vmware®

Global Security Insights Report

Extended enterprise under threat

2021

Introduction

This research was conducted to understand the challenges and issues facing businesses worldwide 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 organizations' plans for securing new technology, adopting a cloud-first security strategy, and dealing with the complexity of the current cybersecurity management environment.

3,542 CIOs, CTOs and CISOs were surveyed from companies in a range of industries for this report. This forms part of a global research project across 14 countries.

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

Management Summary:

Foreword

INSIGHTS FROM THE GLOBAL 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 Global 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 programs 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 balance the demands of work and family. 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 (76 percent) of the 3,542 respondents to our survey said the number of attacks they faced has increased in the past year. Of those, 78 percent said attacks had increased as a result of more employees working from home. 79 percent said attacks had become more sophisticated.

The result? The number of breaches has risen, with respondents who had a cyberattack reporting **2.35 breaches on average per year**. 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: 56 percent of the CISOs surveyed fear that their organization 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 behavior, personal devices, and home network use reduce visibility, creating blind spots and dark corners where attacks go undetected. Consequently:

78%

said attacks increased as a result of home working

2.35

breaches on average have been reported per organization

82%

said they had suffered a material breach

Third-Party Apps and Ransomware Are the Leading Breach Causes

When asked what is causing breaches, three vectors almost tied at the top to build a picture of external threats and internal weaknesses. Third-party applications were the most common culprit, followed closely by ransomware and out-of-date security technology.

The rapid pivot to work from anywhere has exposed organizations that had lapsed in security hygiene and failed to implement multifactor authentication, while process weakness and OS vulnerabilities were also common breach causes.

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 capitalize 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.

14% of all breaches globally were caused by ransomware.

Healthcare held hostage

19% of healthcare sector breaches globally were the result of ransomware.

Apprehension Around App Development and Consumption

Third-party apps are the leading cause of breaches 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 two-thirds of respondents agree[1] they need better visibility over data and apps to prevent attacks. A similar number agrees that better contextual security is needed to track data security through the application lifecycle. The impact of COVID-19 is recognized as three in five respondents agree they need to view security differently than they did in the past due to an expanded attack surface.

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

Workloads are rising significantly as a source of perceived vulnerability.

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

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

A further 4 percent said they had been the most vulnerable point for more than 12 months. Teams are recognizing 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 recognizing attacker behavior. This year, we anticipate organizations will be looking to address these gaps and strengthen defenses 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 organizations are accelerating their cloud security roadmap in response to the challenges of COVID-19. It may be a road they were already traveling, 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 Global Security Insights Report** revealing and informative.

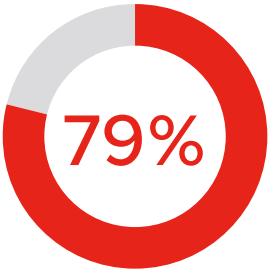
Key Findings

Attack frequency and breach risk remain high

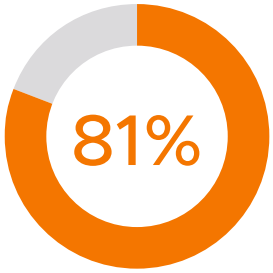
The frequency of attacks is high, their sophistication continues to grow, and breaches are the inevitable result.

76% said attack volumes had increased in the last 12 months, by an average of 52 percent across all affected organizations.

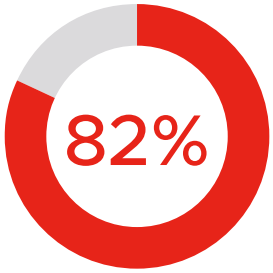
78% of those who have had a cyberattack said attacks increased due to more people working from home.



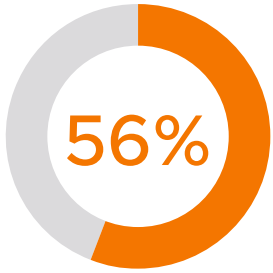
of those who had a cyberattack said attacks were more sophisticated.



have suffered a breach in the past 12 months, with those who have been breached experiencing an average of 2.35 breaches during that time period.



said the breaches they suffered were material.



fear a material breach in the next 12 months.

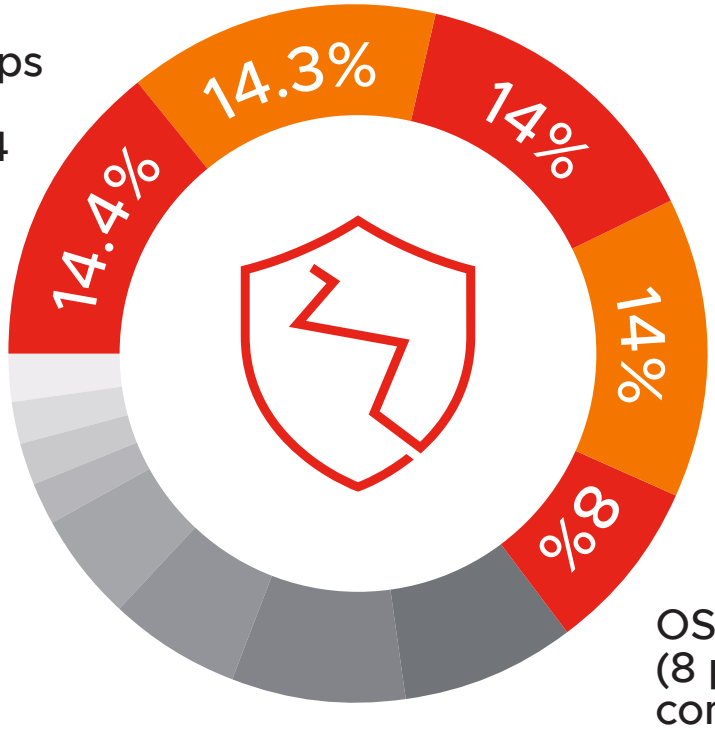
Apps, workloads and ransomware top ciso concerns

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

Top breach causes for those who had a cyberattack:

Ransomware was second with 14.3 percent.

Third-party apps were the top cause with 14.4 percent.



Out-of-date security tech and process weaknesses tied in third with 14 percent.

OS vulnerability (8 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 area 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.

61% nearly two-thirds agree they need to view security differently than they have previously as the attack surface has expanded.

63% agree they need better contextual security in place to track data through the lifecycle.

63% 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, while increasing their security budget to achieve these aims.

43% are building more security into their infrastructure and apps, and reducing the number of point solutions.

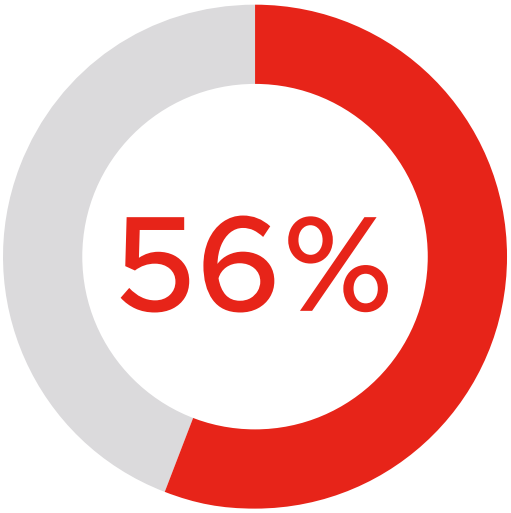
42% have updated their security technology to mitigate risk.

41% have updated their security policy and approach to mitigate risk.

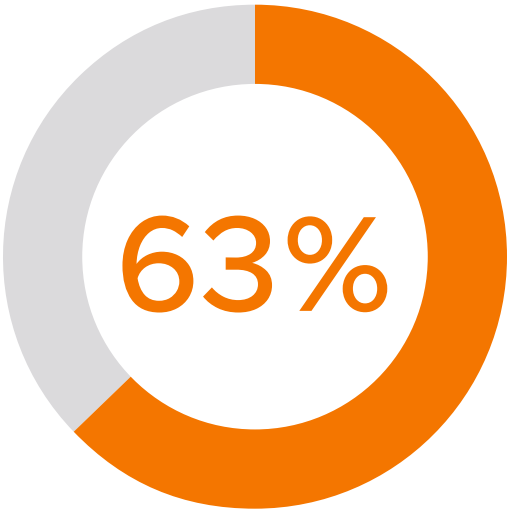
98% already use or plan to shift to a cloud-first security strategy.

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.

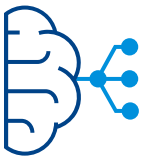


Yet, more than half of respondents worldwide (56 percent) agree security concerns are holding them back from embracing AI/machine learning (ML)-based apps to improve such services.



63 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.

57%

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.

60%

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

62%

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

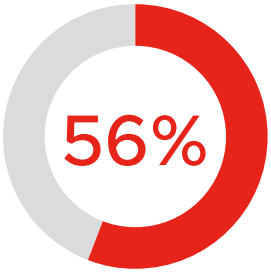
Securing brand and reputation—does it command more urgency for change?

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

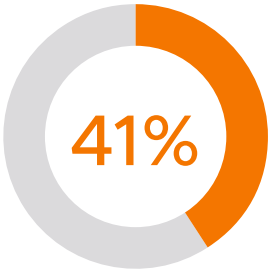
↗ 75% of those who suffered a cyberattack say there was some kind of negative impact on reputation—up from 70 percent in June 2020.

↗ 82% of respondents had to report to regulators or engage an IR firm to overcome the reputational problems caused by material breaches within 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 that 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?

76 percent of the CISOs surveyed said they experienced an increase in the number of cyberattacks on their organization in the past 12 months. This rose to 89 percent in the financial services sector.

Regionally, more respondents from Saudi Arabia were experiencing increases in attack volume, with 92 percent reporting an increase. At the other end of the scale, only 64 percent of respondents from Singapore had seen an increase.

The average increase in attacks experienced was 52 percent, and 37 percent of respondents said attack volumes increased by 51–300 percent. Spain reported the highest average increase at 69 percent.

Size matters when it comes to the volume of attacks faced. Only 69 percent of businesses with 251–500 employees say the volume of attacks increased, compared to 93 percent of those with between 5,001–10,000 employees.

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?

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

France saw the biggest attack increase due to home working with 96 percent seeing an upswing, while the UK (86 percent) and Australia (89 percent) also saw increased attack frequency. Remote working proved slightly less of a problem in the U.S. and Nordic regions with only 63 percent seeing more attacks.

Again, size is a factor. 76 percent of small organizations (251–500 employees) say home working led to an increase in attacks, compared to 89 percent of those with 5,001–10,000 workers.

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

When it comes to attack sophistication, **79 percent of CISOs surveyed who had a cyberattack have seen attacks grow more sophisticated.** This is in line with the 80 percent who said the same in the June 2020 Security Insights Report. 49 percent say they are significantly or moderately more sophisticated.

CISOs surveyed in France are most likely to have seen sophistication rise with 89 percent reporting more complex attacks. Only 66 percent of respondents in Italy say the same.

Adversaries are directing their more sophisticated tactics, techniques and procedures (TTPs) at larger organizations. 90 percent of those with 5,001–10,000 employees who had a cyberattack saw sophistication increase, compared to only 78 percent of those with 251–500 employees. This reflects that the bigger the enterprise, the more valuable and voluminous the data it holds, meaning there is more opportunity for cybercriminals to monetize their work.

> 79 percent of CISOs surveyed who had a cyberattack 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?

Cloud-based attacks are the most frequently experienced, but the proportion of all attacks that they represent has almost halved in the past 12 months from 18 percent to 10 percent. Taking the place of those attacks is ransomware, which has surged compared to June 2020. It now constitutes 9 percent of all attacks, compared to just 4.5 percent in our last Security Insights Report. This chimes with the experience of the VMware Threat Analysis Unit™, which noted a 900 percent increase in ransomware over the first half of 2020, and points to the double-extortion tactics that have grown to prominence in 2020.

In Germany, France, the U.S., the UK, the Nordics and Japan, ransomware was the most commonly experienced attack type.

Attacks on third-party apps were the third most commonly experienced, comprising less than 9 percent of attacks. In the Netherlands, they were more common, comprising 15 percent of attacks, and they were the most experienced attack type in Canada and Australia.

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

More than eight out of 10 of the organizations surveyed suffered a breach in the past year. This is down from 94 percent that reported falling victim to a breach in June 2020.

The average figure disguises some significant regional variation. 97 percent of French organizations and 93 percent of those from the Kingdom of Saudi Arabia said they suffered a breach. At the other end of the scale, only two-thirds (66 percent) of respondents from Singapore and 69 percent from the UK suffered breaches.

> More than eight out of 10 of the organizations surveyed suffered a breach in the past year.

Those who did have breaches are typically having more of them.

On average, CISOs surveyed report they have been breached 2.35 times over the past year, up from 2.17 times in June 2020. 59 percent said they suffered a single breach, but a concerning 14 percent suffered five or more breach incidents.

The U.S. had the highest average number of breaches at 3.44, while Spain fared the best with only 1.6.

What was the primary cause of these breaches?

Third-party applications are the top cause of breaches, accounting for 14 percent of all incidents experienced. This is followed by ransomware and out-of-date security technology (both fractionally lower than 14 percent).

The Netherlands is seeing a particular problem with third-party apps, with 36 percent of organizations saying they are the most common cause of breaches. In terms of vertical sector, 16 percent of government respondents and 21 percent of media and entertainment companies said third-party apps were the prime cause of breaches.

Ransomware is the top cause of breaches in France, Germany, the Nordics, Australia and Japan.

Healthcare is particularly affected by ransomware, with almost one-fifth (19 percent) of respondents in the healthcare industry saying this was the prime breach cause.

Out-of-date security is the primary problem for 19 percent of manufacturing and automotive respondents.

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 (82 percent) had to report to regulators or engage an IR firm to overcome the problems caused by breaches.**

Most respondents (82 percent) had to report to regulators or engage an IR firm to overcome the problems caused by breaches.

The percentage experiencing material breaches was highest in the Kingdom of Saudi Arabia (94 percent) and high in Spain and the U.S., where 92 percent and 90 percent were judged to be material, respectively. Singapore fared better, with only 68 percent reporting material incidents.

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

Less than one-quarter (24 percent) of respondents who suffered a cyberattack said they suffered negative financial impact due to a data breach suffered by their organization. This dropped from 30 percent who said the same in June 2020. However, the percentage saying they saw no negative financial impact dropped from 56 percent to 51 percent. There was a big increase in the proportion who simply don't know what financial impact the breaches caused. 20 percent said they had no idea, compared with 9 percent in June 2020.

Again, there were large regional variations. The financial penalties of breaches were more keenly felt in the UAE, with 47 percent reporting negative impact, and the Netherlands, where 40 percent said the same. At the other end of the scale, only 6 percent in Canada, 9 percent in Italy, and 10 percent in the UK said their business suffered financially due to a breach.

Professional services companies were most likely to report financial impact due to a breach, with 32 percent having recorded losses. 83 percent in this sector said they also suffered reputational damage.

Overall, the effect on brand reputations was larger. Three-quarters of respondents said their brand was negatively affected by a data breach, rising to 89 percent in Japan, and 83 percent in France and Singapore.

Only 19 percent said there was no reputational loss suffered when a breach occurred, a drop from almost one-quarter that said this in 2020.

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

There is a significant fear factor associated with the potential for material breaches in the coming year. More than half (56 percent) are very or somewhat fearful that a breach will hit their business. This rises to 74 percent in France and is lowest in the Netherlands at 37 percent.

The financial services sector and retail sector are most concerned, with 67 percent of respondents in both areas saying that they fear a material breach. Only half of government and healthcare organizations are worried about a breach.

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

When asked about their plans to mitigate breach risk, respondents were prioritizing simplification and consolidation of security solutions with making security intrinsic. Updating technology and policy and committing budget to the issue were also important.

43 percent of respondents said they plan to **build more security into their infrastructure and apps, and reduce the number of point solutions**. This rose to 48 percent in the retail and food and beverage sectors.

More than half of respondents in Italy, Germany, Singapore and Japan plan to adopt intrinsic security and reduce the number of point solutions they use, while this approach is less mature in the Netherlands (32 percent), Canada (34 percent) and the UAE (37 percent).

42 percent said they have **updated their security technology to mitigate the risk**. Respondents from the travel and transport sector are most likely to have taken this approach (54 percent).

Technology updates are most common in Singapore (51 percent), Japan (50 percent) and Australia (48 percent). Least likely to be taking this approach are respondents from Canada (30 percent), the UAE (33 percent) and Spain (35 percent).

41 percent said they **updated their security policy to mitigate risk**—an important tactic given the significant changes to the security landscape in the past year. Media and entertainment companies most favored this tactic (44 percent).

Japan (50 percent), the Nordics (49 percent) and Germany (47 percent) are most likely to be updating security policies to help manage breach risk.

40 percent **adapted security to mitigate risk**, while 39 percent **increased security budget**. The retail (44 percent), healthcare (42 percent) and financial services (41 percent) sectors are more likely to be increasing their budgets.

Japanese respondents (48 percent) are the most likely to be increasing budget, while Italy is least likely at 32 percent.

It is interesting that organizations are putting strategy ahead of simply throwing money at the problem, with increasing budget a lower overall priority than other areas.

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

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

Visibility is a definite concern. 63 percent agree that they **need better visibility over their data and apps to pre-empt attacks**. This rises to 73 percent in the **travel and transport** and **utilities sectors**, and is a prime concern in France, where 84 percent of respondents agreed or strongly agreed.

61 percent of respondents worldwide 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**. Again, those in **travel and transport** and **utilities** are more likely to take this view.

Almost two-thirds (63 percent) agree they **need better contextual security in place to be able to track data/security through the lifecycle**. This points to a prevailing

environment where security tends to be threat-centric and reactive. CISOs are recognizing that dynamic environments require a context-centric approach.

CISOs surveyed are under no illusions about the mission-critical nature of app security to their business. 63 percent agreed that their **ability to innovate as a business depends on their ability to build, manage and distribute apps more securely**. Unsurprisingly this is most keenly felt in consumer-facing industries, with retail (74 percent) and travel and transport (75 percent) sector respondents most likely to agree with this statement.

62 percent of respondents **feel confident in bringing new apps to market because they know they will be secure**. Those in the UAE and Saudi Arabia are most confident bringing apps to market, with 82 percent and 83 percent agreeing, respectively. In contrast, Spanish CISOs are least confident, with only 39 percent agreeing they feel confident and 23 percent saying they are not confident in launching secure apps.

Asked about their view of AI in secure app development, respondents showed signs of conflict. 56 percent agree **security concerns are holding them back from embracing AI/ML-based apps to improve services**, but 62 percent agree **they would like to use more AI and ML in their apps to improve security and services**.

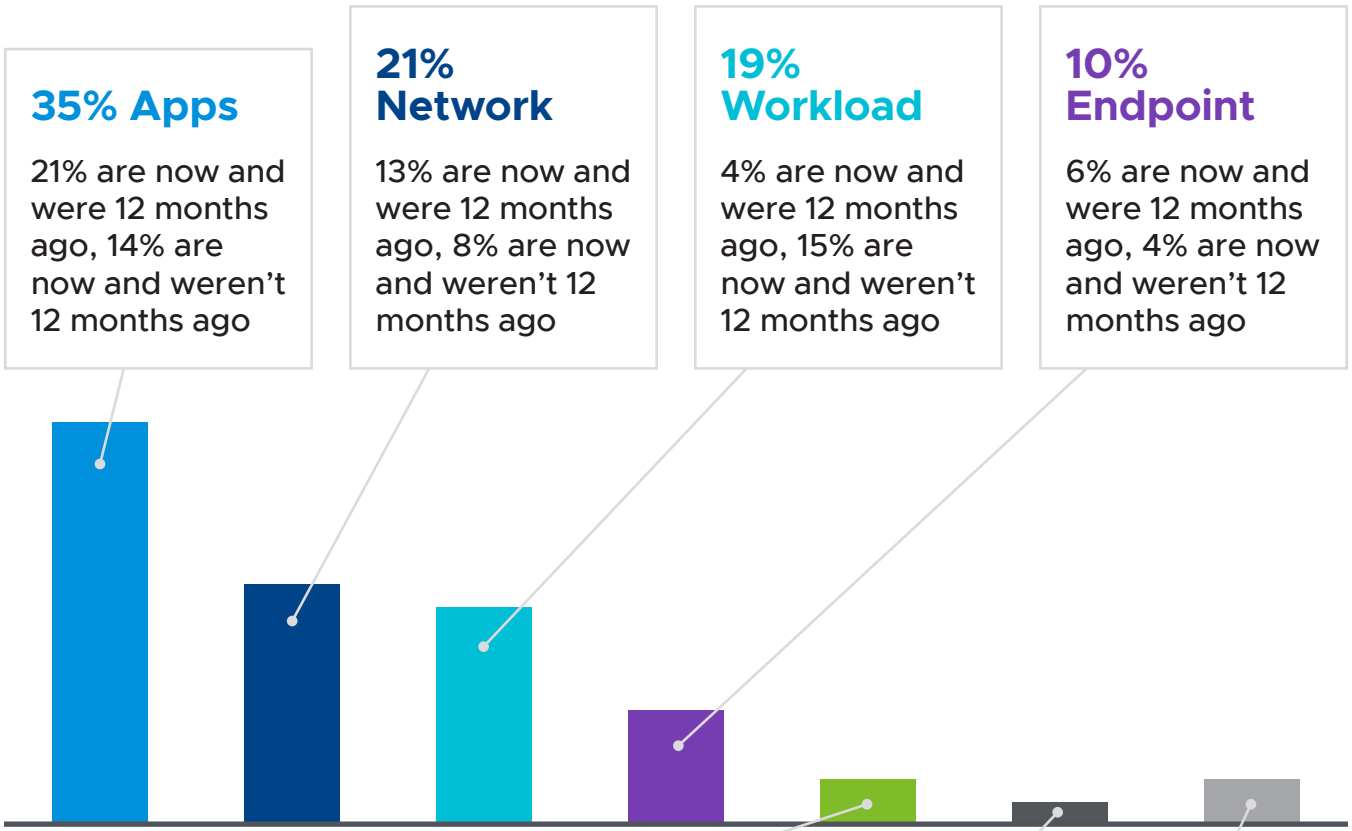
More than half of respondents (57 percent) agreed that **there is too much complexity in the security solutions market to make them change their security policy even though they know today's IT security is not working**, indicating that vendors have work to do to simplify their proposition into a unified approach.

Finally, 60 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/services to market because of the growing threat and damage data breaches/attacks have**. Boards are most likely to be concerned in utilities companies, with three-quarters of CISOs saying the board is worried. This is followed again by the consumer-facing sectors of retail and travel and transport.

Boards in Saudi Arabia and the UAE are most likely to be concerned about app and services launches, with 83 percent and 74 percent agreeing, respectively.

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?

Apps lead this area, which has clearly been a concern for some time. What is most interesting is that workloads are significantly rising as a source of perceived vulnerability.



35% Apps

21% are now and were 12 months ago, 14% are now and weren't 12 months ago

21% Network

13% are now and were 12 months ago, 8% are now and weren't 12 months ago

19% Workload

4% are now and were 12 months ago, 15% are now and weren't 12 months ago

10% Endpoint

6% are now and were 12 months ago, 4% are now and weren't 12 months ago

4% Cloud

2.5% are now and were 12 months ago, 1.9% are now and weren't 12 months ago

2% Container

1.7% are now and were 12 months ago, 0.6% are now and weren't 12 months ago

4% Don't Know

How have organizations 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.

54 percent agree they've been able to get their workforce up and running remotely, and security has not been a barrier. This is a testament to the work of security teams that have been at the heart of operations more than ever before. There are significant regional variations, however, with only 33 percent of UK respondents agreeing that they got their workforce up and running without a hitch—22 percent disagree. Conversely, 76 percent of French CISOs surveyed had few problems.

Respondents acknowledge there is always room for improvement, with 60 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?

> 98 percent overall already use or plan to adopt a cloud-first approach to protect the organization.

Respondents almost universally stated that they are planning to shift to a cloud-first security strategy—if not immediately, it is firmly on the roadmap. **98 percent overall already use or plan to adopt a cloud-first approach to protect the organization.**

100 percent of U.S. respondents are headed for the cloud, but only a comparatively low 87 percent of those in the Netherlands say the same.

46 percent overall say they have been using a cloud-first approach for more than one year, while 30 percent say they have been cloud-first for less than 12 months. A further 11 percent plan to become cloud-first in the coming year, while the switch is further down the track for 11 percent.

Cloud-first maturity is highest in Australia, where 63 percent have been cloud-first for more than 12 months. It is lowest in Canada, where only 25 percent say the same.

Key Insights and Actions

Our fourth Global Security Insights Report finds that senior cybersecurity professionals and the organizations they serve continue to face high-volume, sophisticated threats. These are exacerbated by the pivot to a highly distributed workforce and, though most organizations 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 organizations.

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

Prioritize improving visibility

Organizations 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. Organizations must prioritize improving visibility into all endpoints and workloads to secure the remote work environment. Robust situational intelligence that gives context to threats will help defenders prioritize 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 monetizing stolen data. To avoid becoming victim to repeated attacks, organizations 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 organizations, and the switch to remote working has exposed them further. As we emerge from the immediate response phase and begin to see the shape of the long-term future, organizations 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 center. 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 organizations 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 organizations 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 neighborhood where security is contingent on your own actions and those of your neighbors. You may be able to secure your own resources, but you have no control over those sharing that environment with you. Organizations must prioritize securing cloud workloads at every point in the security lifecycle as the great cloud shift continues.

Ultimately, the 2021 VMware Global 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 organization, Opinion Matters, in December 2020. **3,542 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 Global Security Insights Report from VMware, building on the previous surveys that were undertaken in February 2019, October 2019 and June 2020. This forms part of a global research project across **14 countries**, including Australia, Canada, Saudi Arabia, the Middle East, the United Kingdom, France, Germany, Spain, the Netherlands, the Nordics, Italy, Japan, Singapore, and the United States.

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, 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