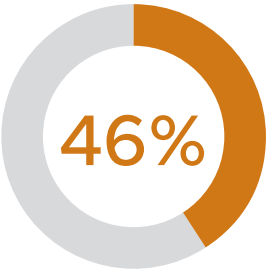
81% of those who suffered a cyberattack say there was some kind of negative impact on reputation—just slightly lower than the nine in 10 that said this in June 2020.

79% of respondents had to report to regulators or engage an IR firm to overcome the reputational problems caused by material breaches in the past 12 months.

There is mixed recognition among respondents of the seriousness of these breaches—and a lack of urgency for change despite the increasing threat landscape.



are fearful they will experience a material breach in the coming year.



have updated their security policy and approach to mitigate the risk.

Full Survey Findings

Have you seen an increase in cyberattacks on your company in the past 12 months? If so, by how much?

72 percent of the CISOs surveyed said they experienced an increase in the number of cyberattacks on their organisation in the past 12 months, and the average increase experienced was 36 percent. This bucks the trend up to now of continued increases in attack volumes with 94 percent reporting this in June 2020.

66 percent of respondents in the financial services sector experienced attack increases at an average of 27 percent. A staggering 91 percent of manufacturing sector respondents experienced attack increases at an above average 40 percent.

Respondents from the healthcare sector fared better than average, with 68 percent reporting attack volume increases.

Larger companies generally had a higher mean average of attacks. This correlated to team size, as well; the larger the size of the IT team, the higher number of attacks.

Has the number of typical overall cyberattacks on your system changed as a result of more employees working from home due to the COVID-19 pandemic?

89 percent of respondents who experienced cyberattacks said they had seen an increase in frequency due to more employees working from home.

More than seven out of 10 (78 percent) respondents from financial services and 91 percent of respondents from healthcare organisations noted an increase in attacks connected to home working.

Size is a factor here, too. Larger companies witnessed more impact from COVID-19. 93.5 percent of CISOs from companies with 1,001–2,000 employees reported an increase, and 93 percent of companies with 2,001–5,000 employees also reported a rise.

Have cyberattacks on your company become more or less sophisticated in the past 12 months?

Levels of attack sophistication remain high, with 80 percent reporting a rise in sophistication. But this has dropped compared to the last Security Insights Report (88 percent).

One-fifth (21 percent) of those who had a cyberattack said that attacks had become significantly more sophisticated. 8 percent said there had been no change in the sophistication of attacks, and 11 percent claimed attacks had become less sophisticated.

Significant increases in sophistication were particularly high in retail and media, both at 29 percent, and financial services (27 percent). Overall, 76 percent of manufacturing respondents witnessed an increase in attack sophistication.

Generally, the larger the organisation, the more likely they were to face more sophisticated attacks. 89 percent of organisations with 2,001–5,000 employees noted an increase in attack sophistication, compared to only two-thirds (62.5 percent) of those with 251–500 workers.

> 80 percent of surveyed CISOs have seen attacks grow more sophisticated.

What has been the most prolific (i.e., most frequent) type of cyberattack your company has experienced in the past 12 months?

The most frequent attacks Australian organisations face has changed since the last report. Third-party apps top the list (16 percent), followed by ransomware (11 percent), custom malware (10 percent), and 5G-related technology (8 percent).

Custom malware attacks have vastly reduced this year, from 19 percent in last year's report to 10 percent. Google Drive attacks have also more than halved to 4.6 percent from 12 percent in 2020. Other prolific attacks in the June 2020 report were related to SSH (10 percent), process hollowing (10 percent), and island hopping (4 percent).

The manufacturing sector was most likely to have experienced attacks via third-party apps (24 percent).

How often has your company been breached by a cyberattack in the past 12 months?

96 percent of CISOs reported their company had been breached by a cyberattack in June 2020. This figure dropped to 77 percent in this report, which is good news for Australian respondents and indicates that systems have been doing their jobs. However, this could be down due to a lack of visibility as employees move to remote working.

There has been a slight rise in the average number of breaches reported, from 2.05 in June 2020 to 2.33 for Australian respondents.

The financial services sector suffered higher-than-average breach frequency at 2.86 per respondent organisation. Government respondents reported lower breach numbers (1.73), as did healthcare (1.24).

Breach frequency is high at organisations with 2,001–5,000 employees, with each experiencing 2.9 on average.

What was the prime cause of these breaches?

For 26 percent of CISOs surveyed who suffered a cyberattack, ransomware was the prime cause. Third-party apps were also high in second place with 19 percent. For 18 percent of respondents, the unwelcome discovery that their processes were not as strong as they thought they were led to breaches. Out-of-date security was the fourth most common cause for Australian organisations with 16 percent. OS vulnerabilities (4.6 percent) complete the top five.

In the June 2020 report, the top three causes of breaches were OS vulnerabilities, third-party application attacks, and web application attacks.

Again, we can see the rapid pivoting to home working is exposing out-of-date technology and process weakness. At the same time, ransomware is increasing as a prime cause alongside third-party apps.

Third-party apps were a particular problem in government, healthcare and manufacturing companies, causing more than a fifth of breaches, at 22 percent, 23 percent and 29 percent, respectively. Healthcare organisations were also disproportionately affected by ransomware, which was at the root of 44 percent of breaches.

What percentage of the breaches by a cyberattack in the past 12 months do you believe were a material breach (i.e., you had to disclose them to regulators/call in an incident response team to recover, etc.)?

When a breach does happen, it is serious business. Most respondents (78 percent) had to report to regulators or engage an IR firm to overcome the problems caused by breaches.

> 78 percent of organisations suffered a material breach.

53 percent of respondents who suffered a cyberattack said that between 21–30 percent were material breaches, and a further 15 percent said 31–40 percent of breaches were material.

In the government sector, 47 percent of respondents said that 21–30 percent of breaches were material.

What were the consequences of these breaches from financial and reputational perspectives to your company?

Only 9 percent of respondents who suffered a cyberattack said they suffered negative financial impact due to a data breach suffered by their organisation. The percentage claiming no financial impact from a breach was more than half (64 percent), and almost a quarter (24 percent) of respondents said they didn't know what financial impact the breach had.

Overall, the effect on brand reputation was greater. 81 percent of respondents said their brand had been negatively affected by a data breach, with 9 percent admitting this was severe. This was slightly down from nine in 10 respondents who reported damage to their corporate image in the June 2020 report. Only 14 percent said there was no reputational loss when a breach occurred.

So, reputational impact is far outstripping financial impact when it comes to breaches.

How fearful are you of the material breaches that you believe your organisation will be hit with in the next 12 months?

What is the psychological position of CISOs around breach risk? Almost two-thirds of Australian respondents (59 percent) are fearful they will experience a material breach in the coming year. Only 3.6 percent of CISOs don't think they will have a material breach. Nearly one-fifth (19 percent) of these respondents admitted to being very fearful.

The financial services and government sectors are highly concerned, with 66 percent and 65 percent of respondents, respectively, saying they fear a breach.

22 percent of respondents with an IT team of 31–40 people admitted to being very fearful.

How are you addressing this (the likelihood of breaches), if at all?

There are signs of consolidation of technology and the adoption of a more intrinsic approach to security as nearly half said **they are building more security into their infrastructure and apps, and reducing the number of point solutions to mitigate the risk (46 percent)**. This is a sign of a maturing approach that recognises security cannot be bolted on, siloed and threat-centric; it has to be unified, context-centric and built in.

A similar number said they had **updated their security policy and approach to mitigate the risk (46 percent)**.

The most selected answer was they have **updated their security technology to mitigate the risks** (48 percent). This is followed by increasing security budget, selected by 47 percent.

49 percent of respondents in the government sector said they have **adapted their security to mitigate the risk**.

> 46 percent plan to build more security into their infrastructure and apps, and reduce the number of point solutions.

48 percent of those in the financial services sector have **adapted their security to mitigate the risk,** while half of healthcare respondents said they were **building more security into their infrastructure and apps, and reducing the number of point solutions**.

To what extent do you agree or disagree with the following statements relating to developing and consuming apps in your organisation?

When asked about the changing way they are viewing security challenges around app development and consumption in their organisation, our respondents offered insight into the issues they are facing.

Visibility is a definite concern. 57 percent agree they **need better visibility over their data and apps to pre-empt attacks**.

56 percent of Australian respondents agreed that the changes to the attack landscape wrought by COVID-19 require a security rethink, agreeing that they **need to view security differently than they have done previously as the attack surface has expanded**.

Nearly two-thirds (60 percent) agree they **need better contextual security in place to track data/security through the lifecycle**. This points to a prevailing environment where security tends to be threat-centric and reactive. CISOs are recognising that dynamic environments require a context-centric approach.

Australian CISOs surveyed are under no illusions about the mission-critical nature of app security to their business. 64 percent agreed that **their ability to innovate as a business depends on their ability to build, manage and distribute apps more securely**.

57 percent of respondents **feel confident in bringing new apps to market because they know they will be secure**.

Asked about their view of AI in secure app development, respondents showed signs of conflict. 48 percent agree **security concerns are holding them back from embracing AI/ML-based apps to improve services**, but 57 percent agree they **would like to use more AI and ML in their apps to improve security and services**.

Less than half of respondents (45 percent) agreed that **there is too much complexity in the security solutions market to make them change their security policy even though they know today's IT security is not working**, indicating that vendors have work to do to simplify their proposition into a unified approach.

Finally, 54 percent agreed that app security is getting board-level attention, and that their **board/senior leadership team feels increasingly worried when they bring new apps to market because of the growing threat and damage data breaches/ attacks have**.

What do you believe to be the most vulnerable breach point on the journey of data within your security infrastructure, and has this changed in the past 12 months?

Applications were designated the most vulnerable breach point on the data journey, and it is clear this has been a concern for some time. What is most interesting is that workloads are significantly rising as a source of perceived vulnerability. We are likely to see organisations placing more focus on tackling this risk in the coming year.

37% Apps

18.3% are now and were 12 months ago, 18.7% are now and weren't 12 months ago

21% Workload

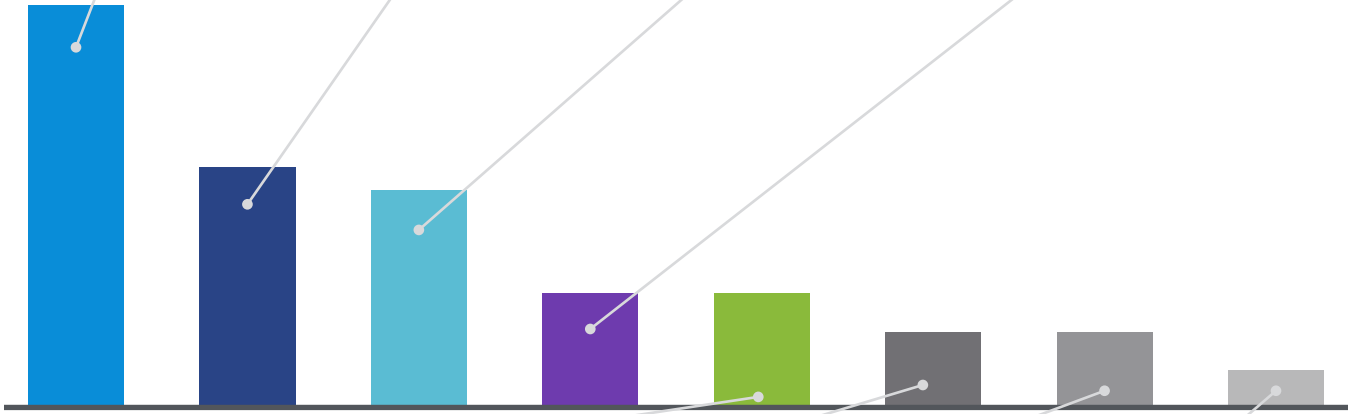
2.4% are now and were 12 months ago, 18.3% are now and weren't 12 months ago

20% Network

15.9% are now and were 12 months ago, 4% are now and weren't 12 months ago

7% Cloud

3.2% are now and were 12 months ago, 4% are now and weren't 12 months ago



6% Endpoint

4.4% are now and were 12 months ago, 1.6% are now and weren't 12 months ago

4% Edge

2% are now and were 12 months ago, 2.4% are now and weren't 12 months ago

4% Container

3.2% are now and were 12 months ago, 0.8% are now and weren't 12 months ago

0.8% Don't Know

How have organisations coped with the challenges of pivoting to remote working?

We asked surveyed CISOs to rate their success in switching the workforce to remote-first working and whether a security-first approach would have helped a more effective transition.

66 percent agree they've been able to get their workforce up and running remotely, and security has not been a barrier. This is testament to the work of security teams that have been at the heart of operations more than ever before.

Respondents acknowledge there is always room for improvement, with 76 percent agreeing a security-first approach would have increased their ability to enable employees to work from alternative locations and remain productive. This was also confirmed in earlier VMware research that found the inability to implement multifactor authentication was the biggest concern for IT professionals in their response to the shift to home working. Now that the profile of security has risen, it should be easier for CISOs to secure board support for a security-first approach.

Do you use or plan to use a cloud-first security strategy?

99 percent already use or plan to adopt a cloud-first approach to protect the organisation.

Respondents universally stated they are planning to shift to a cloud-first security strategy—if not immediately, it is firmly on the roadmap.

62.5 percent overall say they have been using a cloud-first approach for more than one year, while 24 percent say they have been cloud-first for less than 12 months. A further 5.2 percent plan to become cloud-first in the coming year, while the switch is further down the track for 6 percent.

Cloud-first strategy is prevalent among government and financial services companies, where 92 percent and 82 percent, respectively, say they are cloud-first already.

Key Insights and Actions

Our fourth Australia Security Insights Report finds that senior cybersecurity professionals and the organisations they serve continue to face high-volume, sophisticated threats. These are exacerbated by the pivot to a highly distributed workforce and, though most organisations have managed to shift to remote working, CISOs acknowledge that a security-first approach would have made the transition easier.

Undoubtedly, COVID-19 changed the cybersecurity environment significantly and will continue to influence security strategy. For its part, the cybersecurity industry must focus on delivering solutions that reduce operational complexity while robustly protecting the distributed work environments that will become the default future state for most organisations.

Analysis of the survey responses reveals important areas for cybersecurity attention in the coming year.

Prioritise improving visibility

Organisations have a visibility problem resulting from the rapid switch to home working. The true scale of attacks is hard to discern because defenders can't see into the corners where personal mobile devices and home networks have been grafted on to the corporate ecosystem. Add to this the challenges of monitoring third-party apps and vendors, and the number of blind spots escalates.

Put simply, defenders don't know what they don't know, and businesses are exposed as a result. This limited contextual insight into risk puts defenders at a disadvantage when protecting the extended attack surface. Organisations must prioritise improving visibility into all endpoints and workloads to secure the remote work environment. Robust situational intelligence that gives context to threats will help defenders prioritise and remediate risk with confidence.

Respond to the resurgence of ransomware

Cyberattacks have continued to increase in sophistication, and ransomware is no exception. Attackers are gaining undetected access to networks, exfiltrating data, and establishing back doors before launching ransom demands and/or directly monetising stolen data. To avoid becoming victim to repeated attacks, organisations need to combine advanced ransomware protection with robust post-attack remediation that detects the continued presence of adversaries in their environment.

Continue to address ineffective legacy security technology and process weakness

Out-of-date security and process weaknesses continue to pose significant risk to organisations, and the switch to remote working has exposed them still further. As we emerge from the immediate response phase and begin to see the shape of the long-term future, organisations must identify the critical changes to processes and technology needed to support remote and hybrid workers to work securely and reduce risk.

Deliver security as a distributed service

There was a time when security teams were securing company-owned desktops for employees working on campus, connecting to corporate applications running on servers in a company-owned data centre. The world is a more complicated place today with remote workers connecting to applications running on infrastructure that may or may not be managed, owned or controlled by the company. With so many new surfaces and different types of environments to defend, security cannot be delivered as a litany of point products and network choke points. Instead, endpoint and network controls must be delivered as a distributed service. This means delivering security that follows the assets being protected, no matter what type of environment you have.

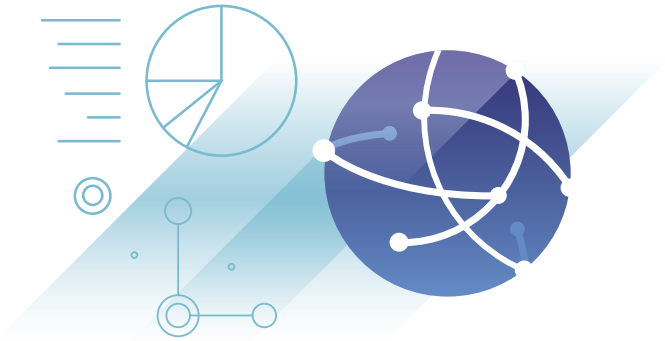
Adopt an intrinsic approach to cloud-first security

The biggest change uncovered by our research is the shift to a cloud-first security strategy. It is difficult to overstate the magnitude of shift that has occurred in such a short space of time; very few CISOs before 2020 described their security strategy as cloud-first. It is the logical result of organisations having to respond to the sudden highly distributed working practices caused by COVID-19.

But moving to the cloud is not a security panacea. Not all clouds are equal, and controls need to be vetted by consumer organisations because if adversaries want to attack at scale, the cloud is the place to do it. As this shift builds momentum, investment in public cloud security will be critical. When you move to a public cloud, you're moving to a very tough neighbourhood where security is contingent on your own actions and those of your neighbours. You may be able to secure your own resources, but you have no control over those sharing that environment with you. Organisations must prioritise securing cloud workloads at every point in the security lifecycle as the great cloud shift continues.

Ultimately, the 2021 VMware Australia Security Insights Report shows an industry that is focused on building on the successes of the past year and responding to the changing threat environment. CISOs have a strong sense of the direction they need to travel and the tools they need to leverage to help stay one step ahead of attackers.

Methodology



VMware commissioned a survey, undertaken by an independent research organisation, Opinion Matters, in December 2020. **251 Australian CIOs, CTOs and CISOs** were surveyed from companies in a range of industries, including financial, healthcare, government and local authority, retail, manufacturing and engineering, food and beverage, utilities, professional services, and media and entertainment. This is the fourth Australia Security Insights Report from VMware, building on the previous survey that was undertaken in June 2020. This forms part of a global research project across **14 countries**, including the United Kingdom, Canada, Saudi Arabia, the United Arab Emirates, the United States, France, Germany, Spain, the Netherlands, the Nordics, Italy, Japan, Singapore, and Australia.

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app moderisation, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit vmware.com/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com