Action1

State of Vulnerability Remediation Report

2023

Contents

Part I. Introduction

About This Report

This report helps organizations tackle modern cybersecurity challenges and reduce data breaches and ransomware risks by offering insights on improving vulnerability management and remediation.

According to Statista, 22,514 common IT security vulnerabilities and exposures (CVEs) were discovered in 2022, the highest reported annual figure so far. 2022 saw some high-profile zero-days, including Microsoft vulnerabilities accounted for about 23%, followed by Google Chrome (17%) and Apple products (17% combined iOS and macOS zero-days), according to SecurityWeek.

The average cost of a data breach is $4.35 million, making prompt detection and remediation of security vulnerabilities crucial for organizations. Also, escalating geopolitical tensions exacerbate the cyber threat landscape, leading to more damaging and widespread attacks and making effective vulnerability management an essential element of an organization's security strategy.

This report analyzes the current state of vulnerability management in organizations, identifies barriers to successful remediation, sheds light on security incidents and root causes, and provides recommendations to improve cybersecurity posture. Based on a survey of 804 IT and IT security professionals from North America, Europe, and the Asia-Pacific (APAC) region.

Geopolitical instability is exacerbating the risk of catastrophic cyberattacks, according to the Global Cybersecurity Outlook 2023 Report launched at the World Economic Forum 2023.

Executive Summary

- Low cybersecurity awareness and insufficient privileged access control were the top two security vulnerabilities that have become harder to remediate than last year. These findings are not surprising. First, cyberattacks, especially social engineering, which relies on the human factor, have increased in scale and sophisticatedness over the last year. Second, privileged access control became more complicated due to the modern work-from-anywhere reality – in fact, 63% of organizations incorporate at least some remote work. Altogether, these factors certainly make cybersecurity more challenging. For example, a successful phishing cyber-attack on a single machine with local admin privileges enabled can have devastating consequences for any organization. After compromising such a machine, hackers can access an organization's critical systems to encrypt, steal or modify data, move laterally through the network, disrupt services, create backdoors for future exploits, and more.

- The economic crisis negatively impacts organizations' cybersecurity since security does not receive enough budget. IT departments put so much effort into keeping business running that there is no time left for ensuring cybersecurity (reported by 34% of organizations). Most worryingly, despite high-profile breaches and public authorities emphasizing the need to improve security amidst increased geopolitical tensions, IT security initiatives do not get any support from executive leadership teams. IT pros rated this as the top factor negatively affecting organizational security posture from the internal point of view. Respectively, the second most negative factor affecting an organization's ability to keep its assets secure was IT budget cuts.

IT departments are overwhelmed with operational issues, with no time left for security

- Every tenth company experienced a data breach, with unpatched vulnerabilities being the most common root cause. Phishing was the most common attack vector indicated by a half (49%) of respondents, which emphasizes the need for building strong cybersecurity awareness on all organizational levels. Data encryption by the ransomware was the most common consequence of breaches cited by 54% of respondents. For organizations lacking effective privilege access management, the damage from such incidents can be especially catastrophic.

20% of enterprise endpoints have legacy security vulnerabilities

- Survey findings reveal critical gaps in all stages of the vulnerability management process. 30% of organizations take over a month to detect known security flaws, 38% do not prioritize vulnerabilities, and 40% need more than a month to remediate newly discovered critical Common Vulnerabilities and Exposures (CVEs). Most concerning, on average, 20% of endpoints remain unpatched after the remediation is complete, meaning that one-fifth of enterprise machines still have many legacy vulnerabilities that threat actors can exploit at any time. Finally, 48% of organizations do not evaluate the effectiveness of their vulnerability remediation efforts.

Part II. Detailed Findings

Organizational Work Model

Unsurprisingly, 63% of organizations continue to incorporate at least some remote or hybrid workforce.

63% of the organizational' workforce is at least somewhat remote or hybrid

On average, 44% of endpoints are permanently located outside the IT department's reach. (Most of these endpoints run on Windows operating systems.) It's important to note that this number includes devices used by fully remote workers and machines located in buildings or geographic areas separate from the IT department.

There are several reasons why organizations might choose to implement remote or hybrid work, even as the COVID-19 pandemic subsides and more businesses return to in-person operations. Remote or hybrid work can provide employees with greater flexibility and work-life balance, resulting in increased job satisfaction and productivity. For employers, it can reduce overhead costs associated with maintaining physical office space and make it easier to attract and retain talented employees, as many people are looking for more flexible work arrangements.

However, remote and hybrid work also make vulnerability management and cybersecurity more difficult for IT and IT security teams.

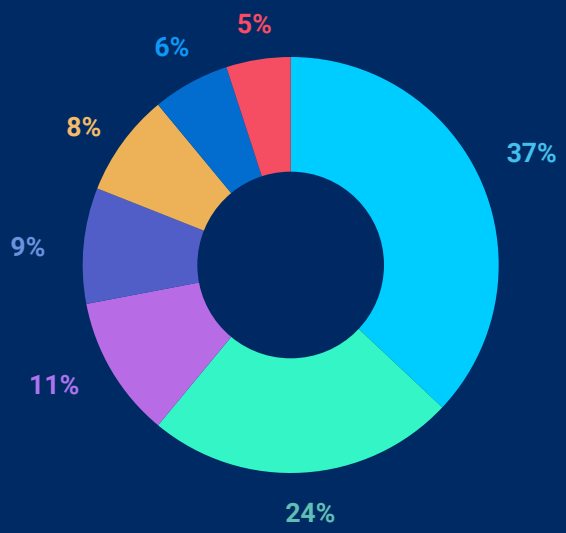


CHART 1.

WHICH PHRASE BEST DESCRIBES YOUR ORGANIZATION'S WORK MODEL?

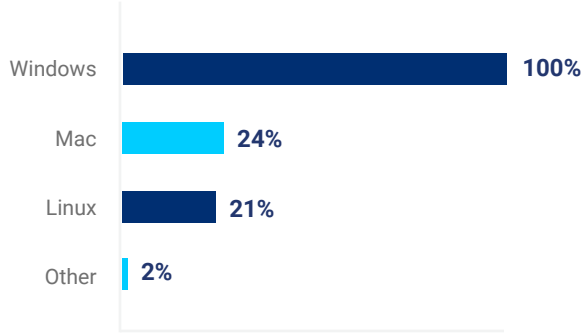
- We are mostly in-office.
- We are mostly hybrid (work-from-anywhere model).
- We are pretty evenly split between in-office, remote, and hybrid (work-from-anywhere model).
- We are mostly remote.
- We are half remote and half hybrid (work-from-anywhere model).
- We are half hybrid (work-from-anywhere model) and half in-office.
- We are half in-office and half remote.

CHART 2.

WHAT PERCENTAGE OF YOUR MANAGED ENDPOINTS ARE OFF-SITE?

CHART 3.

WHAT TYPE OF SYSTEMS DO YOU USE FOR MOST OF YOUR ENDPOINTS? (CHOOSE ALL THAT APPLY.)



Exploring Challenges to Ensure Cybersecurity

Keeping organizational IT assets up to date with the latest security patches is one of the critical elements of sustaining cyber resilience.

The survey showed that the top factor that harmed organizations' ability to keep their IT assets up to date and secure was the lack of support from the executive team for implementing security policies. That's surprising, given the attention paid to cyber security over the past year by media and authorities. Lack of support from the executive team can be a significant barrier to the successful execution of a software update policy. Executives must understand the significance of such a policy and allocate the essential resources and support to ensure its effective implementation. Otherwise, the IT department may face challenges in gaining buy-in from other stakeholders and executing the policy to its fullest potential.

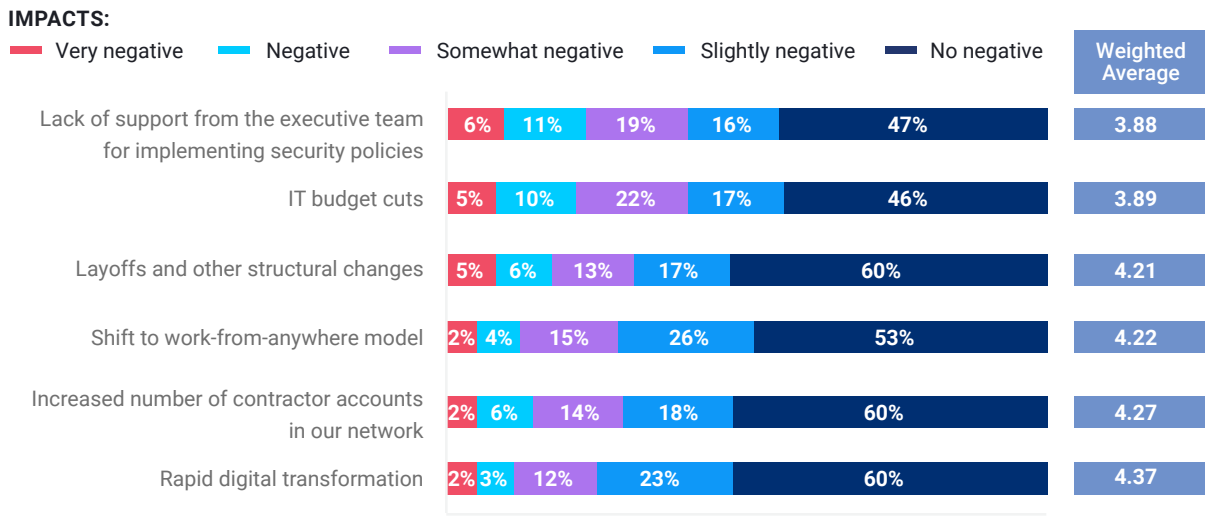
Lack of support from the executive team for implementing security policies is the top factor preventing organizations from keeping their IT assets up to date and secure

The second most crucial factor negatively impacting cyber resilience was IT budget cuts, and the third one, somehow related to it, links to layoffs and other structural changes.

Budget cuts limit the resources necessary to establish an effective automated patch management program. Layoffs also negatively impact the execution of a software update policy, as they reduce the number of staff available to perform the necessary tasks. A staffing shortage can result in a backlog of updates and patches that need to be applied, increasing the risk of breaches.

CHART 4.

HAS YOUR ORGANIZATION EXPERIENCED ANY OF THE FOLLOWING FACTORS DURING THE PRECEDING 12 MONTHS, AND TO WHAT EXTENT DID EACH ONE NEGATIVELY IMPACT ITS ABILITY TO KEEP IT ASSETS UP TO DATE AND SECURE?



As a result of the lack of executive support, budget cuts, and structural changes, IT teams became overloaded with operational issues with no time left to focus on cybersecurity.

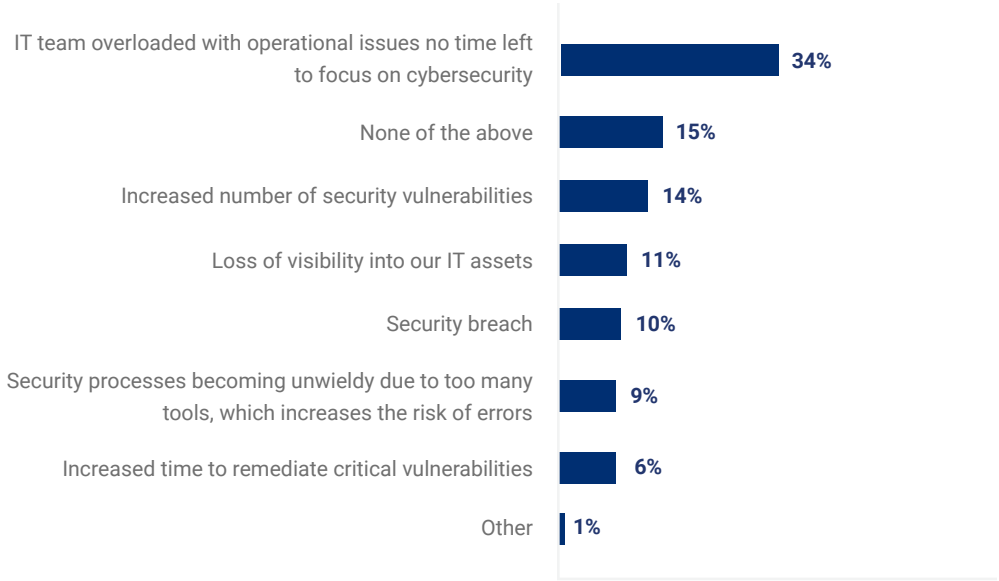
When an IT team is overwhelmed with operational issues, it may not have the capacity to manage and maintain security controls properly, leading to vulnerabilities in the organization's IT systems and infrastructure going unnoticed.

Every tenth organization experienced a data breach over the last year

Therefore, it's no surprise that every tenth organization experienced a data breach.

CHART 5.

WHAT WAS THE MOST NEGATIVE CONSEQUENCE OF THOSE FACTORS ON YOUR ORGANIZATION'S SECURITY?



Analysis of Security Incidents

Although many studies have warned organizations about the danger of unpatched vulnerabilities over recent years, the problem still exists. Our survey showed that unpatched vulnerabilities were the top root cause of the security incidents indicated by 47% of respondents.

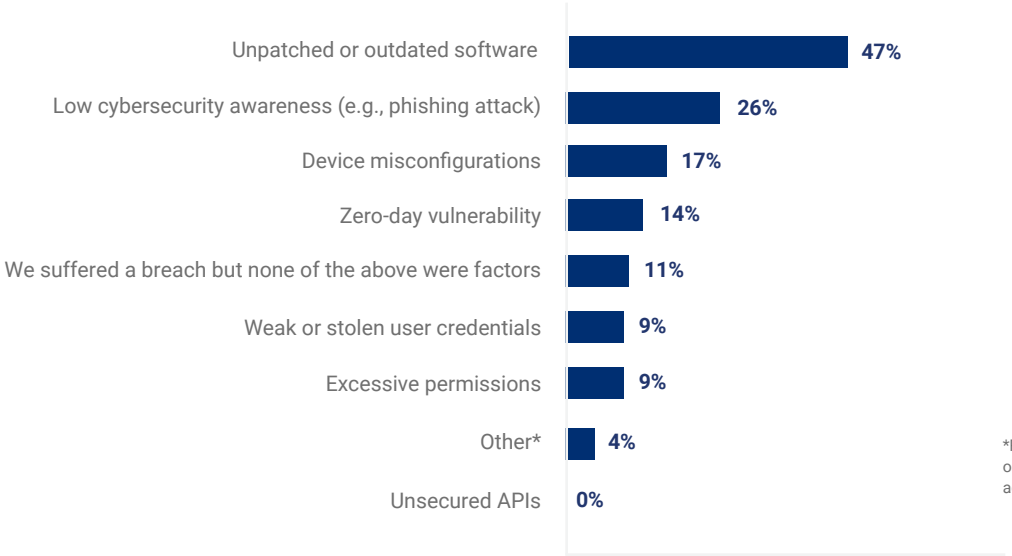
Known security vulnerabilities are easy for cybercriminals to exploit because they can find publicly available proofs of concepts for such vulnerabilities in the darknet. That is why legacy vulnerabilities represent a significant threat to organizations. Threat actors leverage automated tools to scan for known vulnerabilities across systems in many companies simultaneously. Once they identify a vulnerable system, they can use readily available exploit code to break in.

The survey also showed that the top attack vector indicated by 49% of respondents was phishing. Although there may be many reasons why phishing is so popular with cybercriminals, one primary reason is the lack of cybersecurity awareness. Plus, with the vast amount of data leaked over the past, cybercriminals can craft messages highly tailored to the recipient, making them more convincing and harder to detect and increasing hackers' chances to trick users into providing sensitive information or downloading malware. Phishing is a relatively low-cost and low-risk way for attackers to gain initial access to a network and then use that access to move laterally and escalate the attack by finding and exploiting other vulnerabilities in the network.

47% of breaches resulted from unpatched security vulnerabilities

CHART 6.

DID YOUR ORGANIZATION SUFFER A BREACH IN THE PAST 12 MONTHS THAT INVOLVED EXPLOITATION OF ANY OF THE FOLLOWING SECURITY VULNERABILITIES? (CHOOSE ALL THAT APPLY.)



*Respondents who picked the "Other" option indicated human errors and account takeover as breach root causes.

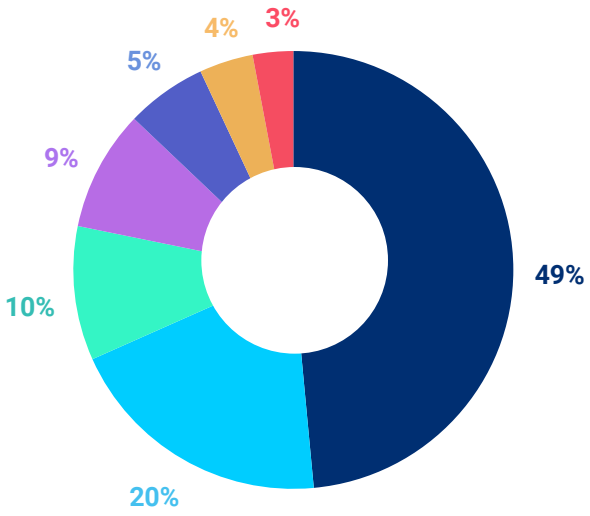


CHART 7.

WHAT WAS THE INITIAL ATTACK VECTOR?

- Phishing
- Non-applicable
- Exploit kit
- Misconfiguration exposure
- Other*
- Credential compromise
- Insider threat

*Respondents who picked the "Other" option indicated rootkits and account takeover and AD forest compromise as breach attack vectors.

Unsurprisingly, data encryption by the ransomware was the most common consequence of the breach.

*According to **Statista**, an average downtime after ransomware attack is around 20 days*

Many high-profile breaches show that a ransomware attack can become a disaster paralyzing an organization's business. Downtime can result in lost productivity, revenue, and reputation damage.

Suppose ransomware victim does not have a backup of their data. In that case, they may permanently lose access to their critical information since they are not guaranteed to receive their files even after the payment. And finally, data compromise by ransomware can lead to legal issues and costly compliance fines.

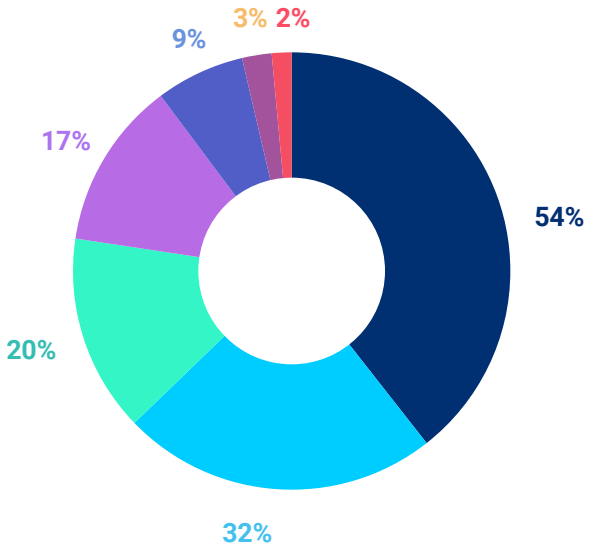


CHART 8.

WHAT WERE THE CONSEQUENCES OF THE BREACH? (CHOOSE ALL THAT APPLY.)

- Data encryption by ransomware
- Non-applicable
- Service disruption
- Data exfiltration
- Data corruption
- Data destruction
- Other

Ability to Remediate Different Types of Vulnerabilities

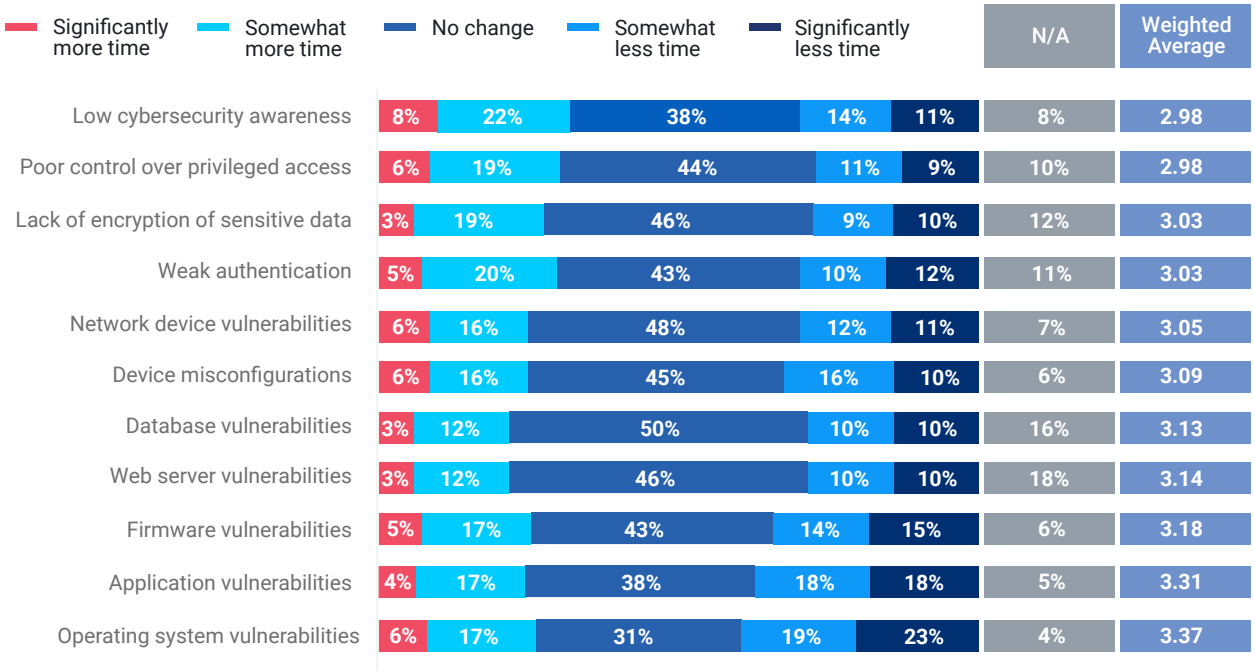
Our survey results showed that managing cybersecurity awareness has become the most time-consuming vulnerability to address. One reason for this could be the widespread adoption of remote and hybrid work, which makes it challenging for IT security teams to ensure that all employees receive consistent training and monitor their actions. Additionally, many organizations may lack resources to allocate to dedicated cybersecurity awareness training, leaving IT teams to create it from scratch. Furthermore, cybercriminals are becoming increasingly sophisticated in their tactics and making their messages more appealing to the recipient, which requires IT teams to invest more effort in educating employees on the techniques used by threat actors and what they should be aware of.

Time to combat low cybersecurity awareness has increased

Lack of least privilege implementation became the second most time-consuming security vulnerability. One reason may be that when endpoints are off-site, IT teams may find it difficult to deploy or manage updates and software without dedicated endpoint management tools since these tasks require local admin privileges. In addition, some users may be granted unneeded privileges simply as a turnaround to save time on solving a particular issue, which further increases the potential attack surface.

CHART 9.

COMPARED TO A YEAR AGO, DOES IT TAKE YOU MORE OR LESS TIME TO ADDRESS THE FOLLOWING VULNERABILITIES?



Tools Organizations Use to Remediate Vulnerabilities

The survey showed that the top three tools that organizations use to remediate vulnerabilities are:

- Endpoint protection system (EPS) - reported by 62% of respondents.
- Manual approach - indicated by 56% of organizations.
- Remote monitoring and management (RMM)/ patch management solution - 36%.

It's worrying that the manual approach to security vulnerability remediation is so widespread. Manually identifying and addressing vulnerabilities can be time-consuming and resource-intensive; plus, it can lead to delays in addressing vulnerabilities and leave systems exposed to attacks for a long time. Moreover, with the increasing number of vulnerabilities, the manual approach becomes increasingly difficult to scale.

56% of organizations remediate security vulnerabilities manually

Similarly, although it's good news that most organizations use EPS, only one-third combine it with a patch management tool. However, while EPS and patch management solutions both play an important role in securing an organization's IT environment, they are not interchangeable.

An EPS is designed to detect and prevent malware and malicious activity on individual devices and servers. EPS can help protect against known and unknown threats using signature-based detection, behavioral analysis, and reputation-based detection.

On the other hand, patch management solutions focus on identifying and addressing known vulnerabilities in software and systems and keeping them up to date.

While an EPS can help to prevent malware from exploiting vulnerabilities, it might not address some underlying vulnerabilities that malware might exploit. A patch management solution, in turn, is a dedicated tool to remediate known vulnerabilities proactively. An EPS must also be updated; a robust patch management platform might help.

The need for organizations to automate patching through a robust patch management platform is especially true, given that there is no dedicated specialist for patching in 69% of organizations. Without a dedicated specialist and with a manual approach, there are no chances to keep your systems continuously patched.

CHART 10.

WHAT TOOLS DO YOU USE TO REMEDIATE IT SECURITY VULNERABILITIES? (CHOOSE ALL THAT APPLY.)

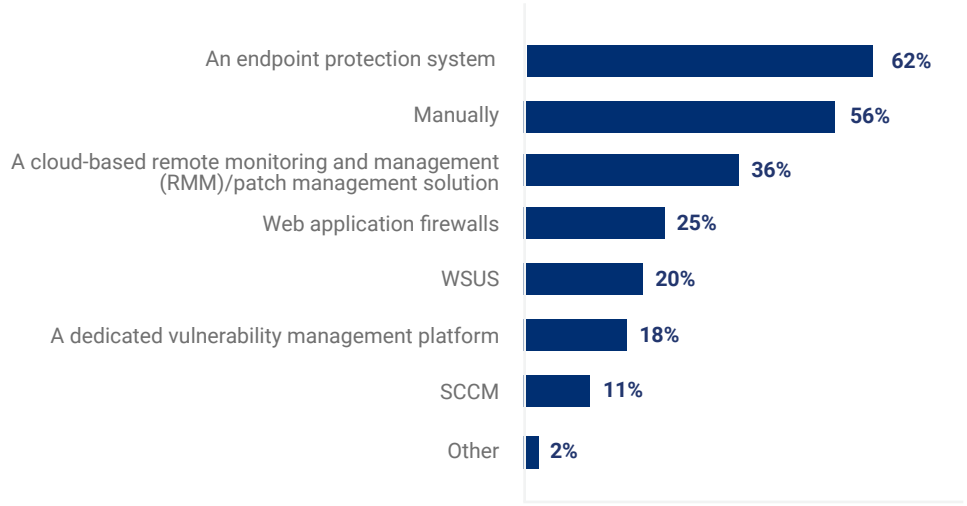
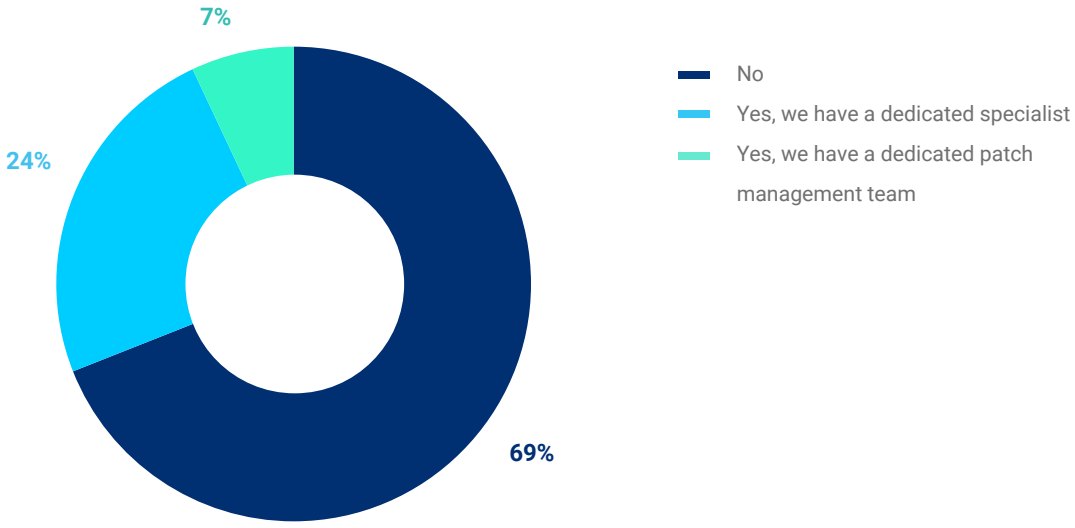


CHART 11.

DO YOU HAVE A DEDICATED SPECIALIST OR TEAM RESPONSIBLE FOR VULNERABILITY PATCHING?



Barriers to Effective Vulnerability Remediation

Half (47%) of respondents named the risk of downtime from deploying a problematic update when asked about the key barriers to effective vulnerability remediation. Although, understandably, updates must be applied cautiously, after thorough testing, such a risk should not prevent organizations from deploying security updates. After all, the potential damage and downtime from a ransomware attack would be much greater.

The fear of downtime prevents organizations from timely patching because they lack resources for proper testing, as 39% of respondents indicated.

The risk of downtime from deploying a problematic update is the key barrier to effective vulnerability remediation.

These findings highlight the need for automation in the crucial security process of deploying updates. Lack of automation makes patching more labor-intensive and error-prone, increasing the risk of delays. Indeed, half of the organizations (50%) had interruptions in the execution of the software update policy aimed at patching critical vulnerabilities.

CHART 12.

WHAT ARE YOUR TOP VULNERABILITY REMEDIATION CHALLENGES? (CHOOSE ALL THAT APPLY).

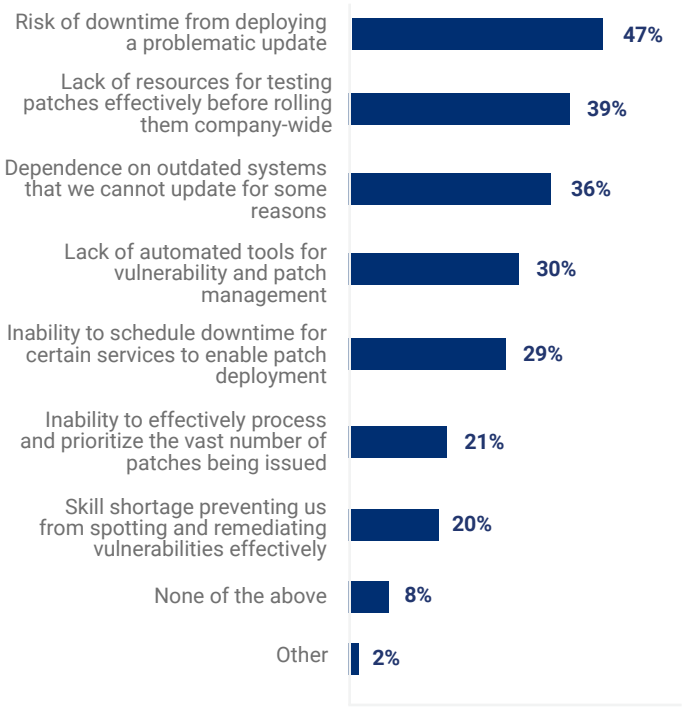
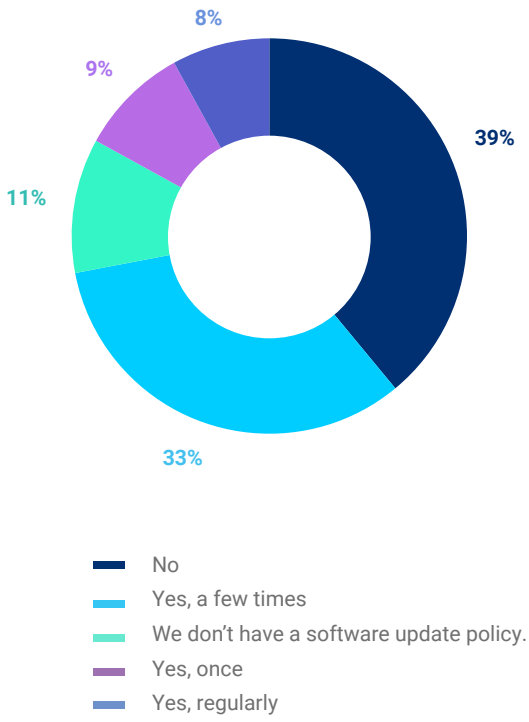


CHART 13.

DURING THE PRECEDING 12 MONTHS, WERE THERE ANY INTERRUPTIONS IN THE EXECUTION OF YOUR SOFTWARE UPDATE POLICY AIMED AT FIXING CRITICAL SECURITY VULNERABILITIES?



Vulnerability Identification and Prioritization

To ensure timely remediation of newly discovered security vulnerabilities, IT teams must continuously identify them. Otherwise, an IT team will not be able to adequately maintain the security of their IT environment by applying patches or other remediation measures.

It is essential to quickly identify critical security vulnerabilities for which a vendor has already released a patch, as attackers can target these flaws. Unfortunately, our survey showed that 30% of organizations take more than a month to detect where newly disclosed CVEs reside in their IT environment, of which 12% take over three months. More than a month is too long, as in most cases, an exploit for a vulnerability becomes publicly available on the darknet a month after a vendor discloses it and releases a patch, or even earlier.

One-third of organizations spend more than a month to detect where newly disclosed CVEs reside across their IT environment.

Over one-third of organizations (38%) do not prioritize vulnerabilities at all; at the same time, prioritizing vulnerabilities is essential because even the most well-equipped IT teams can only remediate around 10% of the millions of security vulnerabilities present in the average enterprise.

While relying on Common Vulnerability Scoring System (CVSS) scores to prioritize vulnerabilities is a common approach, it may nzot be enough. CVSS scores are not regularly updated, so the scores assigned may not reflect the current probability of exploitation. Additionally, CVSS does not analyze the current threat landscape. Only 12% of respondents use this approach.

A more effective approach is to evaluate and re-evaluate vulnerabilities based on the criticality of IT assets. 47% of respondents use this approach. They consider both CVSS scores and the criticality of affected systems to assess vulnerability and

CHART 14.

HOW MUCH TIME DOES IT TAKE YOU TO DETECT WHERE NEWLY DISCOVERED CRITICAL CVES RESIDE ACROSS YOUR IT ENVIRONMENT?

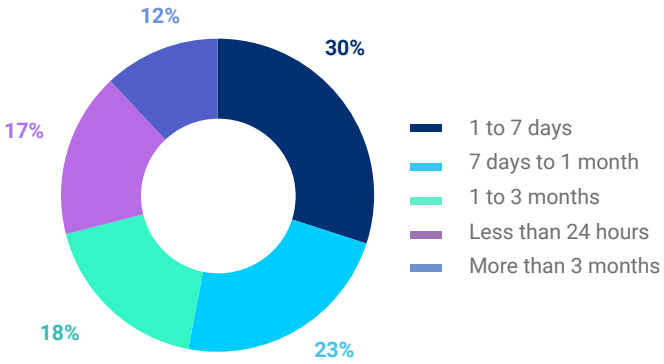
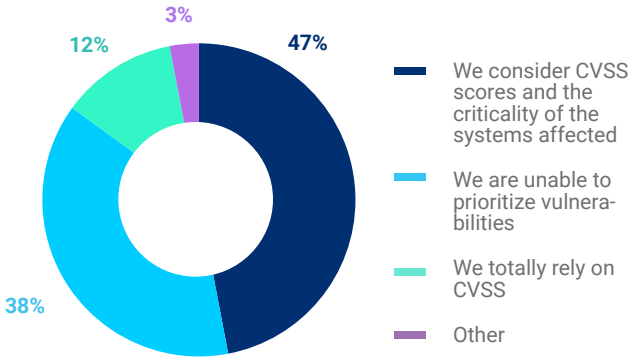


CHART 15.

HOW DO YOU PRIORITIZE DETECTED VULNERABILITIES?



Time to Remediate Vulnerabilities

Our survey showed that 40% of organizations need more than a month to remediate newly discovered critical CVEs. While this figure is indeed sad, it is not surprising; many studies have shown that delays in deploying critical security updates are common among organizations.

20% of enterprise endpoints were found to remain unpatched even after the remediation process

Even more worryingly, only 80% of security updates are applied successfully, meaning that one in five enterprise endpoints does not receive security patches. As a result, such endpoints might be open to severe vulnerabilities for years.

CHART 16.

HOW MUCH TIME DOES IT TAKE YOU TO REMEDIATE NEWLY DISCOVERED CRITICAL CVES?

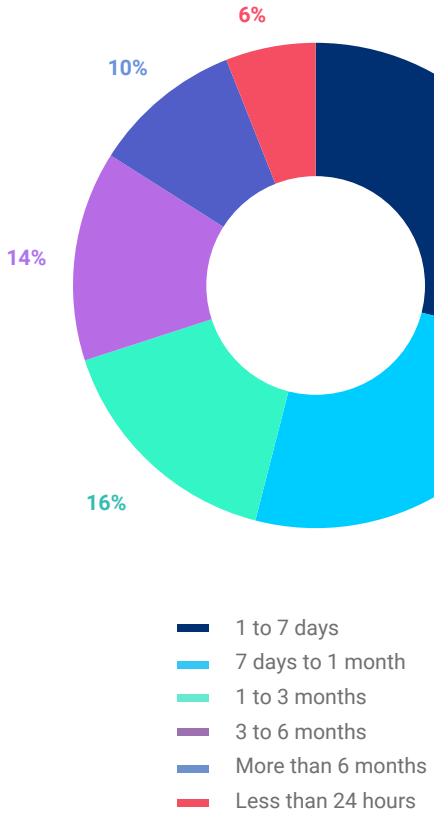
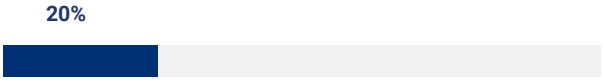


CHART 17.

WHAT PERCENTAGE OF DEVICES USUALLY REMAIN UNPATCHED AFTER THE REMEDIATION IS COMPLETE?



Reasons Why Patching Fails

Understanding the root cause of a problem is always essential because it allows you to take targeted and effective action to resolve the problem rather than just treating the symptoms.

In the case of patching failure, understanding the root cause can improve the overall effectiveness of the patch management process and reduce the risk of future failures.

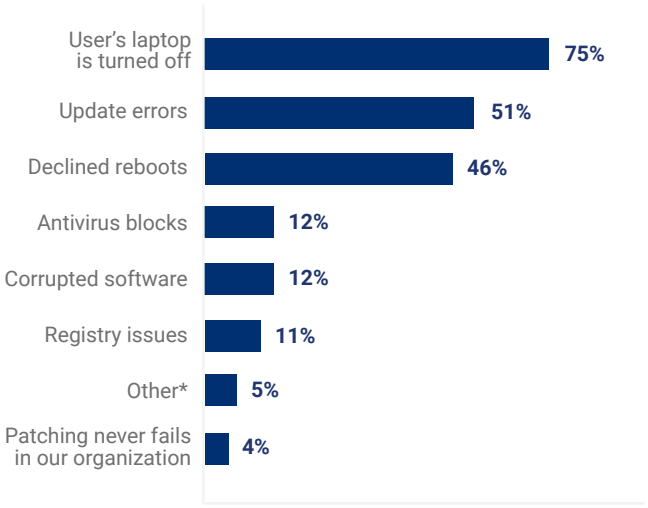
In 75% of cases, the user's laptop is turned off when doing a patch, leading to patch failures

The survey showed that the top three reasons for patching failure include the following:

- The user's laptop being turned off during a patch – in 75% of cases. Without the ability to schedule patch deployment through a dedicated patch management tool and automatically catch up on the missing update schedule for an endpoint when it's online, it's hard for IT teams to ensure that all endpoints receive patches at convenient times for users, especially when endpoints are located remotely from the IT department and in different time zones.
- Update errors – 51%. There can be various reasons for update errors, including patch management software incompatibility, lack of proper testing, and others.
- Declined reboots – 46%. Without adequate notification to users before the reboot and developing a workflow that meets their needs, this problem persists because users generally do not like to reboot their machines, which is often required as part of an update.

CHART 18.

WHAT ARE THE TOP REASONS WHY PATCHING FAILS IN YOUR ORGANIZATION? (CHOOSE ALL THAT APPLY.)



> **Patching is a mess here.**
>
> – Anonymous response

*Here are the most common types of answers specified by the respondents for the "Other" option:

- Application interference
- Poor quality control from the vendor
- Driver corruption
- Old Hardware
- Legacy systems

Monitoring for Results

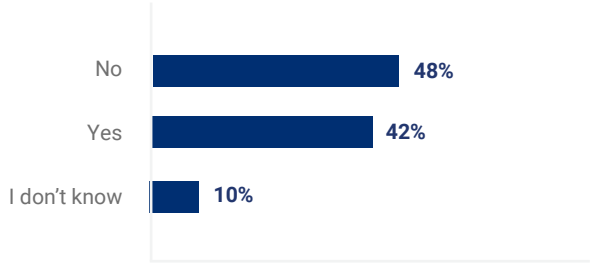
Unfortunately, half of organizations (48%) do not use reports to analyze the effectiveness of their vulnerability remediation efforts.

Half of organizations do not analyze the effectiveness of their vulnerability remediation efforts

Reporting is a critical stage of vulnerability remediation, allowing organizations to identify and analyze gaps in the organization's vulnerability management program. For example, if many vulnerabilities are being re-discovered after they have been patched, this may indicate a gap in the testing or deployment process. Overall, reporting helps organizations identify areas for improvement in their vulnerability management program and improve its effectiveness over time.

CHART 19.

DO YOU USE SCHEDULED REPORTS TO MONITOR THE EFFECTIVENESS OF YOUR VULNERABILITY REMEDIATION EFFORTS?



Part III. Key Recommendations

The survey provided valuable insights into the state of vulnerability remediation among organizations and made recommendations on how organizations can increase resilience under limited resources in 2023:

- **Enforce the zero trust approach.** Implementing least-privilege access everywhere is one of the key principles of zero trust. However, the work-from-anywhere reality may make it challenging for IT teams to control privileged access. Performing IT tasks, such as application deployment on remote workers' devices, requires admin access and can result in unwanted local admin accounts on users' machines, increasing security risk. To address this, organizations should implement technologies that allow IT teams to manage and support their endpoints remotely without requiring local admin rights and build a "closed loop" system for privileged access, ensuring that only trustworthy devices and accounts are used for privileged access to business-sensitive systems. It is also vital to implement granular controls on who is accessing what, push encryption, enforce MFA on all accounts, and enforce endpoint protection.

- **Avoid legacy security vulnerabilities representing the biggest risk.** The most common root cause of breaches is known vulnerabilities, for which proof-of-concept exploit code is publicly available and is broadly leveraged by attackers. That is why any delays in patching publicly known security flaws put the company at significant risk. Organizations must ensure that methods and processes across their fleet of remote and in-office endpoints enable them to detect unpatched security vulnerabilities, prioritize them effectively, and remediate them before they are exploited. It includes establishing a set of policies for continuous patch compliance, allowing IT teams to test updates effectively, and automating patch deployment to meet the needs of an organization and its users.

- **Take cybersecurity awareness to the next level.** Modern social engineering attacks often use a combination of communication channels such as email, phone calls, SMS, and messengers. With the recent theft of terabytes of data, attackers increasingly use this information to personalize their messaging and pose as trusted organizations. In this context, organizations can no longer rely on a passive approach to cybersecurity awareness training. All employees must know how to identify phishing and follow the principle of verifying requests before trusting them. For example, they can use methods other than the initial contact to verify the request, assuming that any data received may have already been leaked and is now being used for hacking purposes.

- **Leverage automation to reduce costs and enhance cybersecurity.** Justifying the need for cybersecurity investment to the executive team may be challenging for tech leaders. Unlike other business functions, the return from investing in IT security is unclear to executives. However, the importance of investing in a strong security posture becomes more evident when compared to the damage from data breaches and ransomware attacks. Plus, by highlighting savings in terms of improved quality of execution of cybersecurity policies and improved IT productivity through automation, it becomes easier to articulate the value of cybersecurity initiatives to the executive team. To get their support, tech leaders should speak with executives in the same language.

Part IV. Appendix

Demography & Methodology

To compile this report, we collected feedback from 804 IT professionals. Respondents were invited to participate in a giveaway to get a chance to win a small monetary reward. Responses were collected in November 2022.

The survey comprised 24 questions. Our analyses of the results are provided in the “Detailed findings” part of the report.

The charts below illustrate detailed demographics for the respondents.

CHART 1. LOCATION

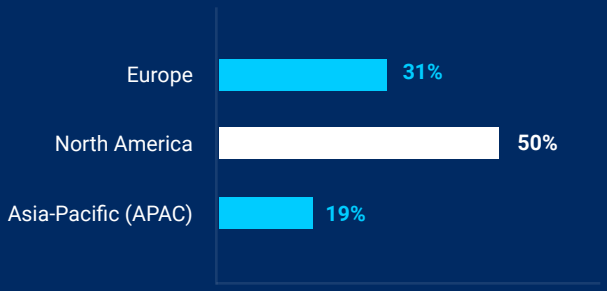


CHART 2. HEADCOUNT

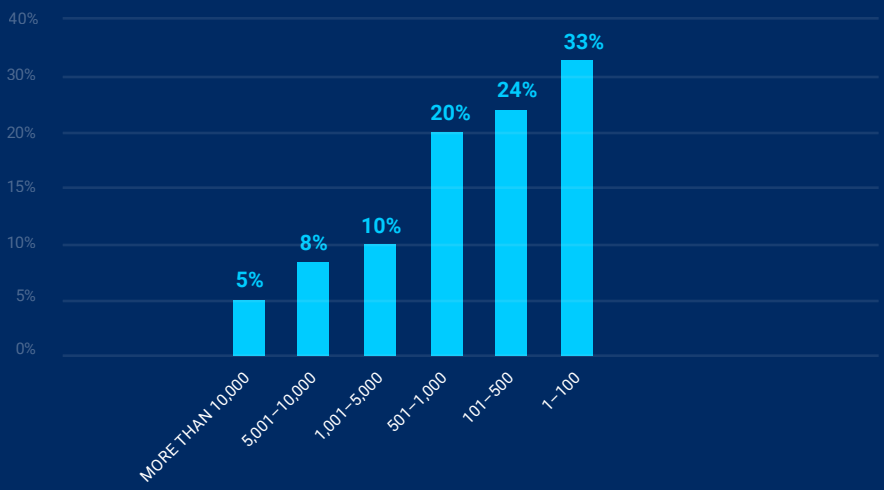


CHART 3. INDUSTRY

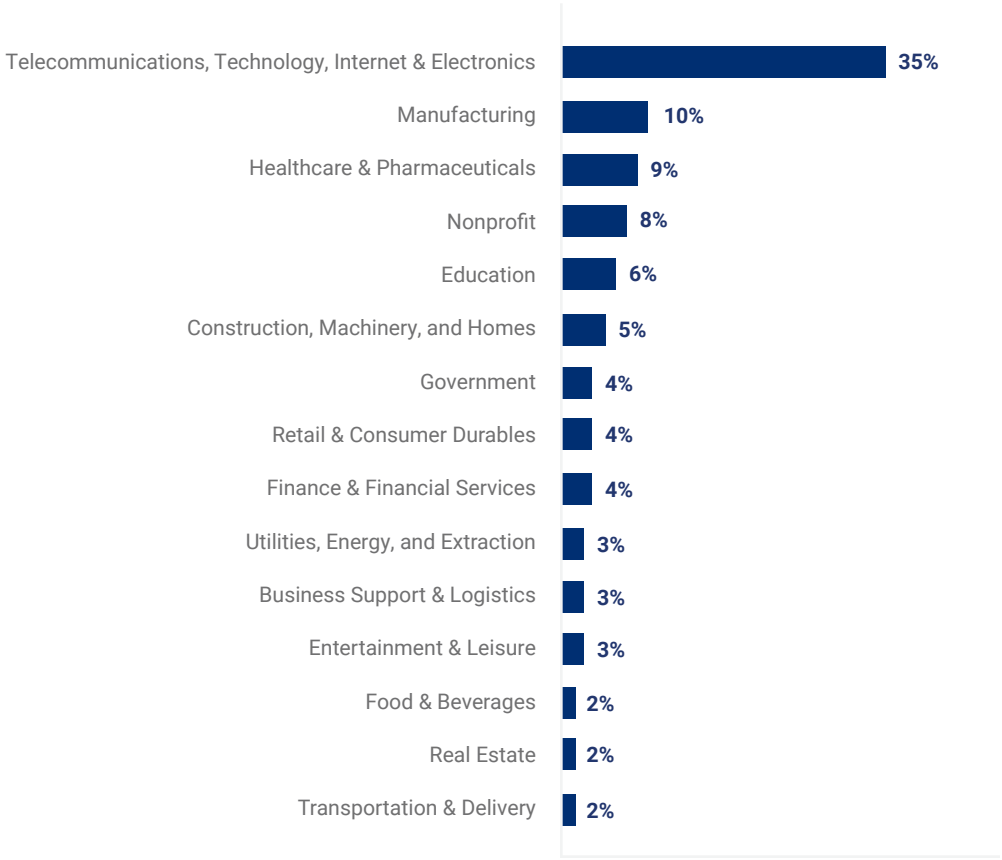


CHART 4. ENDPOINTS MANAGED

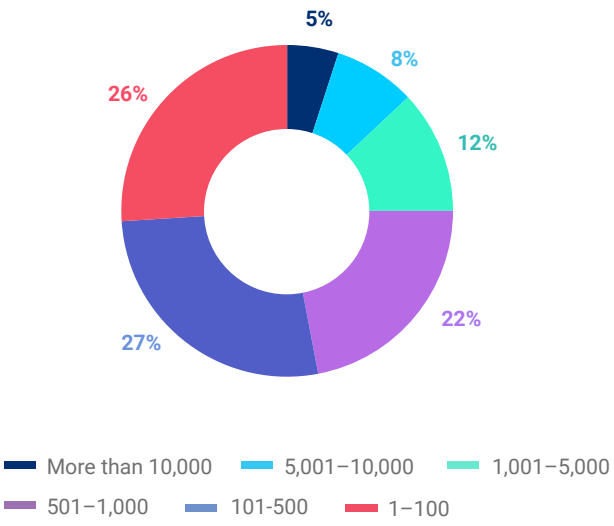
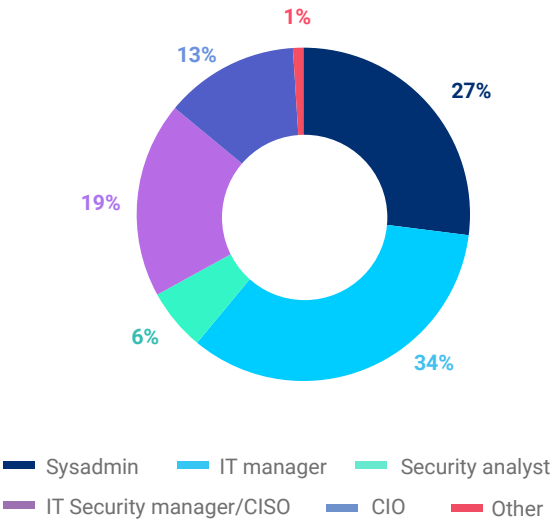


CHART 5. ROLES



About Action1 Research

The report is brought to you by Action1 Research, which conducts industry surveys among IT pros worldwide to discover trends in cybersecurity. For more information, please visit:

www.action1.com/resources/research/

About Action1 Corporation

Action1 is the #1 risk-based patch management platform for distributed networks trusted by thousands of global enterprises. Action1 helps to discover, prioritize, and remediate vulnerabilities in a single solution to prevent security breaches and ransomware attacks. It automates patching of third-party software and operating systems, ensuring continuous patch compliance and remediation of security vulnerabilities before they are exploited.

The company was founded by cybersecurity veterans Alex Vovk and Mike Walters, who previously founded Netwrix, which was acquired by TA Associates. Learn more at: www.action1.com.