vmware®

The Nordics

Nordics Security Insights Report

Extended enterprise under threat

2021

Introduction

This research was conducted to understand the challenges and issues facing Nordic 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 Nordic 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 NORDICS 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 Nordics 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.

Nearly two-thirds (65 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 had increased as a result of more employees working from home. 67 percent said attacks had become more sophisticated.

The result? The number of breaches is significant, and respondents who had a cyberattack reported **2.89 breaches on average per year**. Nor were these minor incidents. In seven 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: 44 percent of Nordic CISOs surveyed fear 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:

63%

said attacks increased as a result of home working

2.89

breaches on average have been reported per organisation, per year

71%

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 was the most common cause, at the root of 18 percent of breaches, followed closely by third-party apps and then by process weaknesses.

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

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.

18% **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. 54 percent 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.

51 percent 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 recognised as more than half (53 percent) of 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.

8 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 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. 100 percent of 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 second **VMware Nordics Security Insights Report** revealing and informative.

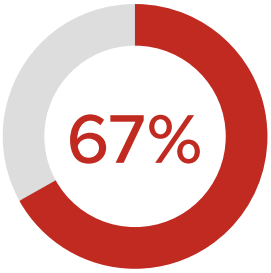
Key Findings

Attack frequency and breach risk remain high

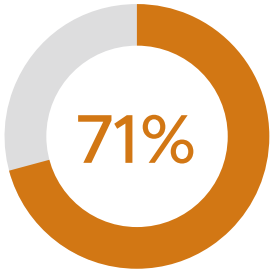
The frequency of attacks is high, their sophistication continues to grow, and breaches are the inevitable result.

65% said attack volumes had increased in the past 12 months. The average reported increase among them was 53 percent.

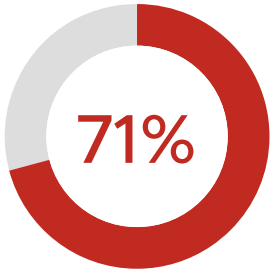
63% of those who had a cyberattack said attacks increased due to more people working from home.



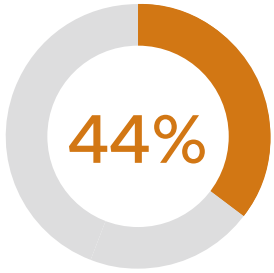
of those who had a cyberattack said attacks were more sophisticated.



have suffered a breach in the past 12 months, with those who have been breached experiencing an average of 2.89 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 weaknesses top CISO concerns

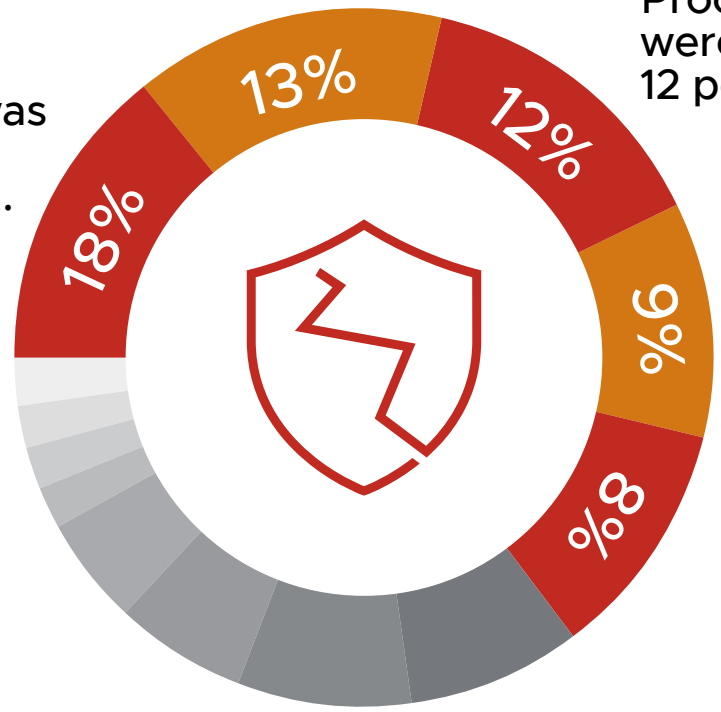
The top vectors that cause breaches build a picture of external threats and internal weaknesses.

Top breach causes for those who had a cyberattack:

Third-party apps were second with 13 percent.

Process weaknesses were third with 12 percent.

Ransomware was the top cause with 18 percent.



Out-of-date security tech (9 percent) and web application attacks (8 percent) complete the top five.

Apps 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.

53% agree they need to view security differently than they have previously as the attack surface has expanded.

53% agree they need better contextual security in place to track data through the lifecycle.

51% 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. 40 percent said they are increasing their security budget to achieve these aims.

↗ 45% have updated their security technology to mitigate the risk.

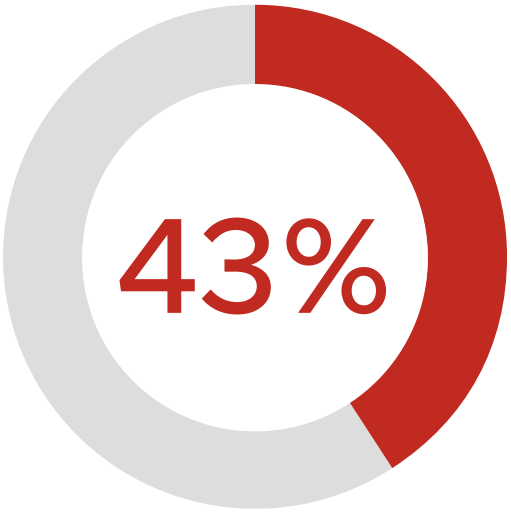
↗ 45% are building more security into their infrastructure and apps, and reducing the number of point solutions.

↗ 49% have updated their security policy and approach to mitigate risk.

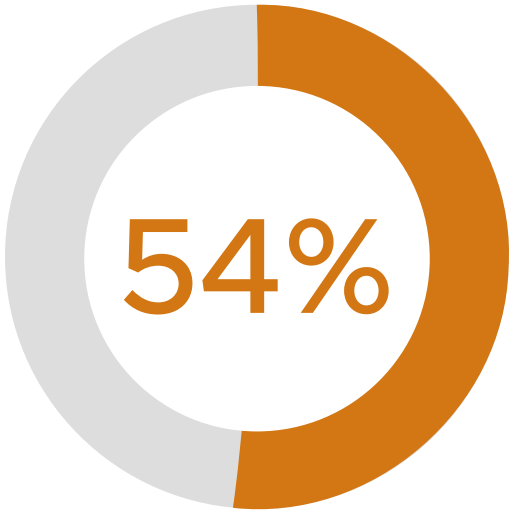
100% have shifted or plan to shift to a cloud-first security strategy.

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.

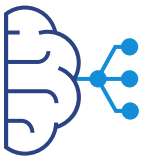


Yet, 43 percent of Nordic respondents agree security concerns are holding them back from embracing AI/ machine learning (ML)-based apps to improve such services.



54 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.

43% 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.

43.5% 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.

51% agree they would like to use more AI/ML in their apps to improve security and services.

51% agree they need better visibility over data and apps to pre-empt attacks.

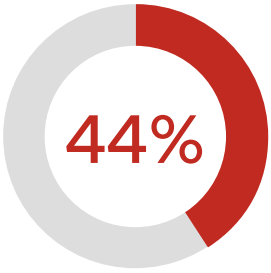
Securing brand and reputation—does it command more urgency for change?

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

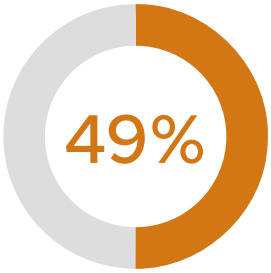
57% of those who suffered a cyberattack say there was some kind of negative impact on reputation—down from 73 percent in June 2020.

71% 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?

65 percent of the CISOs surveyed said they experienced an increase in the number of cyberattacks on their organisation in the past 12 months. The average increase experienced was 53 percent. Across the three countries surveyed, a staggering 97 percent of Swedish respondents said they experienced an attack, while 64.5 percent of Finnish respondents and only 35 percent of Norwegian respondents said they experienced an attack. In fact, 54 percent of respondents from Norway claimed they have not had a cyberattack.

The percentage experiencing attack increases rose to 92 percent in the financial services sector, and the average increase experienced was 64 percent. Interestingly, although government sector respondents had less of an increase in terms of the number of attacks (68 percent), the average increase was high at 77 percent.

Those companies in the 1,001–2,000 employee category experienced a higher average attack volume increase of 92 percent, with the overall proportion reporting increases in attacks at 87.5 percent.

31 percent of respondents with 31–40 people in their IT team reported between a 51–100 percent increase in the volume of cyberattacks.

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. Finland witnessed the highest impact with 72 percent stating the overall number of cyberattacks has increased. This was followed by Sweden at 64 percent and Norway was third with 54 percent.

85 percent of respondents from financial services organisations noted an increase in attacks connected to home working, with an average increase of 15 percent. Surprisingly, 47 percent of government sector respondents said attacks stayed the same, and 16 percent said attacks decreased.

25 percent of respondents with 31–40 people in their IT team said attacks increased by between 25–49 percent.

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

When it comes to attack sophistication, 67 percent of CISOs surveyed who had a cyberattack have seen attacks grow more sophisticated. This is almost on par with the June 2020 report when 68 percent reported increased attack sophistication. This rose to 81 percent for Finnish respondents. However, respondents from Sweden had the highest percentage (11 percent), saying that attacks had become significantly more sophisticated.

However, 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.

Evidence suggests they may be directing these techniques at the financial services sector, where 89 percent reported increased sophistication. Almost two-thirds (62 percent) said attacks had become moderately or significantly more complex.

> 67 percent of surveyed CISOs have seen attacks grow more sophisticated.

Adversaries are directing their more sophisticated attacks at larger organisations, with a higher percentage claiming that attacks have become significantly more sophisticated. 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 monetise 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 Nordic attack environment is diverse, with few respondents experiencing the same mix of attack types and no single attack type dominating. This underlines the challenges Nordic CISOs face; they need to build strategic and tactical responses to an incredibly varied mix of attack vectors and techniques.

Ransomware tops the list, with 15 percent of respondents who had a cyberattack seeing this most frequently. Google Drive (cloud-based attacks) was also a top attack type for 12 percent of respondents.

Ransomware was the most prolific attack type in Norway (21 percent) and Finland (22 percent), but was less prevalent in Sweden (10 percent). Supply chain attacks were very frequent in Finland (16 percent). Sweden had twice as many attacks via process hollowing (8 percent) than Norway (4 percent).

Supply chain attacks and process hollowing each account for 9 percent and 7 percent, respectively, for those who have been cyberattacked. In the June 2020 report, Google Drive topped the list with 26 percent of respondents experiencing this attack most frequently.

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

Seven out of 10 of the CISOs who took part in our research said their organisation suffered a breach as a result of a cyberattack in the past year (71 percent). This is down from 99.6 percent who reported falling victim to a breach in June 2020. Again, there was considerable variation between countries. 98 percent of Swedish survey participants said their organisation suffered a breach, while in Norway, the figure was just 46 percent, reflecting the high number of respondents who say they haven't suffered any attacks. Among Finnish respondents, 71 percent suffered a breach as a result of a cyberattack.

> 71 percent of surveyed organisations suffered a security breach in the past year.

However, the average number of breaches suffered by each organisation increased, from 1.79 in June 2020 to 2.89 in this report. 22 percent of respondents said their organisations had been breached between 5–10 times. Sweden experienced the highest average number of breaches at 3.46, and Norway had the lowest at 2.04. In Finland, the figure was 2.41.

The government sector suffered the highest average number of breaches at 4.50. Other notable sectors reporting higher-than-average breach frequency are utilities (4.25) and professional services (4.08).

Breach frequency is highest in organisations with 501–1,000 employees, with each experiencing 3.75 on average.

What was the prime cause of these breaches?

For 18 percent of CISOs surveyed who suffered breaches as a result of a cyberattack, ransomware was the main culprit. For 13 percent, a breach came via third-party apps, while the unwelcome discovery that their processes were not as strong as they thought they were led to breaches for a further 12 percent. Compounding this issue were out-of-date security technology (9 percent) and web application attacks (8 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.

Further down the list but still significant, 7 percent of breaches were attributed to phishing attacks. Interestingly, 8 percent didn't know what the prime cause of the breaches were, and 5.5 percent said there was no prime cause. Once again, this diversity of breach causes highlights the many fronts on which Nordic CISOs have to defend their organisation.

Ransomware attacks caused the most breaches in Norway (27 percent), whereas in Sweden, respondents experienced more problems with third-party apps and process weakness, causing 18 percent of breaches in each case. Finland had a high percentage of respondents claiming not to know what the prime cause was (28 percent) and also had a high percentage of breaches due to phishing attacks (16 percent).

Surprisingly, process weaknesses were a particular problem in financial services organisations, causing 21 percent of breaches. This was closely followed by ransomware at 17 percent. Interestingly, 18 percent of respondents from the government sector didn't know what the prime cause of a breach was.

Organisations with 501–1,000 employees were particularly susceptible to breaches caused by ransomware, with 25 percent of breaches caused in this way. And those with IT team sizes between 31–40 people experienced a high percentage of breaches due to third-party app attacks (19 percent).

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. Nearly three-quarters of respondents (71 percent) had to report to regulators or engage an IR firm to overcome the problems caused by breaches.

Nearly half (43 percent) of respondents who suffered a cyberattack said that between 21–30 percent were material breaches, and a further 26.5 percent said 31–40 percent of breaches were material.

Swedish respondents had the highest mean average of material breaches at 27 percent, while respondents from Finland had the lowest out of the three countries at 17 percent. 39 percent of respondents from Sweden said that 31–40 percent of breaches were material.

Government sector respondents had the highest mean average at 26.52 percent, with 45 percent saying that 31–40 percent of breaches were material. Financial services respondents also reported high figures, with 60 percent admitting that 21–30 percent of breaches had to be disclosed to regulators.

71 percent of organisations suffered a material breach.

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

Less than two out of 10 respondents (18 percent) who suffered a cyberattack said they suffered negative financial impact due to a data breach suffered by their organisation. This is lower than the global average of 24 percent.

The percentage claiming no financial impact from a breach slightly increased, from 46 percent in June 2020 to 48 percent in this report.

Out of the three countries, Norway scored highest on reporting no financial impact from a breach, with 56 percent compared to 53 percent in Finland and 43 percent in Sweden. More than half (52.5 percent) of Swedish respondents admitted they didn't know what the financial impact was of a breach. Likewise, Sweden scored lowest (17 percent) on no reputational impact compared to 31 percent for Norway and 25 percent for Finland.

Overall, the effect on brand reputation was greater. 57 percent of respondents who suffered a cyberattack said their brand had been negatively affected by a data breach, down from 73 percent in the June 2020 report. 4 percent said the damage was severe.

Only 22 percent said there was no reputational loss suffered when a breach occurred.

57 percent of financial services respondents said there was no negative financial impact compared to 15 percent who said there was no negative reputational impact.

How fearful are you of the material breaches that you believe your organisation 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. 44 percent are very or somewhat fearful that a breach will hit their business.

Even though Finland had the lowest percentage of material breaches, respondents from this country scored highest with regard to how fearful they are of being hit by a material breach. 73 percent were very fearful or somewhat fearful (20 percent said they were very fearful), compared to 47 percent in Sweden and 29.5 percent in Norway.

The financial services sector is more concerned, with 71 percent of respondents saying they fear a breach.

14 percent of organisations with 251–500 employees were very fearful.

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

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

45 percent of respondents said they plan to **build more security into their infrastructure and apps, and reduce the number of point solutions**.

38 percent say they have **adapted security to mitigate risk** using existing assets. In particular, healthcare organisations are more likely than others to be considering adapting technology (48 percent). 45 percent of respondents said they have **updated their security technology to mitigate the risk**. This rose to 56 percent for Norwegian respondents.

49 percent said they **have updated their security policy and approach to mitigate risk**, an important tactic given the significant changes to the security landscape in the past year. 60 percent of respondents from Finland have taken this approach as have 58 percent of healthcare organisations.

40 percent have **increased security budget**. Out of the three countries, Norway had the highest proportion that increased budgets, at 45 percent, followed by Finland (42 percent) and Sweden (34 percent).

It is interesting that organisations are putting strategy ahead of simply throwing money at the problem, with increasing budget fourth on the priority list behind updating policy 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.

In general, Finland scored higher on either agreeing or somewhat agreeing with all of the statements compared to Sweden and Norway.

Visibility is a definite concern. 51 percent agree they **need better visibility over their data and apps to pre-empt attacks**.

53 percent of Nordic 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**.

53 percent say 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. IT leaders are recognising that dynamic environments require a context-centric approach.

51 percent need better visibility over data and apps.

Nordic CISOs surveyed are under no illusions about the mission-critical nature of app security to their business. 54 percent agreed that their **ability to innovate as a business depends on their ability to build, manage and distribute apps more securely.**

55 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. 43 percent agree **security concerns are holding them back from embracing AI/ML-based apps to improve services**, but 51 percent agree they **would like to use more AI and ML in their apps to improve security and services**.

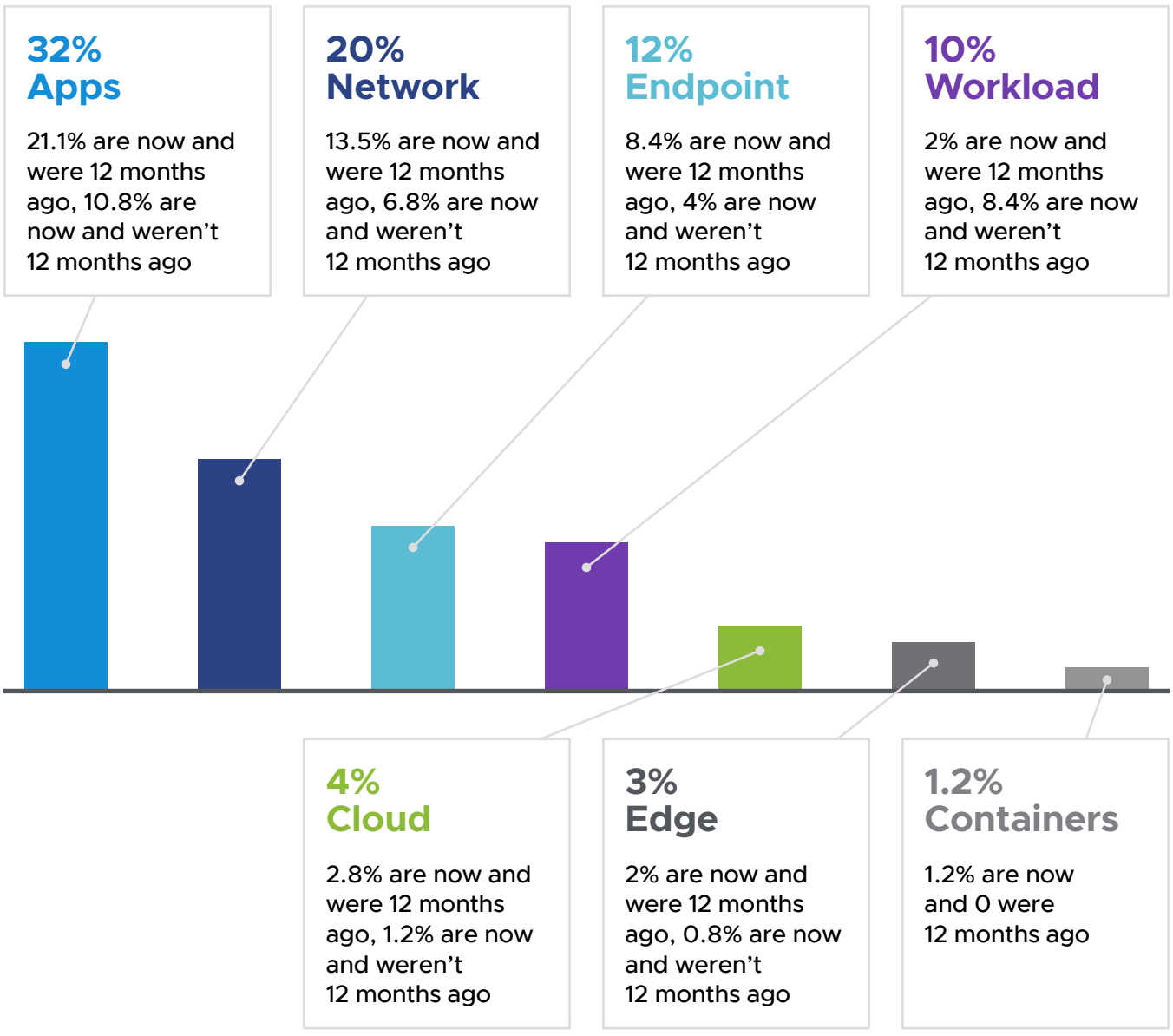
More than half of respondents (43 percent) agreed that **there is too much complexity in the security solutions market to make them change their security policy even though they know today's IT security is not working**, indicating that vendors have work to do to simplify their proposition into a unified approach.

Finally, 43.5 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**.

43.5 percent say their board is increasingly worried about the security risks of bringing new apps to market.

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.



Country breakdown

	SWEDEN	NORWAY	FINLAND
Workload is now the most vulnerable breach point and was 12 months ago	2%	2%	2%
Workload is now the most vulnerable breach point but wasn't 12 months ago	9%	9%	7%
Apps are now the most vulnerable breach point and were 12 months ago	22%	24%	13%
Apps are now the most vulnerable breach point but weren't 12 months ago	15%	7%	11%

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.

37 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. This figure rose to more than half where Finnish respondents were concerned (56 percent) compared to 34 percent and 32 percent for Norway and Sweden, respectively.

Respondents acknowledge there is always room for improvement, with 41 percent agreeing a security-first approach would have increased their ability to enable employees to work from alternative locations and remain productive. Again, this was highest for respondents from Finland, with 67 percent agreeing with this statement.

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?

All respondents (100 percent) stated they are planning to shift to a cloud-first security strategy—if not immediately, it is firmly on the roadmap.

42 percent overall say they have been using a cloud-first approach for more than one year, while 27 percent say they have been cloud-first for less than 12 months. A further 31 percent either plan to become cloud-first in the coming year or they will make the switch further down the track.

Norway was the most mature out of the three countries surveyed when it came to their cloud-first strategy, with 64 percent having a cloud-first strategy for more than 12 months, compared to 26 percent in both Sweden and Finland.

Cloud-first maturity is high among healthcare organisations, where 60 percent have been cloud-first for more than 12 months. 41 percent of financial services organisations have been cloud-first for less than 12 months.

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

Key Insights and Actions

Our second Nordics 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 Nordics 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 Nordic 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 Nordics 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, the Netherlands, Germany, Spain, France, 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 modernisation, 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