vmware®

United States

U.S. Security Insights Report

Extended enterprise under threat

2021

Introduction

This research was conducted to understand the challenges and issues facing businesses in the United States (U.S.) 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 U.S. organizations' 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 defenses to make security intrinsic to infrastructure and operations.

Management Summary:

Foreword

INSIGHTS FROM THE U.S. 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 second edition of our U.S. 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 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.

More than three-quarters (77 percent) of the 251 respondents to our survey said the number of attacks they faced increased in the past year. Of those, 63 percent said attacks increased as a result of more employees working from home. 70 percent said attacks had become more sophisticated.

The result? The number of breaches has risen, and respondents who had a cyberattack reported **3.44 breaches on average per year**. Nor were these minor incidents. In nine 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: 62 percent of the U.S. CISOs surveyed fear 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:

63%

said attacks increased as a result of home working

3.44

breaches on average have been reported per organization, per year

90%

said they had suffered a material breach

Process Weakness, Out-of-Date Security Technology, and the Supply Chain 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. Process weakness was the most common cause, at the root of 15 percent of breaches, closely followed by out-of-date security technology and then by breaches via the supply chain.

The rapid pivot to work from anywhere exposed organizations that had lapsed in security hygiene and failed to implement multifactor authentication, while the extended enterprise is under increasing tension as third parties introduce significant breach risk.

In addition to these threats, the rapid escalation in ransomware has added unwelcome tension and was the fourth most common breach cause. 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.

11% of all breaches were caused by ransomware.

Apprehension Around App Development and Consumption

Third-party apps are a common cause of breaches according to our surveyed CISOs. Two-thirds say their ability to innovate as a business depends on them, 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.

13 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 5 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 under way. 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 second **VMware U.S. Security Insights Report** revealing and informative.

Key Findings

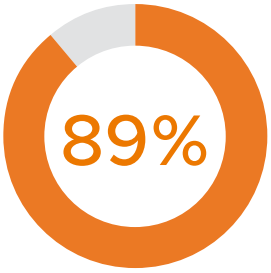
Attack frequency and breach risk remain high

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

77% said attack volumes increased in the past 12 months. The average reported increase among them was 67 percent.

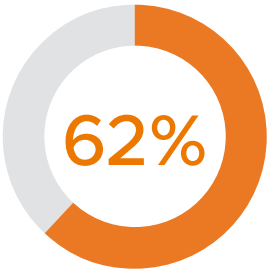
63% of those who had a cyberattack said attacks increased due to more people working from home.

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 3.44 breaches in that time period.

said the breaches they suffered were material.



fear a material breach in the next 12 months.

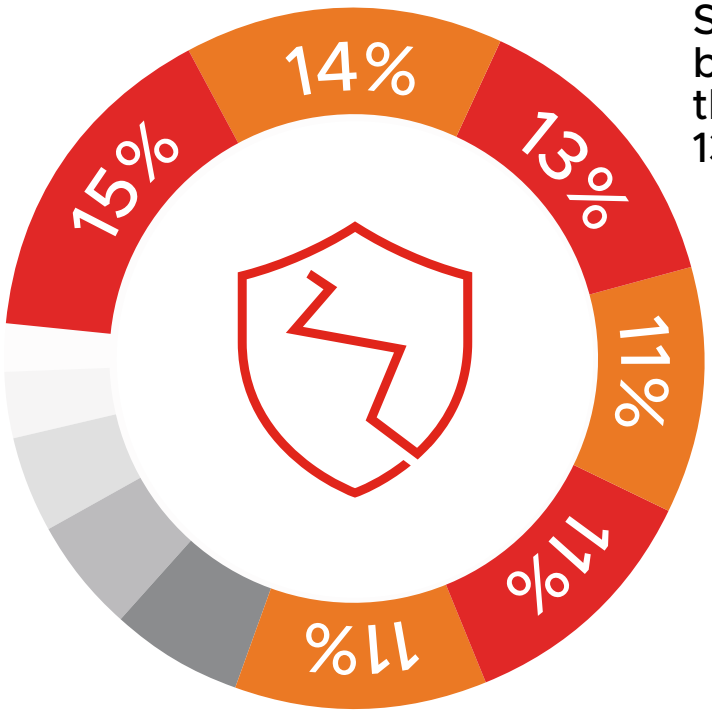
Process weakness, supply chain, and workloads top CISO concerns

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

Top breach causes for those who had a cyberattack:

Out-of-date security tech was second with 14 percent.

Process weaknesses topped the list with 15 percent.



Supply chain breaches were third with 13 percent.

Ransomware, web application attacks, and third-party apps (all 11 percent) complete the top six.

Apps and the network topped the list as the most vulnerable points 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.

63% agree they need to view security differently than they have previously as the attack surface has expanded.

66% agree they need better contextual security in place to track data through the lifecycle.

65% 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. 35 percent say they are increasing their security budget to achieve these aims.

38% have updated their security technology to mitigate the risk.

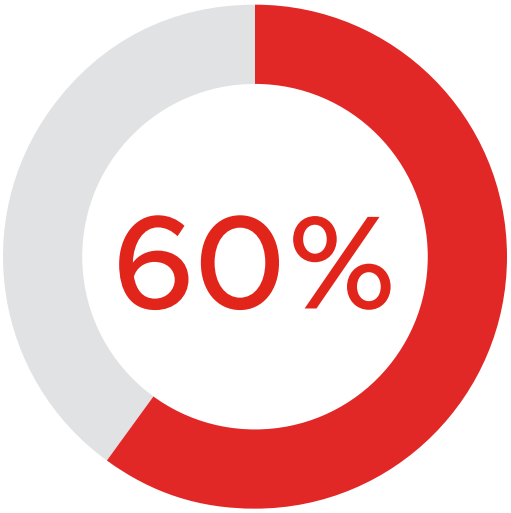
40% are building more security into their infrastructure and apps, and reducing the number of point solutions.

36% have updated their security policy and approach to mitigate risk.

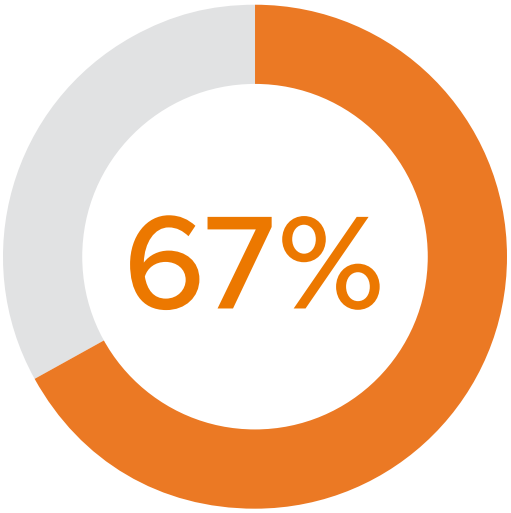
100% have shifted or plan to shift to a cloud-first security strategy.

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.

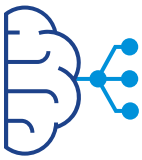


Yet, 60 percent of U.S. respondents agree security concerns are holding them back from embracing AI/machine learning (ML)-based apps to improve such services.



Two-thirds (67 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 market 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.

63% agree they would like to use more AI/ML in their apps to improve security and services.

65% agree they need better visibility over data and apps to pre-empt attacks.

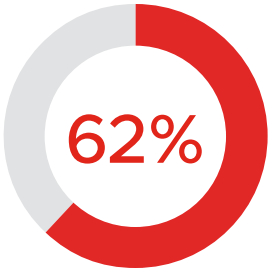
Securing brand and reputation—does it command more urgency for change?

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

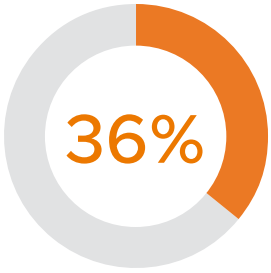
71% of those who suffered a cyberattack say there was some kind of negative impact on reputation—up from 62 percent in June 2020.

90% 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 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?

77 percent of the CISOs surveyed said they experienced an increase in the number of cyberattacks on their organization in the past 12 months. The average increase experienced was 67 percent. This rose to 86 percent in the financial services sector, where respondents had seen an average increase in attacks of a staggering 89 percent.

Respondents from the healthcare sector fared better than average, with 60 percent reporting attack volume increases.

Size matters when it comes to the volume of attacks faced. Only 60 percent of businesses with 251–500 employees say the volume of attacks increased, compared to 79 percent of those with 1,001–2,000 employees.

Similarly, larger IT teams suffered more attacks. Those with 41–50 people in their IT team reported an average attack volume increase of 90 percent, compared with an average increase of 83 percent among those with 31–40 people in their team.

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?

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

Three in five (60 percent) respondents from government organizations noted an increase in attacks connected to home working, while 65 percent of manufacturing respondents said the same.

Size is a factor here, too. 94 percent of organizations with 5,001–10,000 employees noted an increase in attacks due to home working, compared to only two-thirds (67 percent) of those with 251–500 workers.

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

When it comes to attack sophistication, 70 percent of CISOs surveyed who had a cyberattack have seen attacks grow more sophisticated. This is a drop from the 84 percent who reported increased attack sophistication in the June 2020 report and reflects the commoditization of malware.

40 percent of those who had a cyberattack say the attacks they face are significantly or moderately more sophisticated, indicating there is a kernel of bad actors that continues to develop and enhance attack techniques.

70 percent of CISOs surveyed who had a cyberattack have seen attacks grow more sophisticated.

Evidence suggests they may be directing these techniques at the financial services sector, where 84 percent reported increased sophistication and 63 percent said attacks had become moderately or significantly more complex. In contrast, the healthcare sector is less affected by evolving attack types, with only 21 percent noting moderate or significant advances in attack sophistication.

Adversaries are directing their more sophisticated tactics, techniques and procedures (TTPs) at larger organizations, with 88 percent of those with 5,001–10,000 employees seeing sophistication increase, compared to only 60 percent of those with 501–1,000 employees. This reflects the fact 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.

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

The U.S. attack environment is diverse, with few respondents experiencing the same mix of attack types and no single attack type dominating. This underlines the challenges U.S. CISOs face; they need to build strategic and tactical responses to an incredibly varied mix of attack vectors and techniques.

Attacks on the network and endpoints top the list, with 10 percent of respondents who had a cyberattack seeing these most frequently. However, ransomware and attacks via third-party apps are close behind as the top attack types for 8 percent of respondents in each case.

Commodity malware, Google Drive (cloud-based attacks), cryptojacking, and supply chain attacks each account for 7 percent for those who have been cyberattacked.

Government organizations are more likely to experience attacks on the network, with 18 percent of respondents saying this was the most common attack type they experienced. Ransomware is disproportionately targeted at the healthcare sector, with 17 percent seeing this most frequently. It was also more of a problem than average for financial services companies, affecting 12 percent.

In the manufacturing sector, attacks via third-party apps were the most commonly reported.

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

89 percent of surveyed organizations suffered a security breach in the past year.

Almost nine out of 10 of the CISOs who took part in our research said their organization suffered a breach as a result of a cyberattack in the past year (89 percent). This is down from 97 percent who reported falling victim to a breach in June 2020.

However, the average number of breaches suffered by each organization increased significantly, from 2.7 in June 2020 to 3.44 in this report. 32 percent of respondents said their organization had been breached five times or more.

The food and beverage sector suffered the highest average number of breaches at 5.67, while financial services companies suffered just 2.02 breach incidents. Other notable sectors reporting a higher-than-average breach frequency are professional services (4.42), manufacturing and engineering (4.11), and government (4.03).

Breach frequency is highest at midsize organizations with 1,001–2,000 employees, with each experiencing 4 on average.

High breach frequency is also found in organizations with larger IT teams of 31–40 people, reporting 4.04 breaches on average.

What was the prime cause of these breaches?

For 15 percent of CISOs surveyed who suffered a cyberattack, the unwelcome discovery that their processes were not as strong as they thought they were led to breaches. Compounding this issue was out-of-date security technology, which was the cause of breaches for 14 percent. The strain exerted by the sudden shift to remote working clearly exposed those areas where policy and technology failed to keep pace with the changing environment.

The responsibility was not all laid at the organization's door, with 13 percent of breaches originating in the supply chain. Further down the list but still significant, 11 percent of breaches were attributed to ransomware, 11 percent to third-party applications, and 11 percent to web applications. Once again, this diversity of breach causes highlights the many fronts on which U.S. CISOs have to defend their organization.

Process weakness was a particular problem in financial services companies, causing one-fifth (22 percent) of breaches. For manufacturers, out-of-date security technology was the culprit in 21 percent of incidents.

The higher prevalence of ransomware attacks on healthcare organizations translated to 14 percent of breaches in that sector. It was also a problem for financial services companies, causing 18 percent of breaches.

Larger organizations were more susceptible to breaches caused by process weakness, with 38 percent of breaches at companies with 5,001–10,000 employees caused in this way.

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

42 percent of respondents who suffered a cyberattack said that between 21–30 percent were material breaches, and a further 34 percent said 31–40 percent of breaches were material.

In the government sector, 45 percent of respondents said that 31–40 percent of breaches were material, while only 26 percent said the same in the healthcare sector.

90 percent of organizations suffered a material breach.

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

One-third (33 percent) of respondents who suffered a cyberattack said they suffered negative financial impact due to a data breach suffered by their organization. This is higher than the global average of 24 percent and has risen significantly from the 19 percent who said they suffered financial impact in the June 2020 survey. This is likely related to the implementation of new data privacy legislation, such as the California Consumer Privacy Act (CCPA), that has reached the enforcement phase in the intervening period. Organizations are much more aware of the financial penalties associated with data loss.

The percentage claiming no financial impact from a breach also dropped, from 68 percent in June 2020 to 47 percent in this report.

Interestingly, among financial services companies, only 10 percent said there had been a negative financial impact, but an incredible 29 percent said they didn't know what financial damage breaches had caused. Healthcare organizations were most likely to say they hadn't experienced financial impact, with 62 percent saying they had been unaffected.

Overall, the effect on brand reputation was greater. 71 percent of respondents who suffered a cyberattack said their brand had been negatively affected by a data breach, up from 62 percent in the June 2020 report. 7 percent said the damage was severe.

Only 21 percent said there was no reputational loss suffered when a breach occurred.

Financial services companies were most likely to report reputational damage, with 86 percent saying they had been affected. Also suffering brand damage were media and entertainment companies (82 percent) and travel and transport businesses (100 percent).

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. Almost two-thirds (62 percent) are very or somewhat fearful that a breach will hit their business.

The financial services sector is most concerned, with 78 percent of respondents saying they fear a breach. Less than half (48 percent) of government respondents and 58 percent of healthcare organizations are worried about a breach.

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

> 40 percent plan to build more security into their infrastructure and apps, and reduce the number of point solutions.

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

40 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 46 percent in the financial services sector.

38 percent said they have **updated their security technology to mitigate the risk**. Again, it is the financial services sector that is most likely to be taking this approach (54 percent), although healthcare organizations are also slightly more likely than others to be considering technology updates (44 percent). Similarly, 38 percent say they have **adapted security to mitigate risk** using existing assets.

36 percent said they **have updated their security policy to mitigate risk**, an important tactic given the significant changes to the security landscape in the past year. 52 percent of financial services companies, 50 percent of food and beverage companies, and 46 percent of media and entertainment companies have taken this approach.

35 percent have **increased security budget**. The retail (45 percent), professional services (42 percent), and healthcare (38 percent) sectors are more likely to be increasing their budgets.

It is interesting that organizations are putting strategy ahead of simply throwing money at the problem, with increasing budget a lower overall priority than the 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. 65 percent agree they **need better visibility over their data and apps to pre-empt attacks**. This rises to 72 percent in the financial services sector.

> 65 percent need better visibility over data and apps.

63 percent of U.S. 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**. Those in the retail (85 percent) and travel and transport (83 percent) sectors are more likely to take this view.

Two-thirds (66 percent) say 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. IT leaders are recognizing that dynamic environments require a context-centric approach.

66 percent agree they need better contextual security in place to track data/security through the lifecycle.

U.S. CISOs surveyed are under no illusions about the mission-critical nature of app security to their business. 67 percent agreed that their ability to innovate as a business depends on their **ability to build, manage and distribute apps more securely**.

60 percent of respondents **feel confident in bringing new apps to market because they know they will be secure**. Confidence is lowest among government respondents.

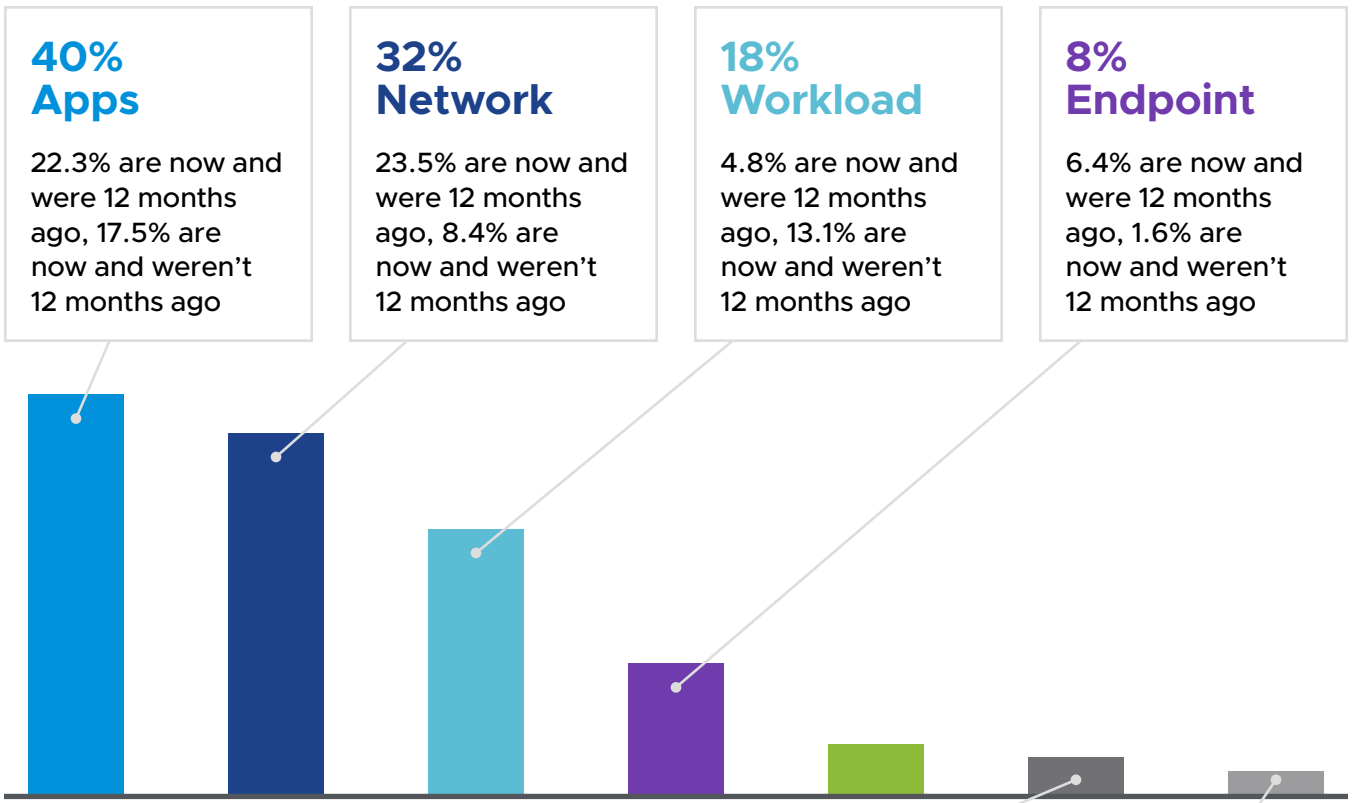
Asked about their view of AI in secure app development, respondents showed signs of conflict. 60 percent agree **security concerns are holding them back from embracing AI/ML-based apps to improve services**, but 63 percent agree they **would like to use more AI and ML in their apps to improve security and services**.

More than half of respondents (57 percent) agreed **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 to market because of the growing threat and damage data breaches have**. Boards are most likely to be concerned in utilities companies, with all CISOs in this sector saying the board is worried. This is followed again by the consumer-facing sectors of retail and travel and transport.

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 organizations placing more focus on tackling this risk in the coming year.



40% Apps

22.3% are now and were 12 months ago, 17.5% are now and weren't 12 months ago

32% Network

23.5% are now and were 12 months ago, 8.4% are now and weren't 12 months ago

18% Workload

4.8% are now and were 12 months ago, 13.1% are now and weren't 12 months ago

8% Endpoint

6.4% are now and were 12 months ago, 1.6% are now and weren't 12 months ago

1% Edge

0.4% are now and were 12 months ago, 0.8% are now and weren't 12 months ago

1% Cloud

1.2% are now and were 12 months ago

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

We 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.

49 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. Healthcare respondents fared well, with 58 percent agreeing they experienced no security barriers to setting up home working. On the other hand, financial services CISOs experienced difficulties, with 36 percent disagreeing that they had been able to get their workforce up and running without problems.

Respondents acknowledge there is always room for improvement, with 54 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?

Respondents universally stated they are planning to shift to a cloud-first security strategy—if not immediately, it is firmly on the roadmap. 100 percent already use or plan to adopt a cloud-first approach to protect the organization.

35 percent 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 16 percent plan to become cloud-first in the coming year, while the switch is further down the track for 19 percent.

> 100 percent already use or plan to adopt a cloud-first approach to protect the organization.

Cloud-first maturity is high among financial services companies, where 40 percent have been cloud-first for more than 12 months and 42 percent for less than 12 months. 28 percent of government respondents have been operating a cloud-first security strategy for more than a year.

Key Insights and Actions

Our second U.S. 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 still 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 U.S. 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. **251 U.S. 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 second U.S. 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 Australia, Canada, Saudi Arabia, the United Arab Emirates, 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
 Item No: 863494aq-sec-insgt-rprt-en-us-uslet 5/21