Sponsored by

The state of vulnerability management in the cloud and on-premises

Independently conducted by
Ponemon Institute LLC

Publication Date: August 2020

Table of contents

Executive summary

The purpose of this study, sponsored by X-Force Red, IBM Security's team of hackers, is to understand the security challenges organizations face across their on-premises and cloud-based vulnerability management programs.

In April 2020, the Ponemon Institute conducted a global survey of 1,848 IT and IT security professionals. Most of the respondents work in enterprise organizations with at least 1000 employees across a variety of industries. Here are the highlights:

The real risk to organizations is that just one unpatched vulnerability can result in a costly data breach or other security exploit. As shown in this research, an average of 779,935 individual vulnerabilities are identified when running scans. Over the course of six months, an average of 28 percent of these vulnerabilities remain unmitigated. Organizations in this research have an average backlog of 57,555 identified vulnerabilities.

Prioritization and remediation management are critical to an effective vulnerability management program. However, as shown in this research, organizations have difficulty in identifying, prioritizing and patching in a timely manner those vulnerabilities that pose the most risk. As a consequence, organizations face the threat of a criminal compromise.

Top four reasons why patching delays occur

1. Inability to track whether vulnerabilities are patched in a timely manner, according to 58 percent of respondents.
2. No tolerance for the downtime required for patching, according to 58 percent of respondents.
3. Not enough resources to keep up with the volume of patches, according to 55 percent of respondents.
4. No common view of applications and assets across security and IT teams, according to 55 percent of respondents.

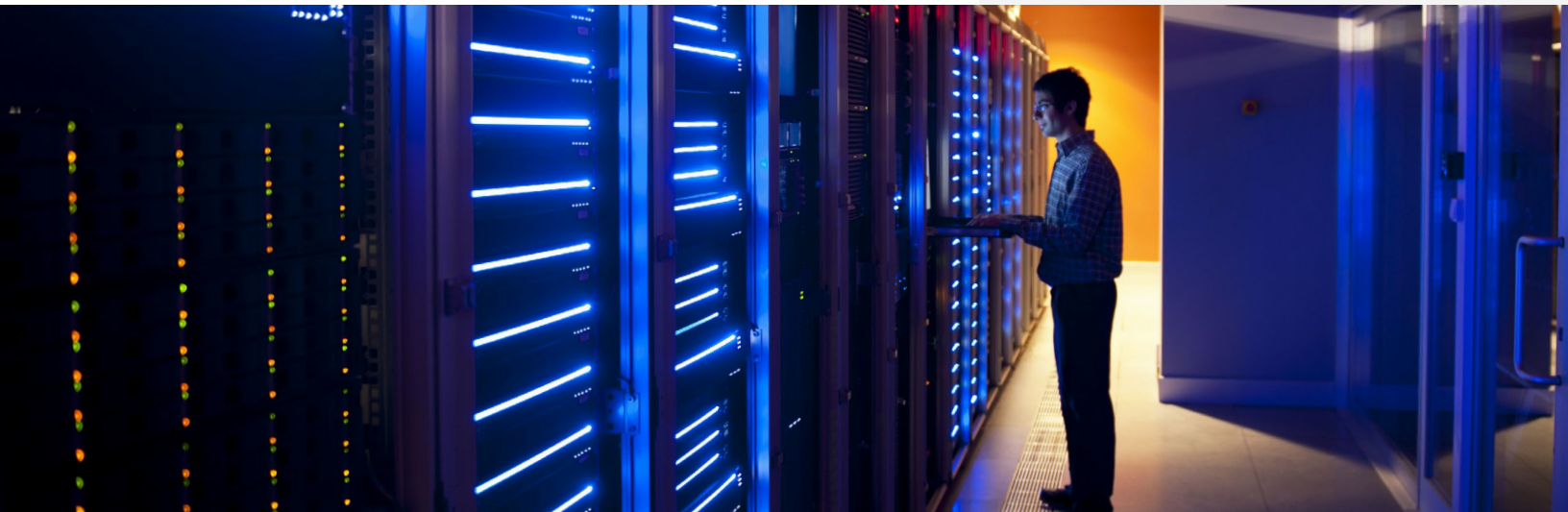
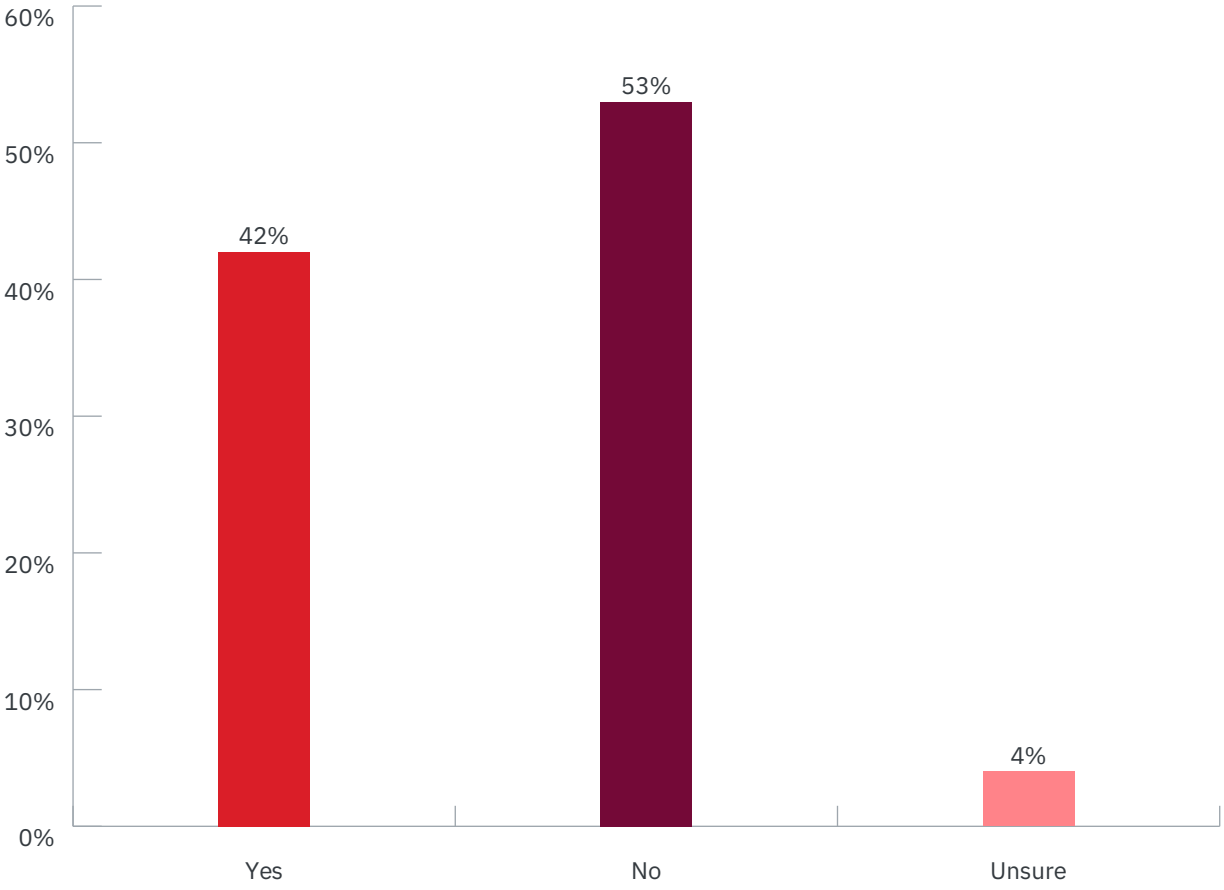


Figure 1:

Did any of these data breaches occur because a patch was available for a known vulnerability but not applied?

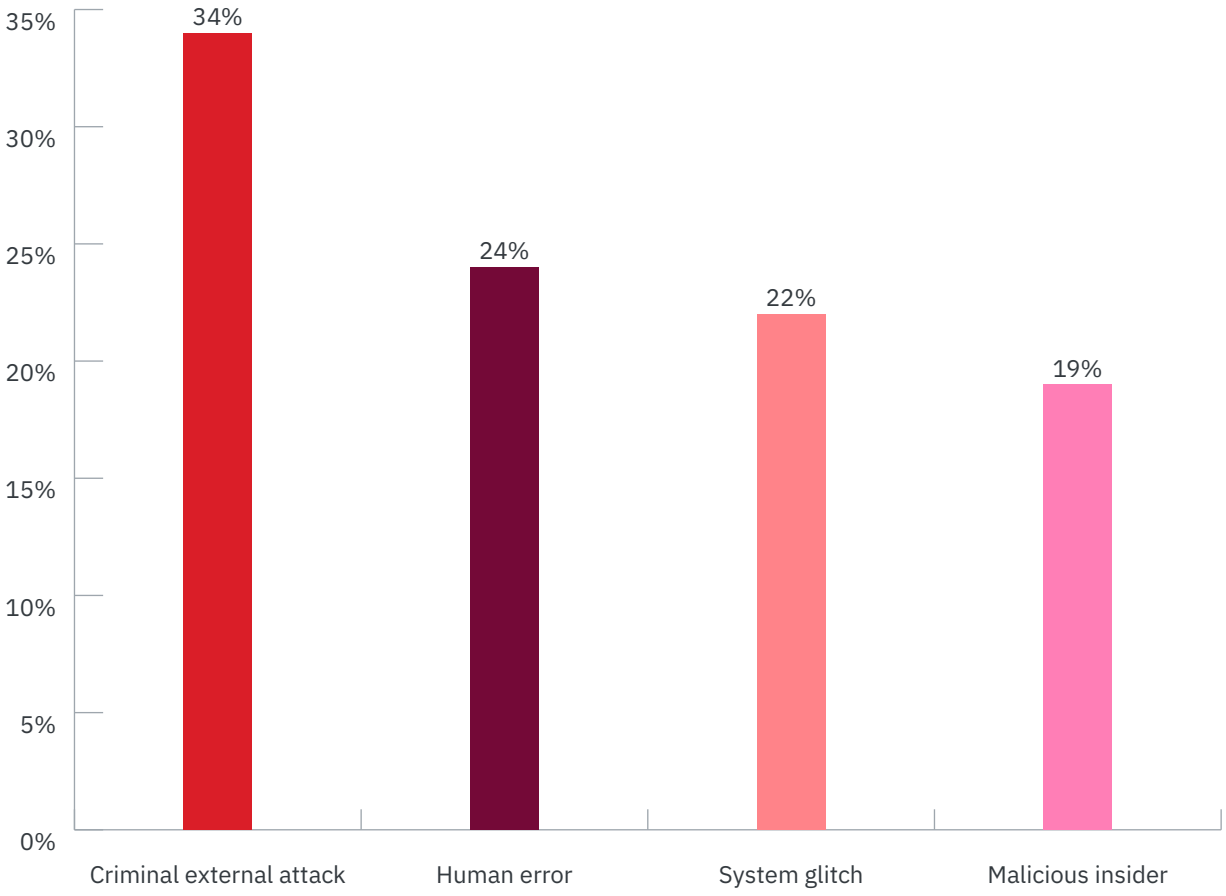


Data breaches occurred because a patch was available but not applied. Fifty-three percent of respondents say their organizations had a data breach in the past two years. As shown in Figure 2, of these data breaches, 42 percent of respondents say they occurred because a patch was available for a known vulnerability but not applied.

Figure 2:

What were the root causes of these data breaches?

Only one choice permitted



According to Figure 2, criminal external attacks were most responsible for these data breaches followed by human error, 34 percent and 24 percent of respondents, respectively.

The following are barriers to achieving an effective vulnerability management program:

- **Most organizations are not prioritizing vulnerabilities based on which exposed assets are most important to the business.** Fifty-seven percent of respondents say their organizations do not know which vulnerabilities pose the highest risk to their businesses. As a result, only 25 percent of respondents are able to prioritize vulnerabilities based on which assets are the most important to the business. Only 37 percent of respondents say their primary method for prioritization is the identification of which vulnerabilities are weaponized.
- **The use of manual processes prevents the timely patching of vulnerabilities.** Fifty percent of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes. More than half (53 percent) of respondents say IT security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable vulnerability backlog.
- **Timely patching is difficult to achieve.** Only 21 percent of respondents say their organizations are highly effective in patching vulnerabilities in a timely manner. According to the research, it can take almost a month (28 days) to patch once a critical or high-risk vulnerability is detected on-premises and 19 days if it is detected in the cloud.
- **Most organizations do not have a single view of the full vulnerability management lifecycle, including exception handling.** Only 27 percent of respondents say they have visibility into the vulnerability management lifecycle making it difficult to ascertain how well their organizations are prioritizing, remediating and patching vulnerabilities.
- **Poor patching because of problems with staffing leads to the exposure of organizations' valuable assets.** Less than half (49 percent) of respondents say their organizations have enough staff to patch in a timely manner and only 41 percent of respondents say the IT security team has the necessary patching skills and training to fix vulnerabilities.

Data stats

57%

of respondents say their organizations do not know which vulnerabilities pose the highest risk to their businesses.

51%

of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes.

21%

of respondents say their organizations are highly effective in patching vulnerabilities in a timely manner.

27%

of respondents say they have visibility into the vulnerability management lifecycle.

49%

of respondents say their organizations have enough staff to patch in a timely manner.

- **Chasing down false positives leaves the most valuable assets exposed.** Sixty percent of respondents say as a result of chasing down false positives and vulnerabilities that pose minimal risk, the most dangerous vulnerabilities continue to expose valuable assets.
- **Nineteen percent of respondents say their organizations do not scan during cloud migration.** Thirty-eight percent scan the cloud during migration and 43 percent of respondents say they scan the cloud environment after migration. Only 30 percent of respondents say their organizations scan systems, applications and networks for vulnerabilities more than once per day or daily.
- **Organizations face challenges when storing business-critical applications in containers in the cloud.** Only about one-third (34 percent) of respondents say their organizations put applications in containers. Respondents report that on average 42 percent of their organizations' applications are business-critical and 38 percent of these applications are in containers.
- **The majority of organizations are uncertain about the security of applications in containers and placed in the cloud.** Of those respondents that store business-critical applications, 57 percent of respondents say they do not know if the applications in the containers were designed securely and 56 percent of respondents say they are uncertain as to whether the applications in the containers were tested to find and fix high-risk vulnerabilities that an attacker may exploit.
- **To overcome uncertainty about the security of applications in containers, organizations primarily use scanning tools.** Fifty-nine percent of respondents say their organizations use a scanning tool to identify which applications are business-critical and what kind of data resides in them and 53 percent of respondents say their organizations use a scanning tool to assess the overall security of the container environment on a quarterly basis.

Data stats

60%

of respondents say as a result of chasing down false positives and vulnerabilities that pose minimal risk, the most dangerous vulnerabilities continue to expose valuable assets.

19%

of respondents say their organizations do not scan during cloud migration.

34%

of respondents say their organizations put applications in containers.

57%

of respondents say they do not know if the applications in the containers were designed securely.

59%

of respondents say their organizations use a scanning tool to identify which applications are business-critical and what kind of data resides in them.

Key findings

The Ponemon Institute surveyed 1,848 IT and IT security professionals in the following regions: North America, EMEA, Asia-Pac and Latin America. In this report, we present the consolidated global findings.

Most respondents are responsible for securing systems (60 percent), patching vulnerabilities (53 percent), evaluating vendors (38 percent) and setting priorities (38 percent). All organizations represented in this study use the following cloud services: SaaS (58 percent), PaaS (41 percent) and IaaS (47 percent).

In this section, we present an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. The findings are organized by the following themes:

- Patching is too little, too late
- Problems with current remediation management practices
- Vulnerability management in the cloud vs. on-premises
- Container security challenges
- Conclusion: The X-Force Red Point of View

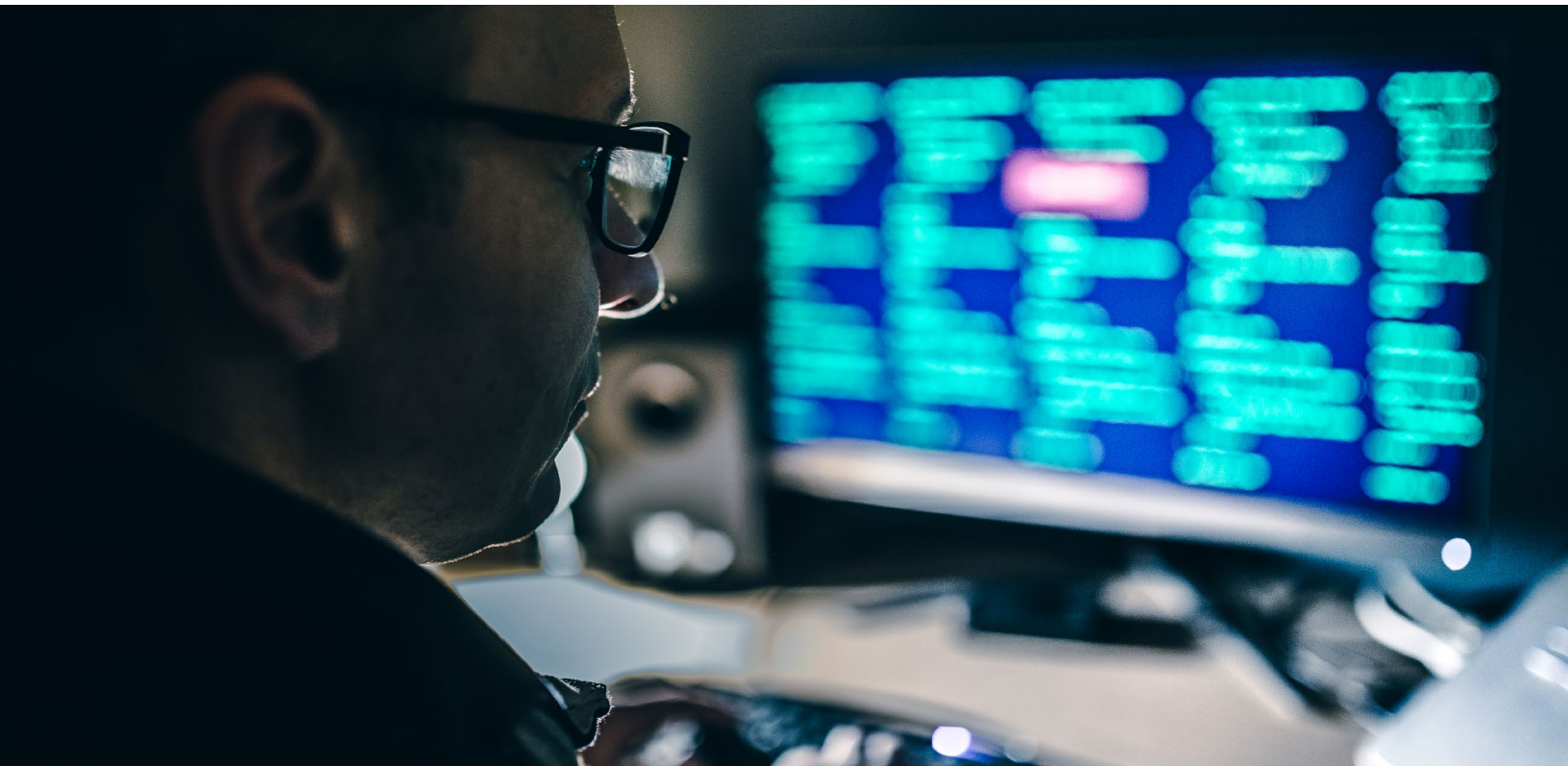
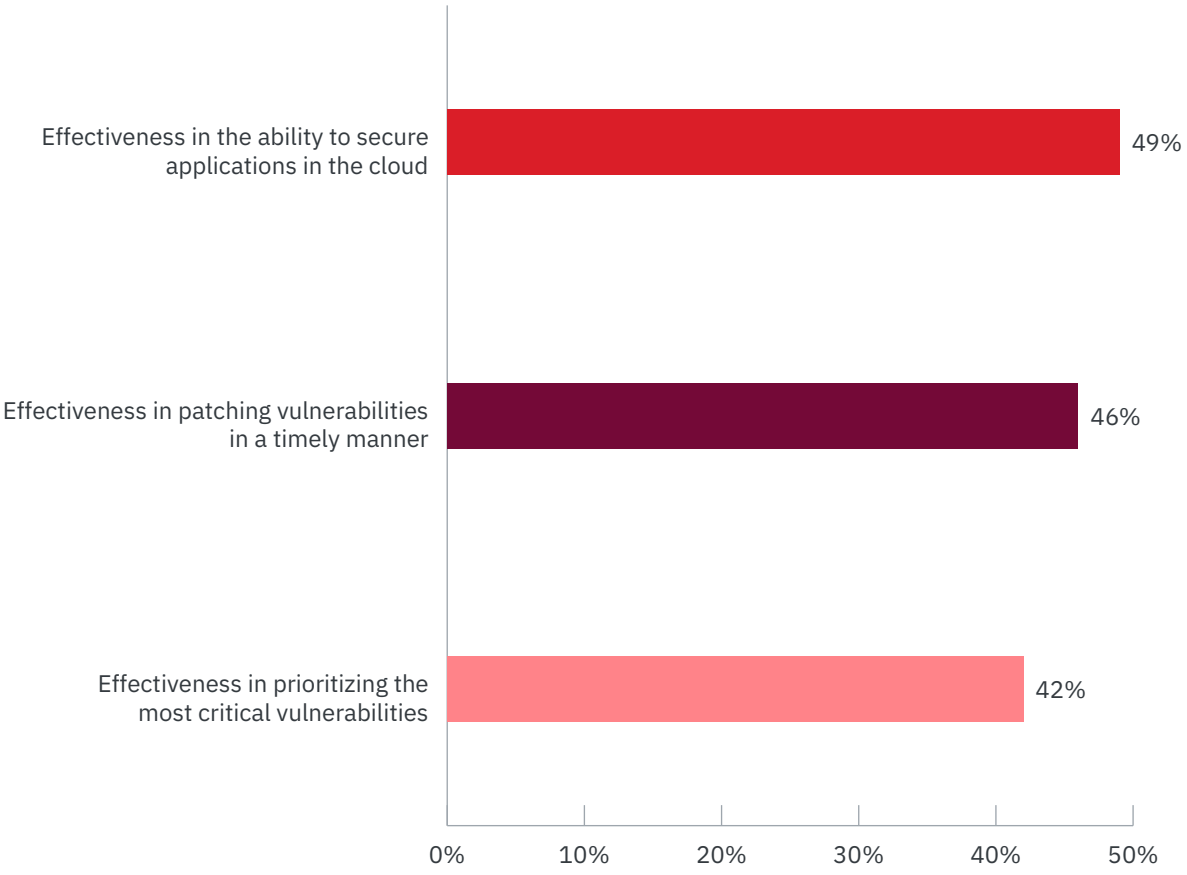


Figure 3:

Perceptions about effectiveness in prioritizing and patching vulnerabilities in a timely manner

On a scale from 1 = low effectiveness to 10 = high effectiveness, Percent of respondents who rated 7 or above



Patching is too little, too late

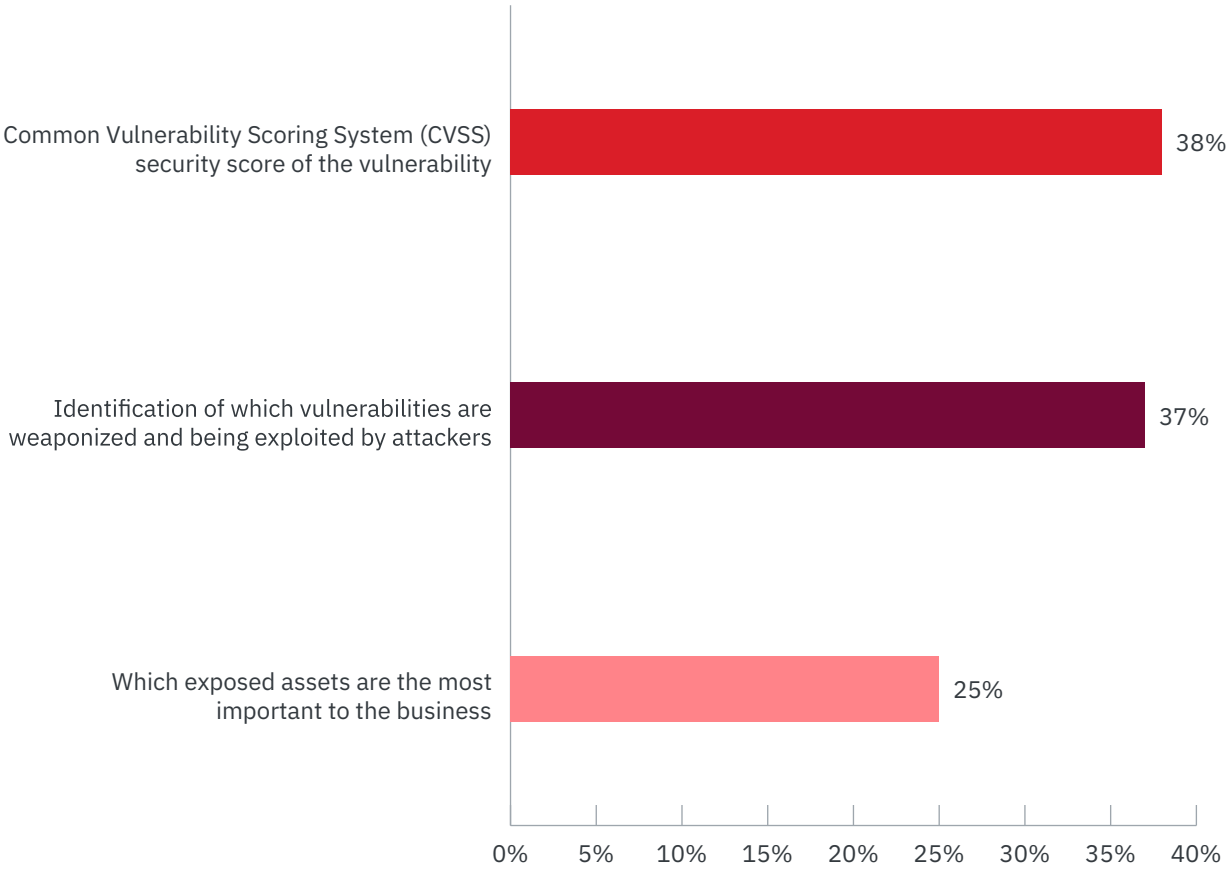
The majority of respondents self-report that their effectiveness in prioritizing and patching vulnerabilities is low, as well as securing applications in the cloud. Respondents were asked to rate the effectiveness of their ability to patch vulnerabilities in a timely manner, to prioritize vulnerabilities and to secure applications in the cloud on a scale of 1= low effectiveness to 10= high effectiveness.

Less than half (49 percent) of respondents rate their effectiveness in securing applications as very high and only 46 percent of respondents say their organizations are very effective in timely patching. Even fewer respondents (42 percent) say their organizations are very effective in prioritizing those vulnerabilities that pose the greatest risk of a compromise, as shown in Figure 3.

Figure 4:

What is your primary method for prioritizing vulnerabilities?

One choice permitted



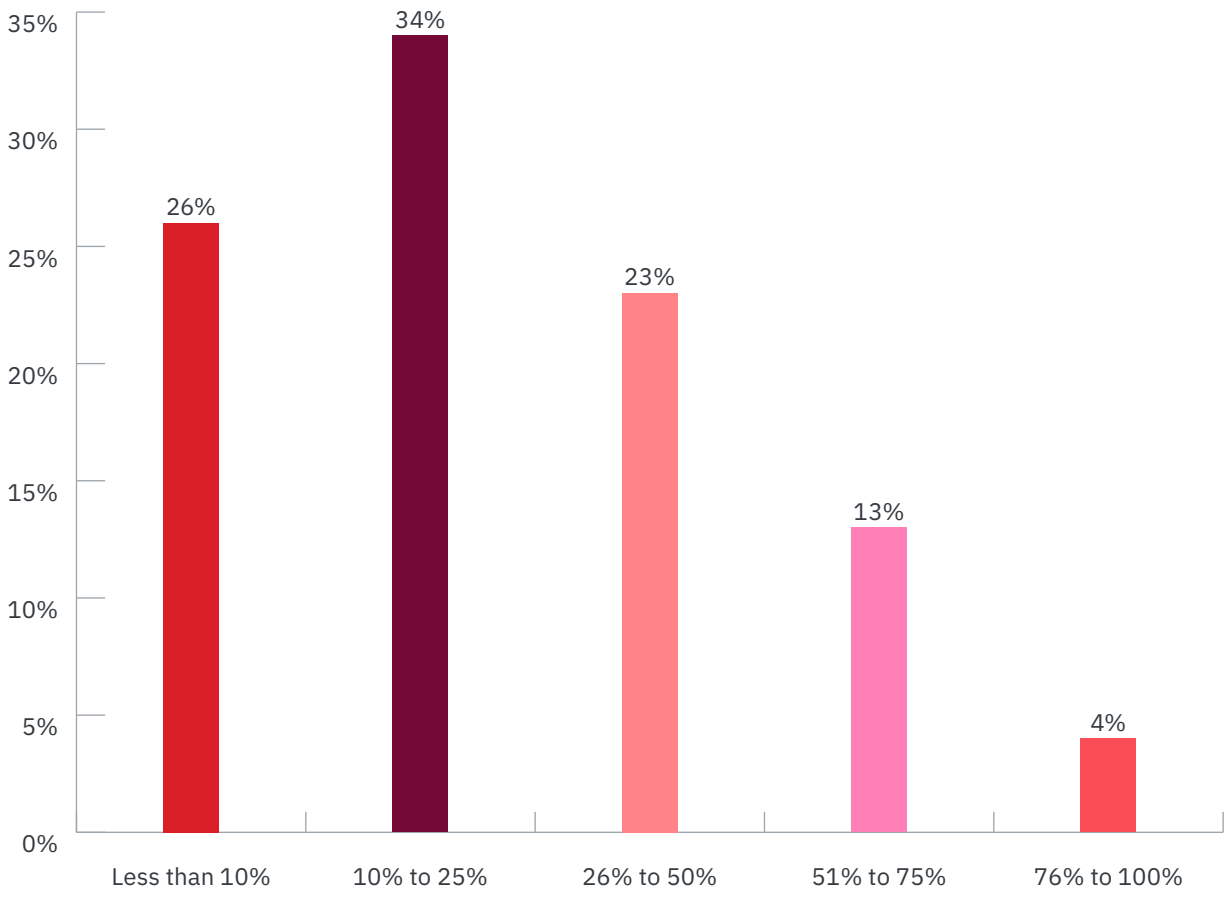
Only 43 percent of respondents say their organizations know which vulnerabilities pose the highest risk. The CVSS is used to rate the severity and risk based on the Common Vulnerabilities and Exposures (CVE) formula. The CVSS generates a numerical criticality score based on many factors, including type of attack, level of access required and overall complexity. The CVSS score ranks vulnerabilities from zero to 10. A 10 indicates the vulnerability is the most critical.

As shown in Figure 4, 38 percent of respondents use CVSS and 37 percent of respondents say their primary method for prioritization is the identification of which vulnerabilities are weaponized and being exploited by attackers. Only 25 percent of respondents say they prioritize based on which exposed assets are the most important to the business. As shown in this research, only 43 percent of respondents say their organizations know which vulnerabilities pose the highest risk.

Figure 5:

What percentage of vulnerabilities remain unmitigated?

Extrapolated value = 28 percent

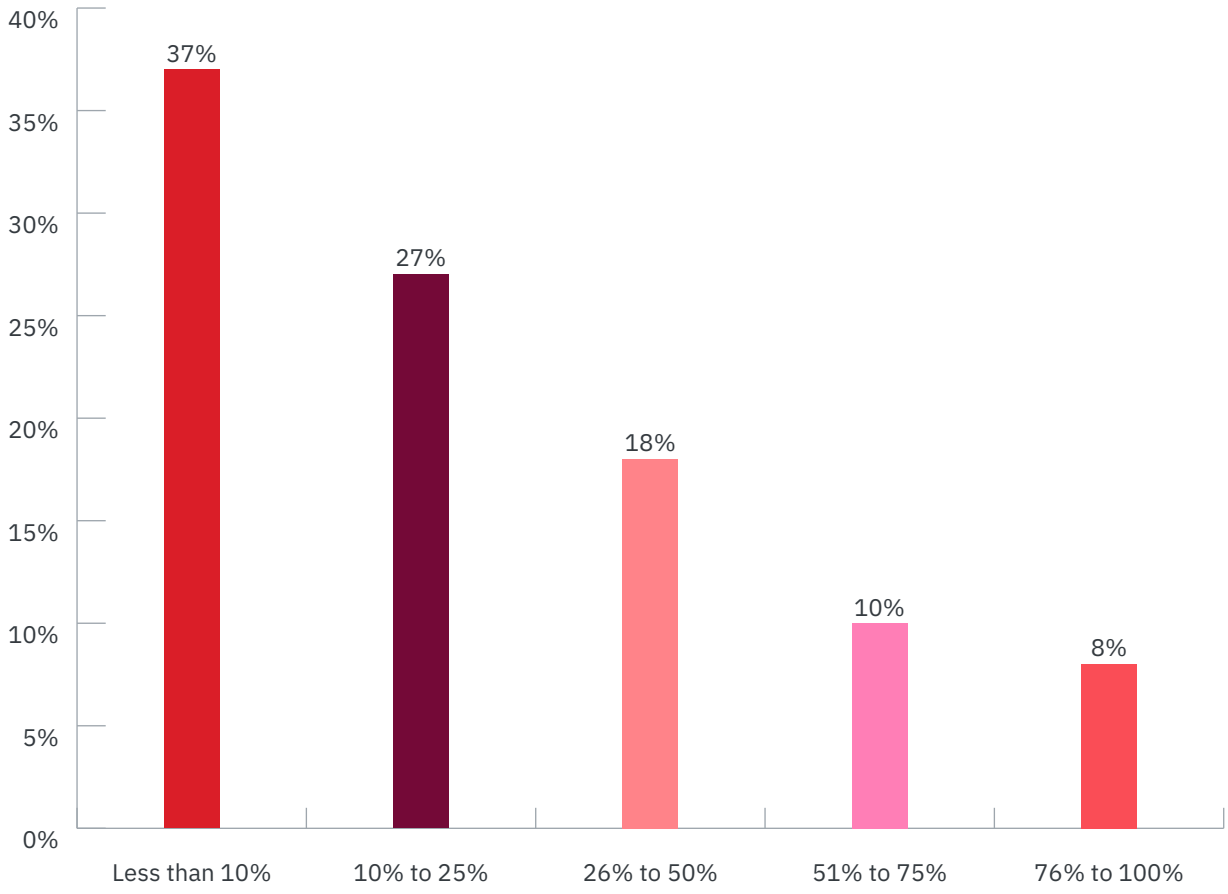


An average of 28 percent of vulnerabilities remain unmitigated. An average of 779,935 individual vulnerabilities are identified when running scans and, as shown in Figure 5, over the course of six months, an average of 28 percent of these vulnerabilities remain unmitigated. Organizations represented in this research have an average vulnerability backlog of 57,555.

Figure 6:

What percentage of unmitigated vulnerabilities are a high risk?

Extrapolated value = 27 percent

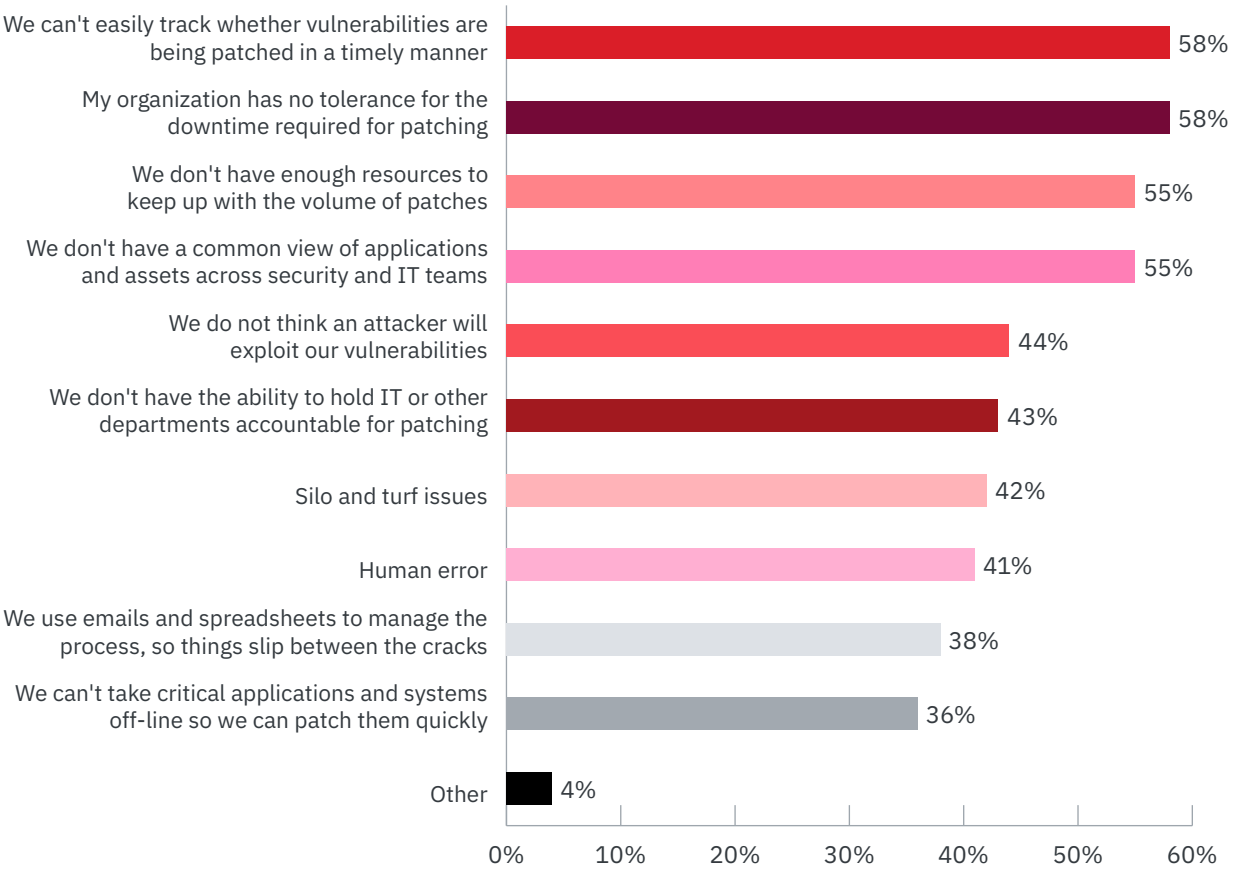


Fifty-seven percent of respondents do not know which unmitigated vulnerabilities are a high risk. Those who do know which vulnerabilities are of greatest risk (43 percent of respondents), an average of 27 percent of these remain unmitigated, according to Figure 6.

Figure 7:

What causes major delays in your vulnerability patching process?

More than one response permitted



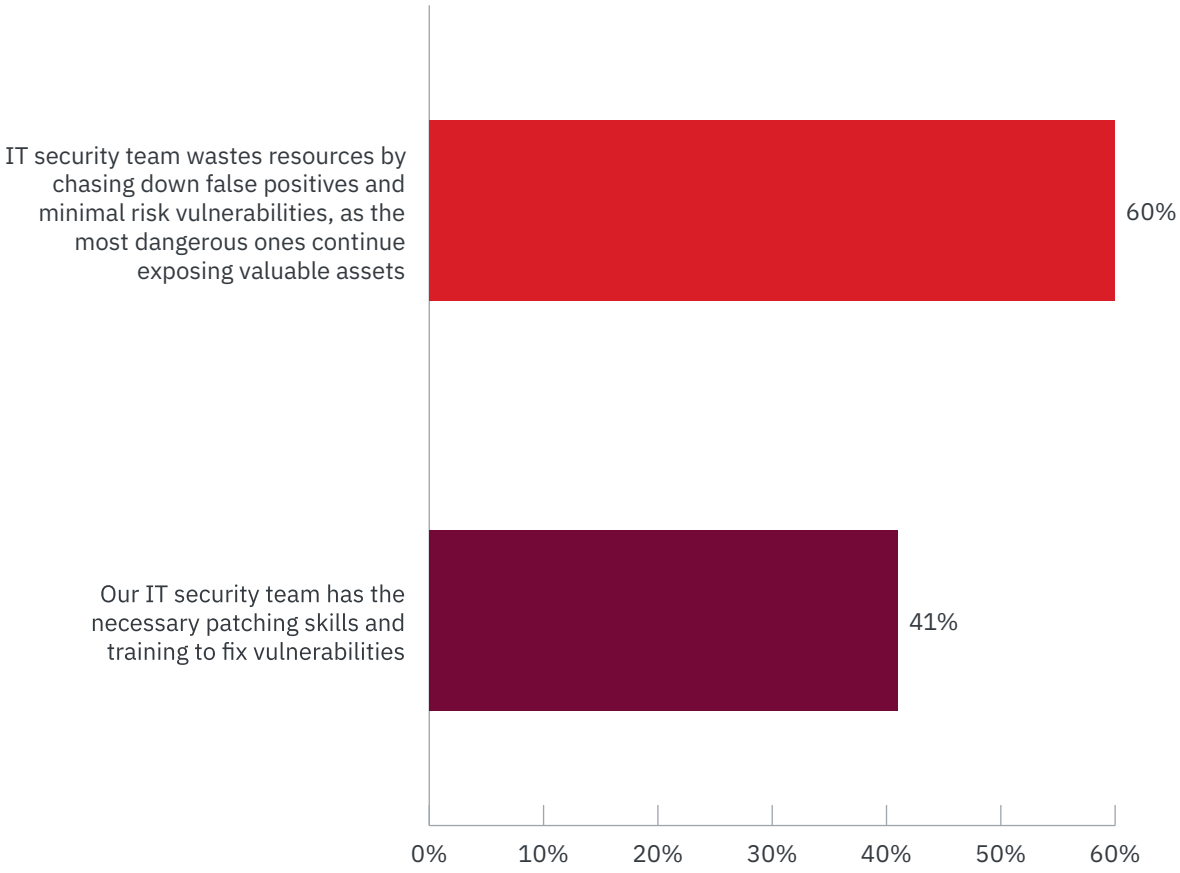
Timely patching is difficult to achieve. Only 21 percent of respondents say their organizations are highly effective in patching vulnerabilities in a timely manner. According to the research, it can take almost a month (28 days) to patch a critical or high-risk vulnerability once it is detected on-premises and 19 days if it is detected in the cloud.

Figure 7 presents a list of reasons why major delays occur in the vulnerability patching process. The majority of respondents cite the inability to track whether vulnerabilities are being patched in a timely manner (58 percent). Another 58 percent of respondents say their organizations have no tolerance for the downtime required for patching. This is followed by not having enough resources to keep up with the volume of patches (55 percent) and the lack of a common view of applications and assets across security and IT teams (55 percent).

Figure 8:

Problems in vulnerability management staffing and patching

Strongly agree and Agree responses combined

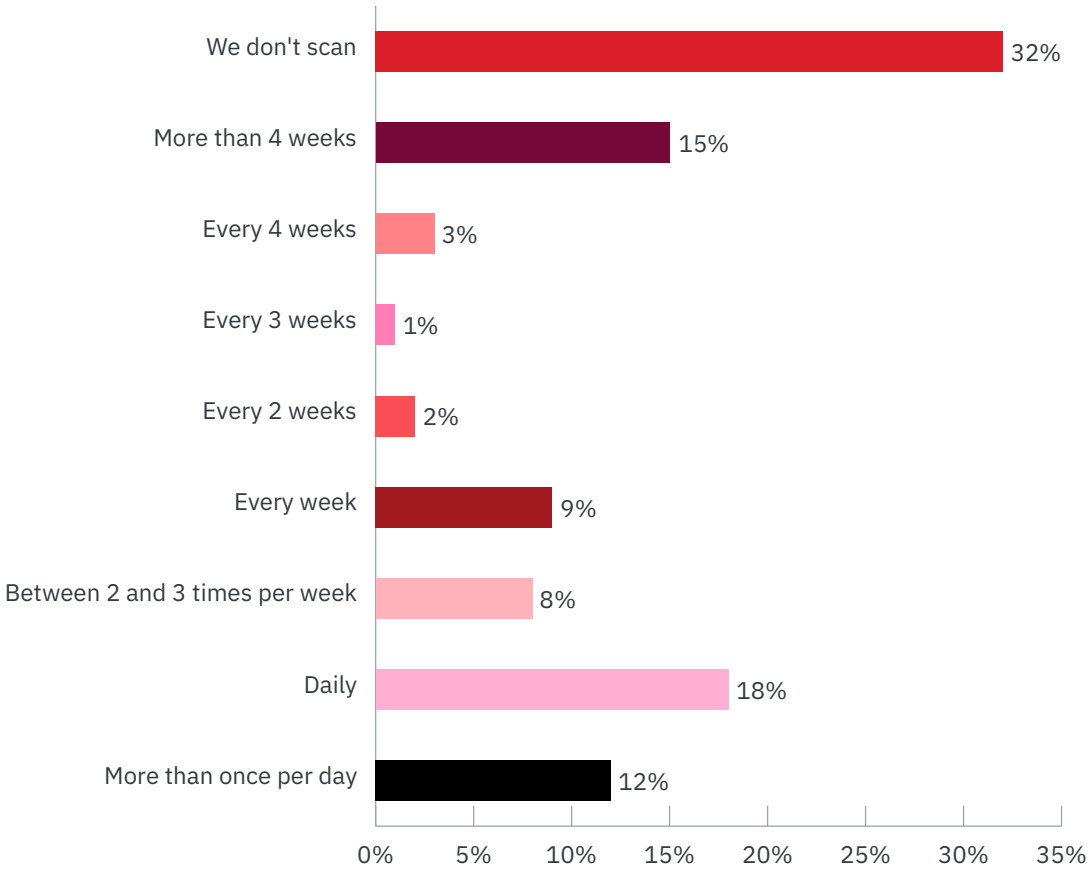


Poor patching because of problems with staffing leads to the exposure of organizations' valuable assets. Less than half (49 percent) of respondents say their organizations have enough staff to patch in a timely manner. More than half (53 percent) of respondents say they will hire staff dedicated to patching in the next 12 months.

According to Figure 8, 60 percent of respondents say as a result of wasted resources caused by chasing down false positives and vulnerabilities that pose minimal risk, the most dangerous vulnerabilities continue exposing valuable assets. Another problem is that only 41 percent of respondents say the IT security team has the necessary patching skills and training to fix vulnerabilities.

Figure 9:

How often does your organization scan systems, applications and networks for vulnerabilities?



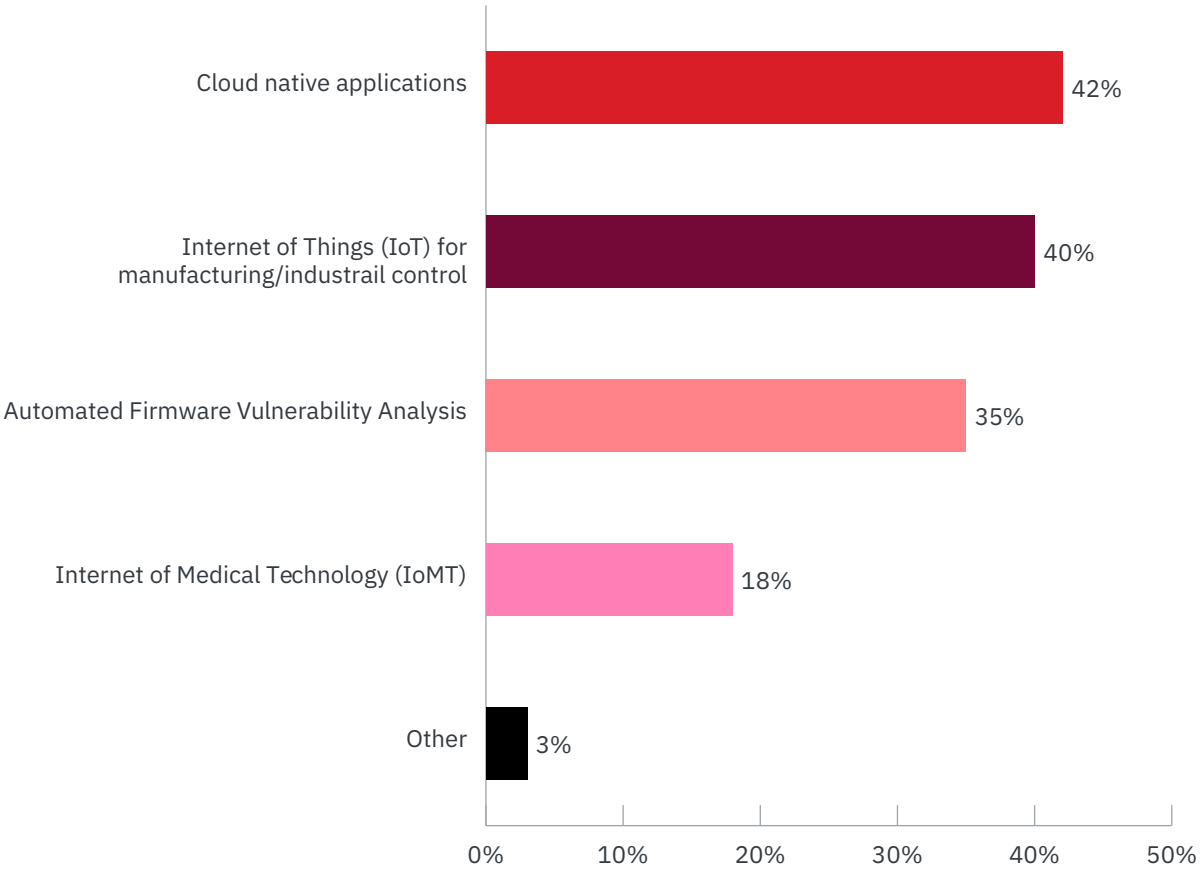
Vulnerability management and remediation

Frequent scanning rarely occurs. Only 30 percent of respondents say their organizations scan systems, applications and networks for vulnerabilities more than once per day or daily, as shown in Figure 9. About one-third (32 percent) of respondents do not scan their systems, applications and networks.

Figure 10:

Is your organization considering vulnerability scanning for any of the emerging technology sectors?

More than one response permitted

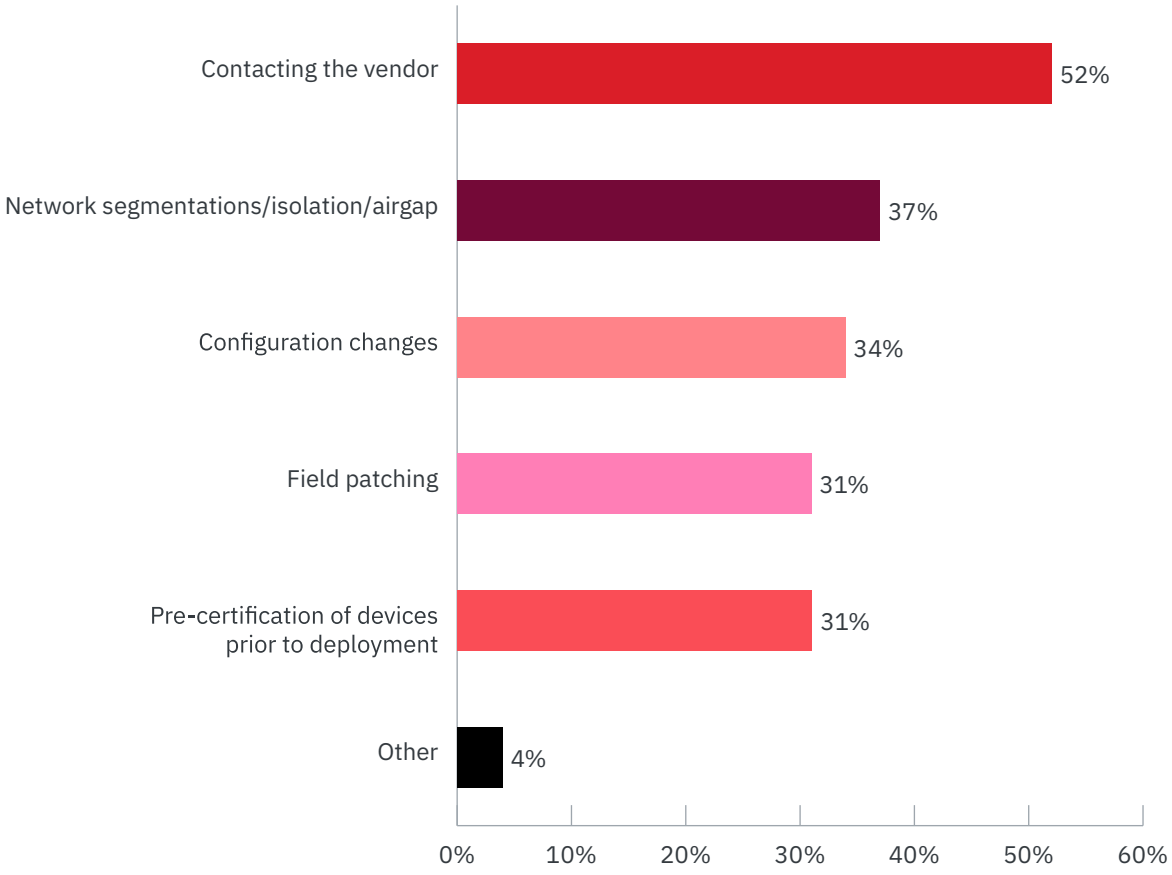


Organizations are considering vulnerability scanning for IoT devices in manufacturing/industrial controls. According to Figure 10, 42 percent of respondents say their organizations are considering vulnerability scanning of cloud native applications followed by 40 percent of respondents who say their organizations might scan IoT devices in manufacturing/industrial controls.

Figure 11:

What remediation strategies does your organization perform based on IoT scanner findings?

More than one response permitted

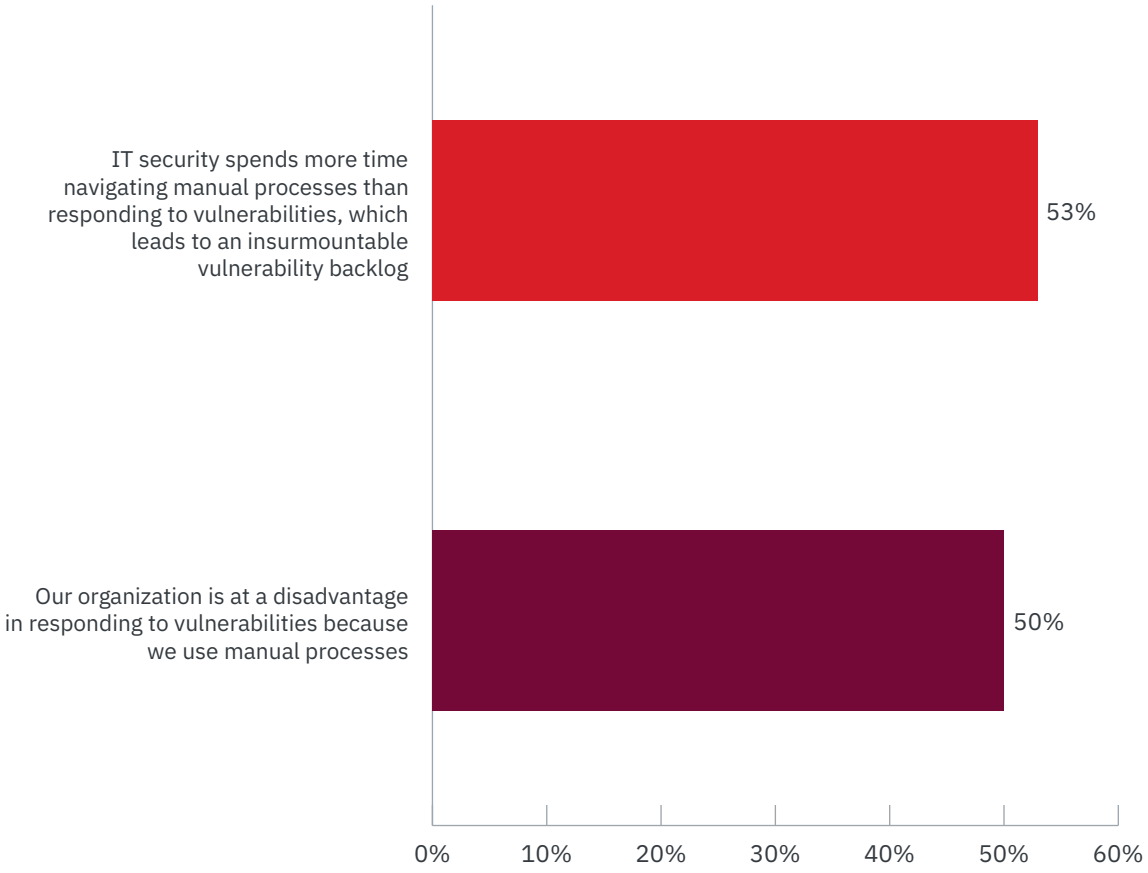


Despite the risk created by unsecured IoT devices, only 32 percent of respondents say their organizations currently perform vulnerability scanning on IoT devices. According to Figure 11, if they do scan, the remediation strategy most often used is to contact the vendor (52 percent of respondents) followed by network segmentation/airgap (37 percent of respondents). Only 31 percent of respondents say they require pre-certification of devices prior to deployment.

Figure 12:

Perceptions about the use of manual processes

Strongly agree and Agree responses combined



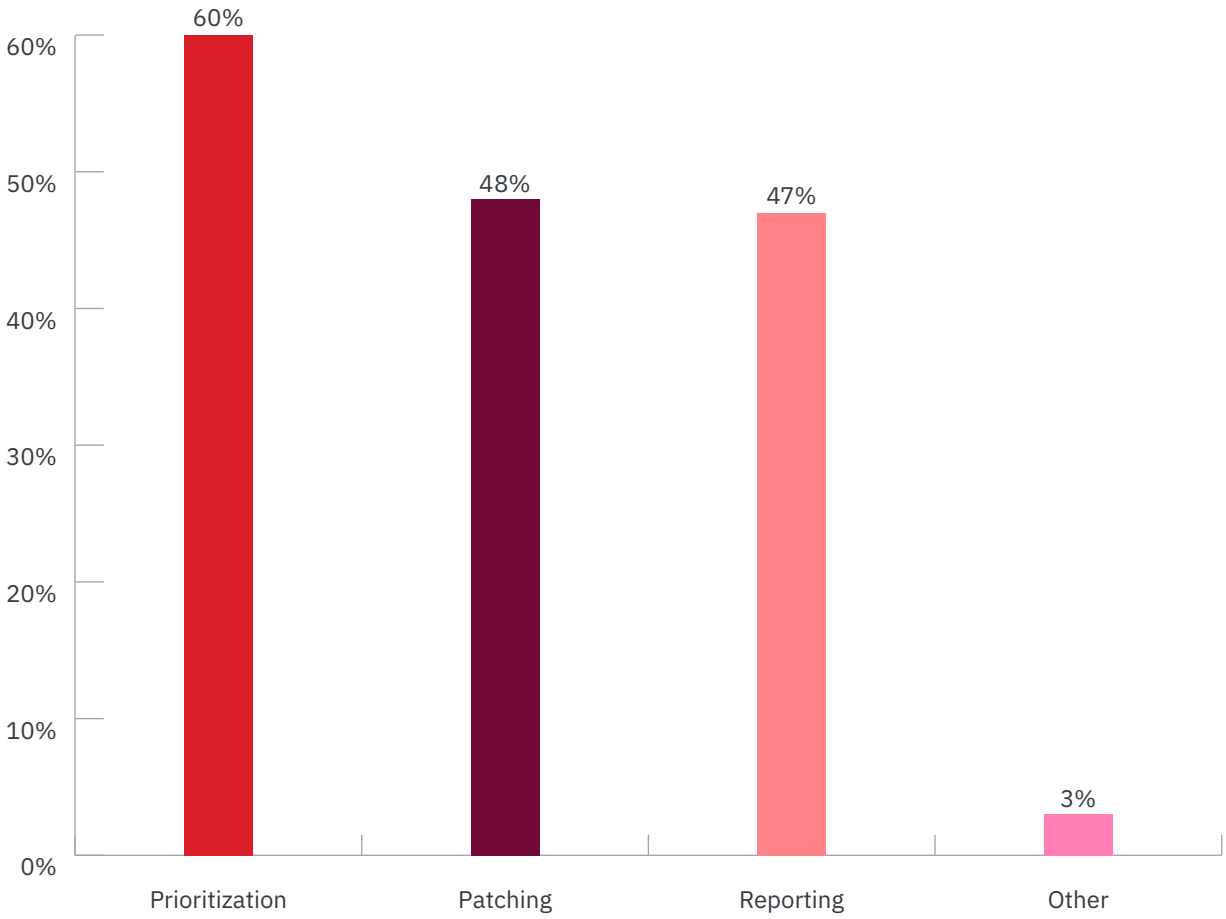
The use of manual processes prevents the timely patching of vulnerabilities. In contrast to automated processes, which are programmed to auto-assign tasks, manual processes require a human to push the tasks through every step and know whom to send them to. In addition, manual processes require all fields to be completed manually while automation allows some fields to be auto-filled with regular details and computations.

As shown in Figure 12, more than half (53 percent) of respondents say IT security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable vulnerability backlog. Fifty percent of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes.

Figure 13:

What steps do you automate?

More than one response permitted

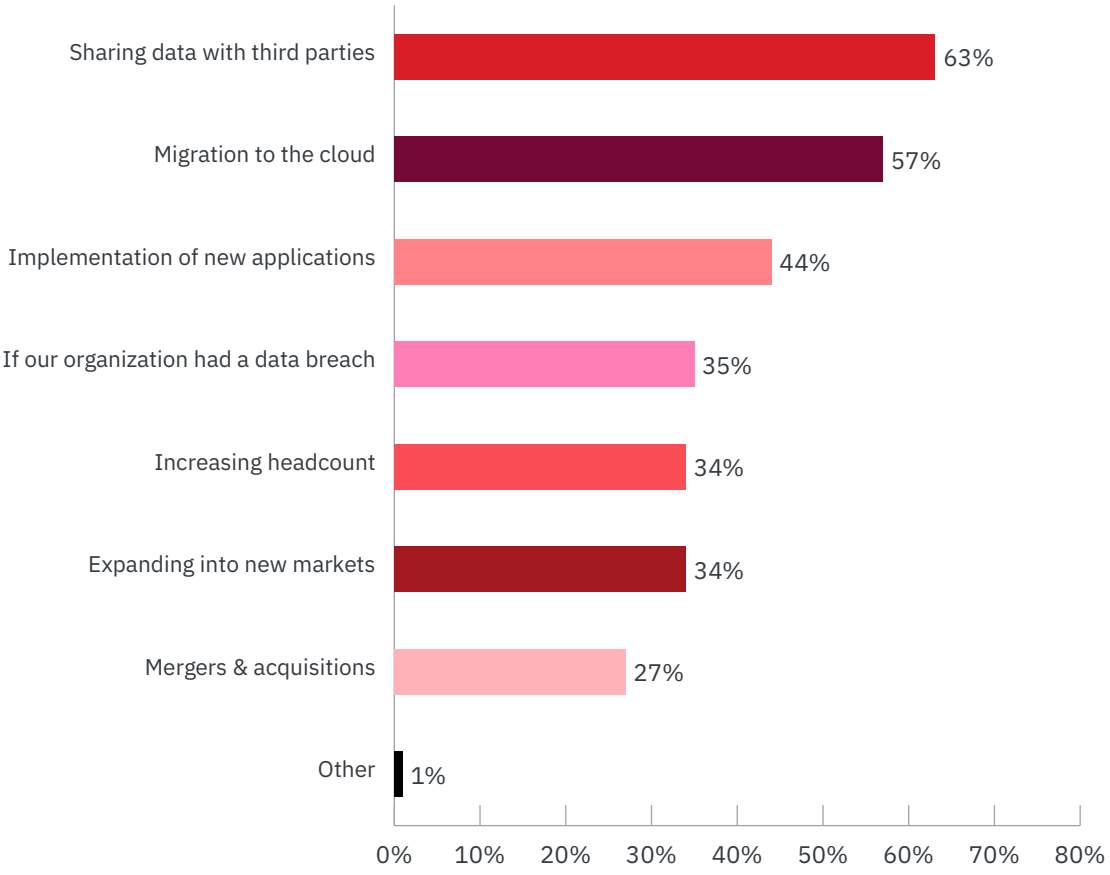


Most organizations are automating the prioritization of vulnerabilities. Fifty-six percent of respondents say organizations use automation to assist with vulnerability management. As shown in Figure 13, of those respondents, 60 percent say their organizations use automation to prioritize vulnerabilities followed by patching (48 percent of respondents) and reporting (47 percent of respondents).

Figure 14:

Which events do you believe can increase vulnerabilities?

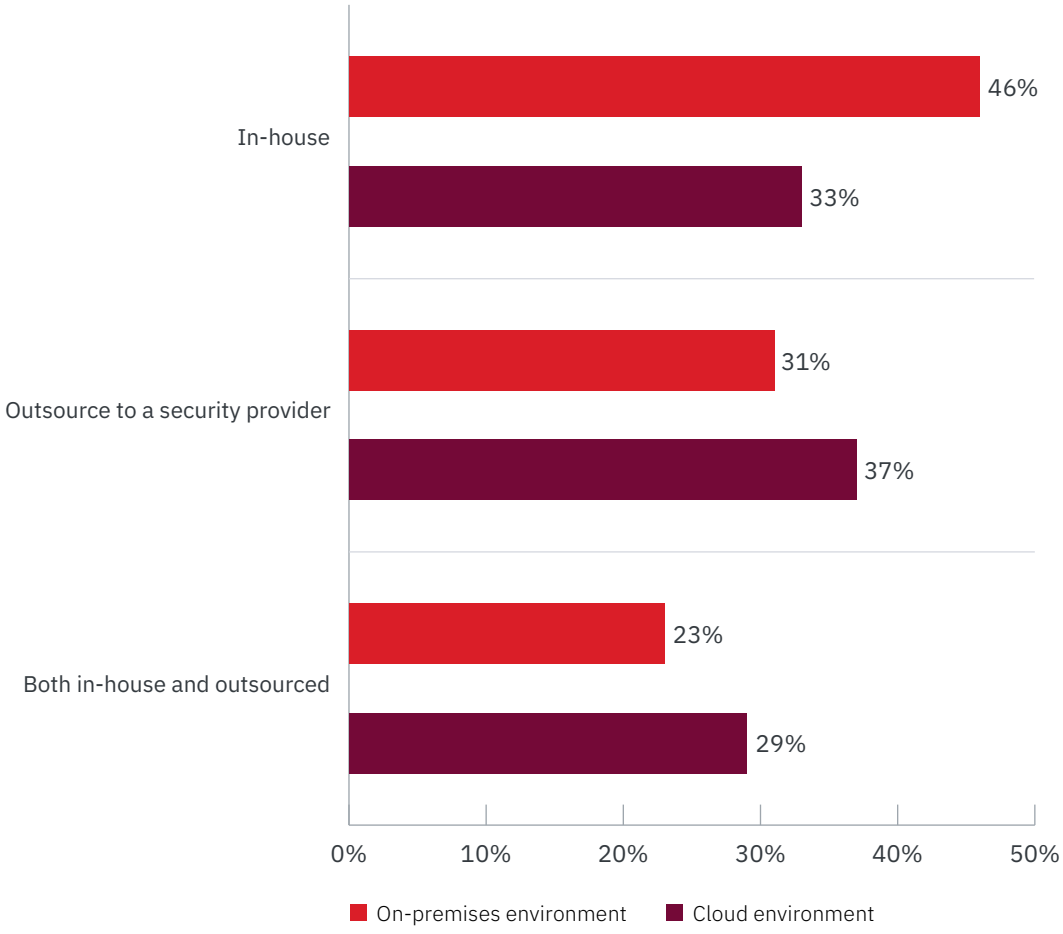
More than one response permitted



Third-party risk is top of mind with respondents. Figure 14 presents a series of events that can increase vulnerabilities. Sixty-three percent of respondents say sharing data with third parties can increase vulnerabilities followed by migration to the cloud (57 percent of respondents). The least likely to increase vulnerabilities is expanding into new markets and engaging in mergers and acquisitions.

Figure 15:

How is the vulnerability management program managed in the on-premises and cloud environments?



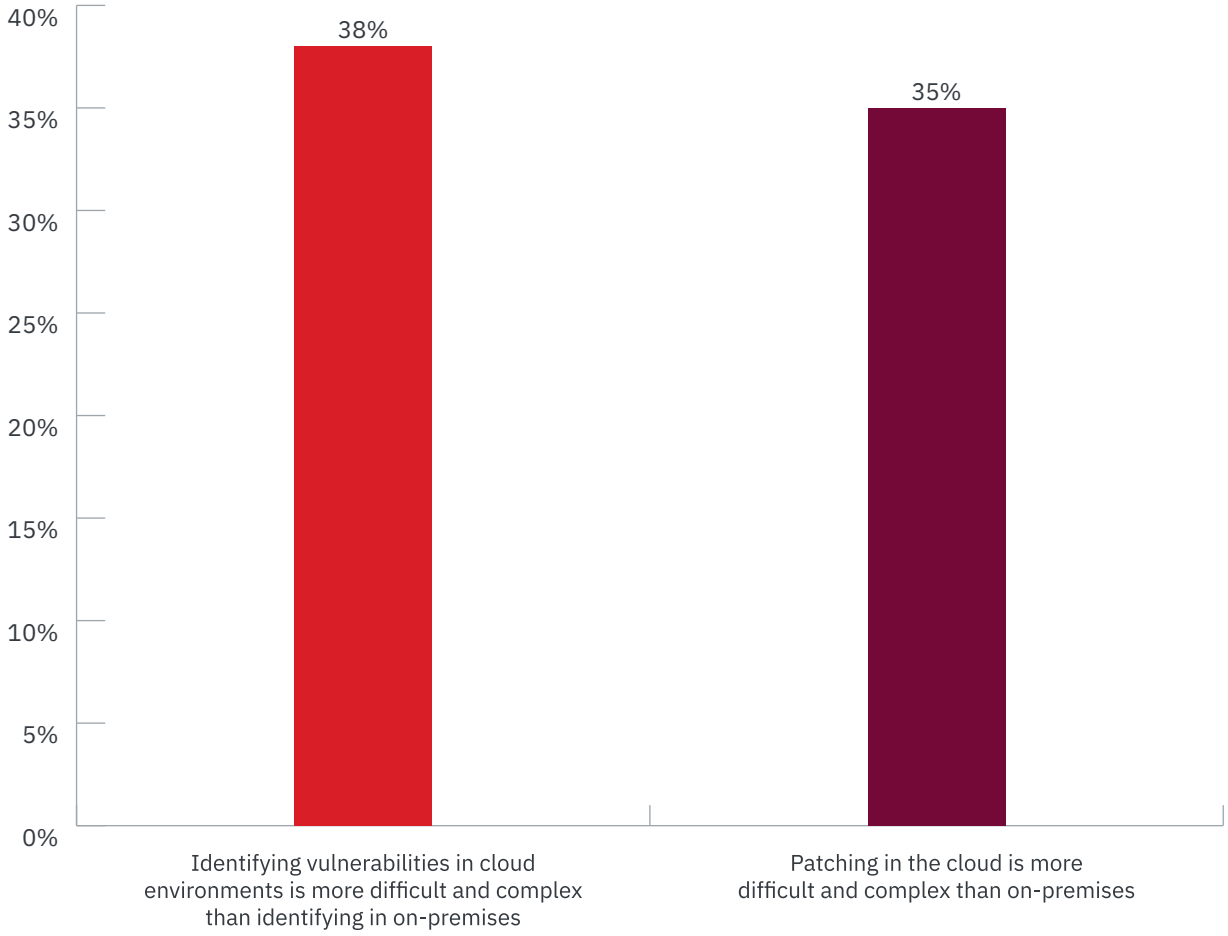
Vulnerability management practices in the cloud and on-premises

Vulnerability management varies significantly based on whether it occurs on-premises or in the cloud. According to Figure 15, 46 percent of respondents say their on-premises vulnerability management programs are managed in-house. In contrast, if vulnerabilities are managed in the cloud, only one-third (33 percent) of respondents say their vulnerability management programs are managed in-house. Slightly more organizations that manage vulnerabilities in the cloud say they outsource the management to a security provider (37 percent of respondents vs. 31 percent of respondents).

Figure 16:

Perceptions about vulnerability management and patching in the cloud and on-premise

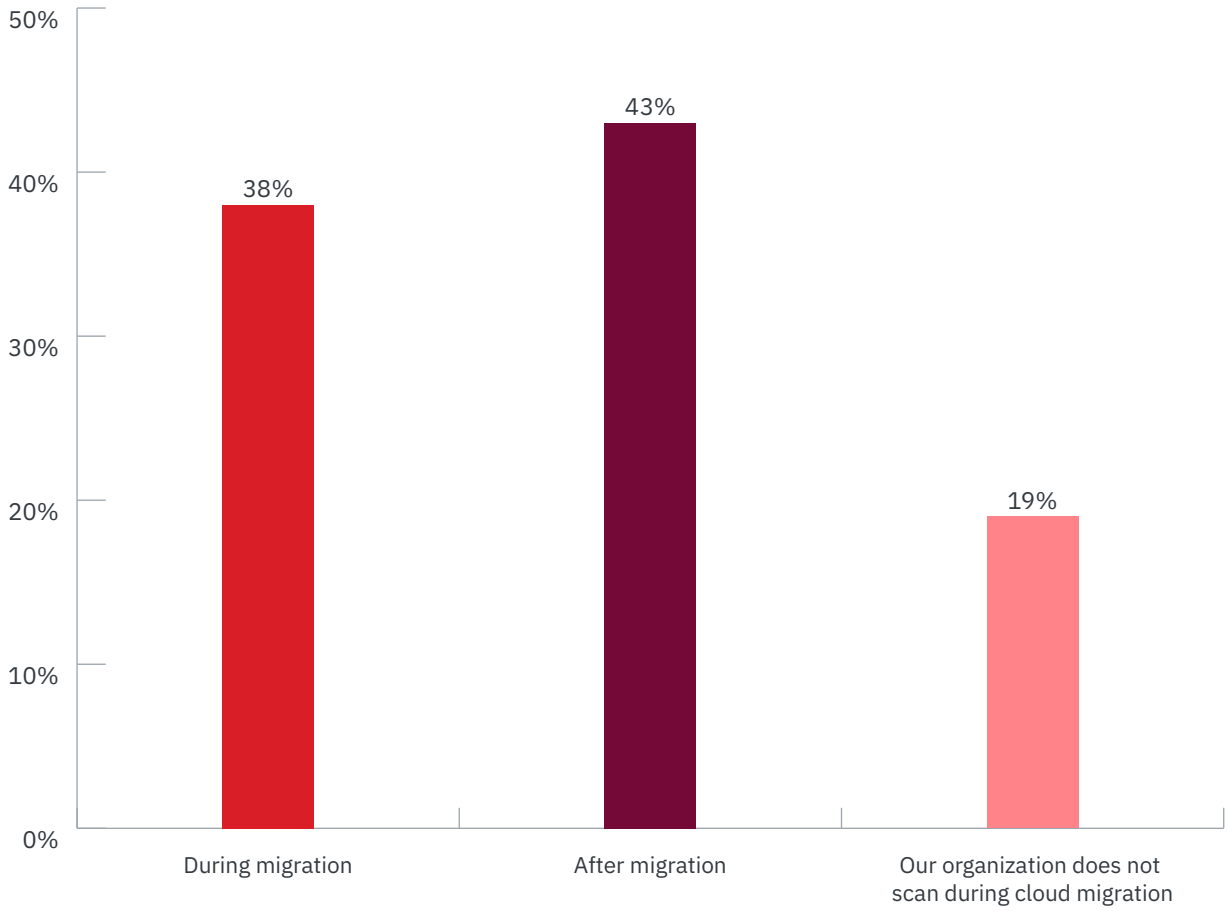
Strongly agree and Agree responses combined



The cloud does not make it more difficult to identify and patch vulnerabilities. As shown in Figure 16, only 38 percent of respondents say identifying vulnerabilities in cloud environments is more difficult and complex than identifying vulnerabilities on-premises. Only 35 percent of respondents say patching in the cloud is more difficult and complex than on-premises.

Figure 17:

During migration at what point does your organization scan the cloud environment?

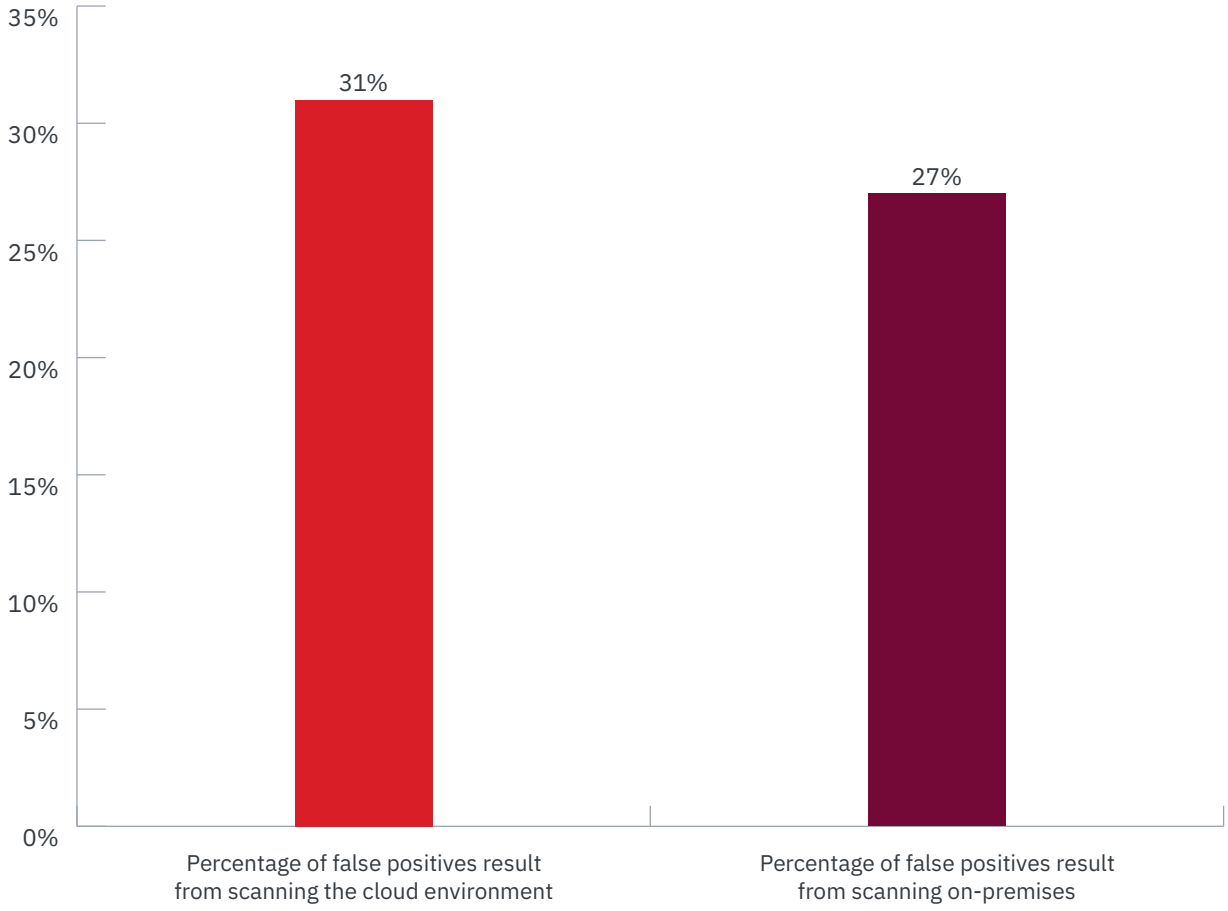


Nineteen percent of respondents say their organizations do not scan during cloud migration. According to Figure 17, 19 percent of respondents say their organizations do not scan the cloud environment for vulnerabilities during migration. Forty-three percent of respondents say their organization scans for vulnerabilities after migration to the cloud. Only 38 percent of respondents say their scans occurred during migration.

Figure 18:

What percentage of false positives result from scanning in the cloud and on-premises

Extrapolated values presented

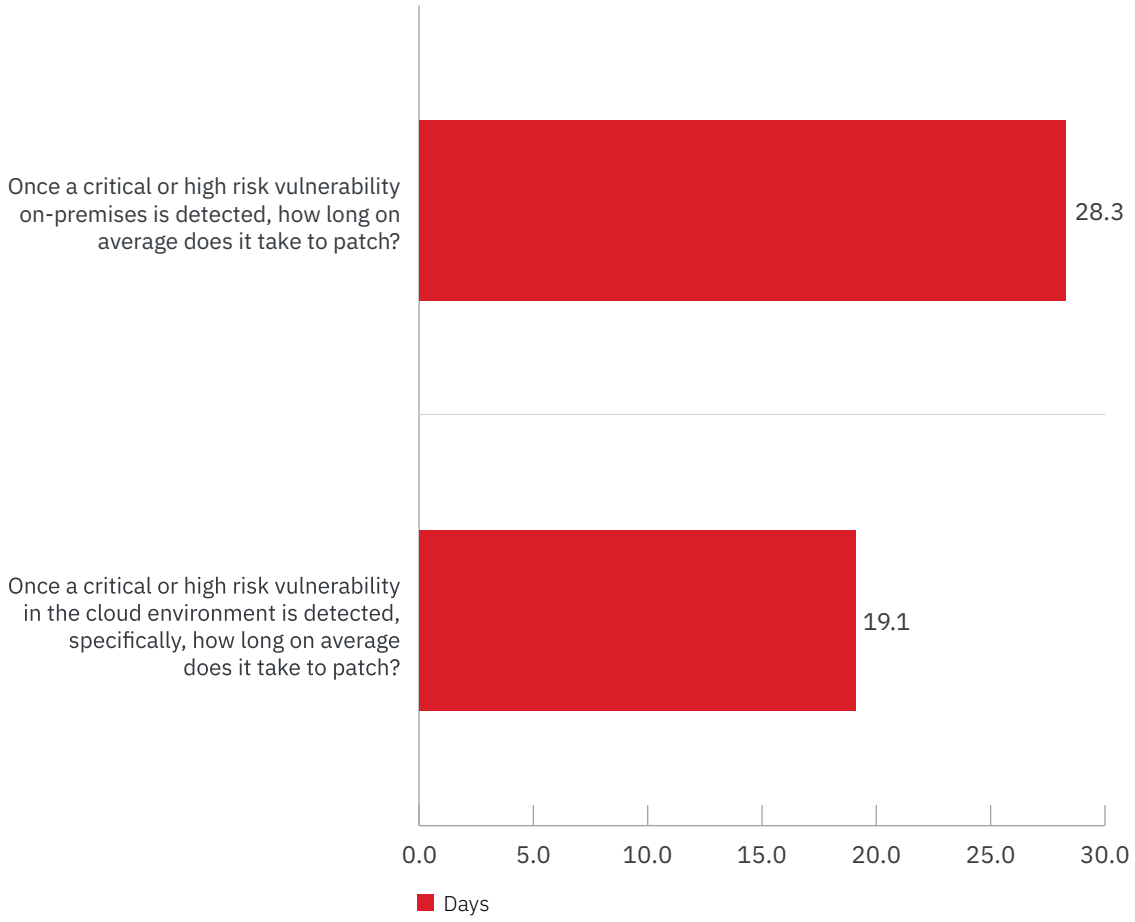


Slightly more false positives result from scanning the cloud environment. According to Figure 18, the average percentage of false positives that results from scanning the cloud environment is 31 percent, whereas scanning on-premises results in an average of 27 percent of false positives.

Figure 19:

Time to patch a critical or high-risk vulnerability in the cloud and on-premises

Extrapolated value (days) presented

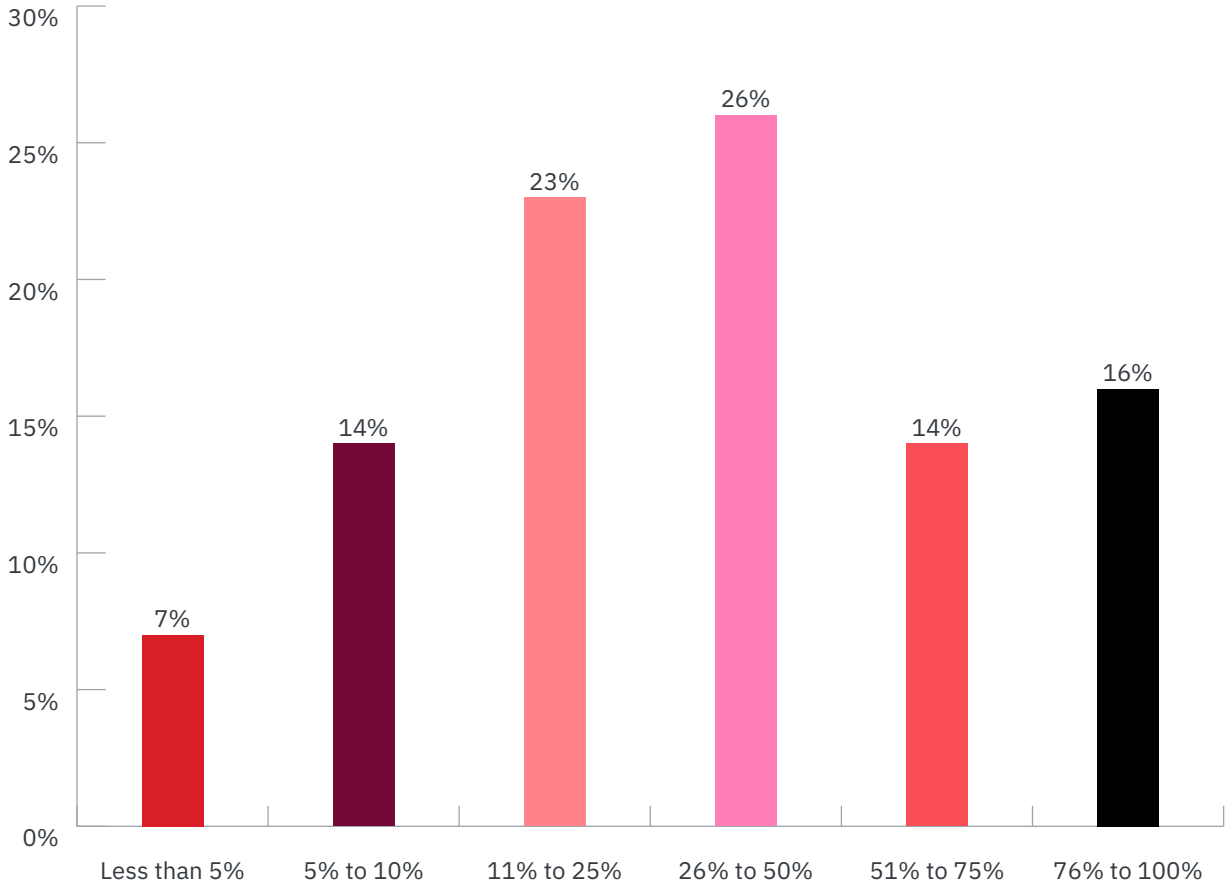


It takes longer to patch a critical or high-risk vulnerability on-premises. As shown in Figure 19, it can take an average of almost one month to patch a critical or high-risk vulnerability once it is detected on-premises, whereas in the cloud, it takes an average of 19 days.

Figure 20:

What percentage of your organization's applications considered business-critical are in containers?

Extrapolated value = 38 percent



Container security challenges

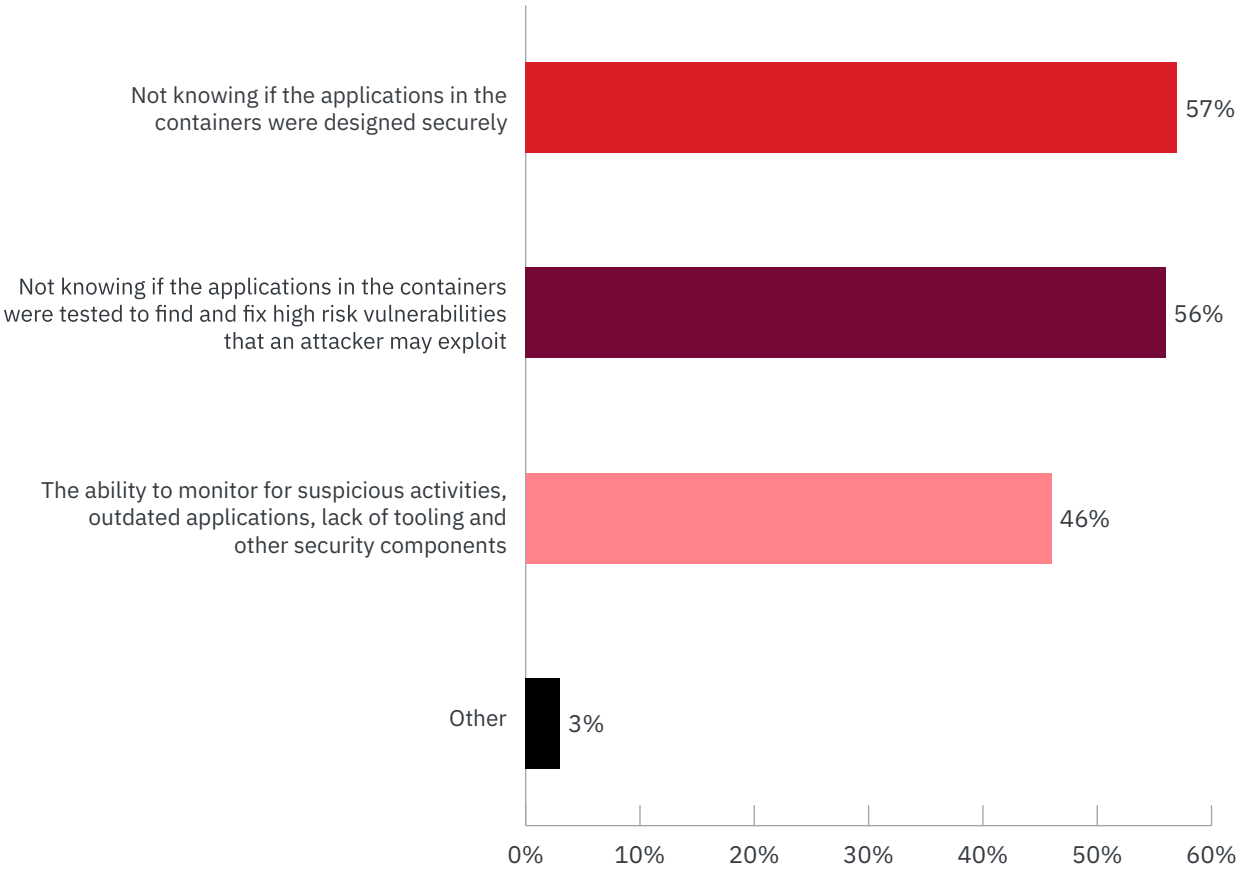
Organizations face challenges when storing business-critical applications in containers. In the context of this research, container security has a much different set of security challenges that differ from a traditional virtual machine (VM). In traditional virtualization—whether it be on-premises or in the cloud—a hypervisor is leveraged to virtualize physical hardware. Each VM then contains a guest OS, a virtual copy of the hardware that the OS requires to run, along with an application and its associated libraries and dependencies.

Instead of virtualizing the underlying hardware, containers virtualize the operating system (typically some base version of Linux) so each individual container contains only the application and its libraries and dependencies. The absence of the guest OS is why containers are so lightweight and, thus, fast and portable. However, the improved speed of building, sharing and deploying applications in containers can lead to vulnerabilities being introduced from obsolete vulnerable code or production host environments that have not been hardened.

Figure 21:

What challenges does your organization face in ensuring container security?

More than one response permitted

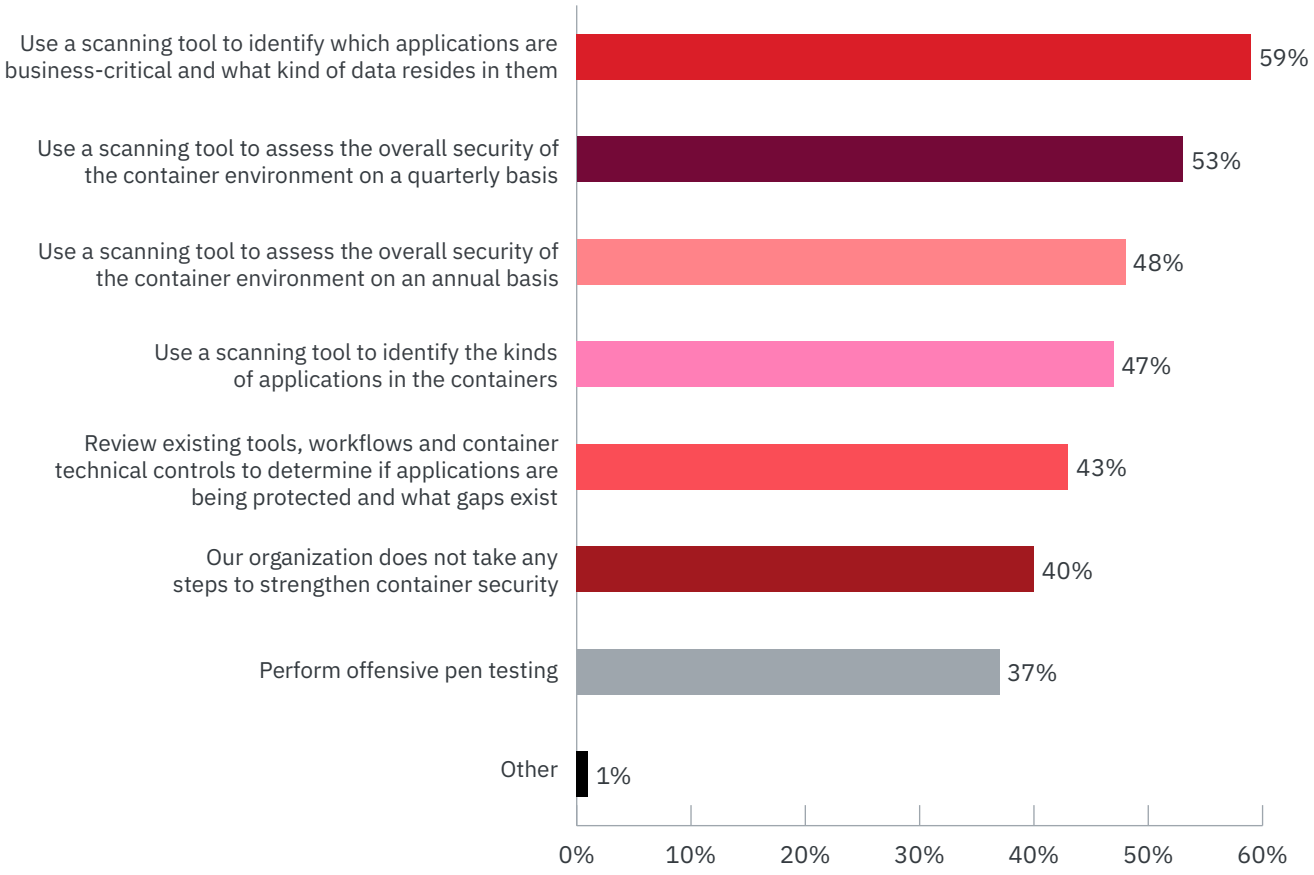


The majority of organizations are uncertain about the security of applications in containers and placed in the cloud. As discussed above, 34 percent of respondents say their organizations are using containers. Of those respondents, 57 percent say they do not know if the applications in the containers were designed securely and 56 percent say they are uncertain as to whether the applications were tested to find and fix high-risk vulnerabilities that an attacker may exploit, according to Figure 21.

Figure 22:

What steps does your organization take to strengthen container security?

More than one response permitted



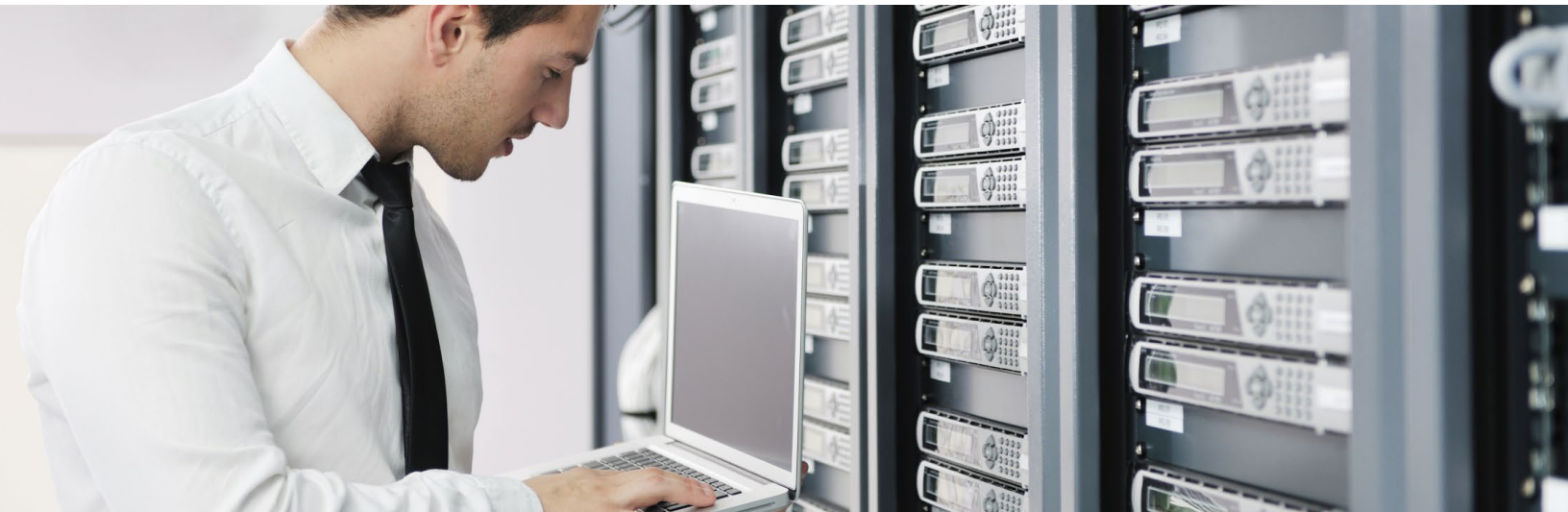
To overcome uncertainty about the security of applications, organizations primarily use scanning tools. Figure 22 presents a list of actions organizations can take to improve container security. Fifty-nine percent of respondents say their organizations use a scanning tool to identify which applications are business-critical and what kind of data resides in them and 53 percent of respondents say their organizations use a scanning tool to assess the overall security of the container environment on a quarterly basis.

Conclusion: The X-Force Red point of view

Based on what our X-Force Red team has experienced when testing and running vulnerability management programs for organizations worldwide, the findings in this report do not surprise us.

The data highlights consistencies our team has been seeing for the past couple of years. Many security teams continue to be overwhelmed by a backlog of vulnerabilities. Some manually try to prioritize them, which only widens the attack opportunity window, and then executing the remediation process can be a struggle. It is not enough to only identify vulnerabilities. Security teams need to tie in prioritization and remediation.

One of the most important findings is that 60 percent of respondents say that as a result of chasing down false positives and minor vulnerabilities, the most dangerous vulnerabilities continue to expose valuable assets. Most security leaders know false positives are a problem. The question they should be asking is “why?” We believe the issue revolves around how security teams are incentivized. In many organizations, security employees are assessed based on how many issues they have resolved. False positives tend to be the easiest ones to fix, so security teams make removing them the top priority. While removing false positives may clean up the report, it obviously does not make the organization more secure. It’s like buying a vowel in the game “Wheel of Fortune”; it may provide more clarity to solving the puzzle but will not earn you money. X-Force Red does not support that strategy.



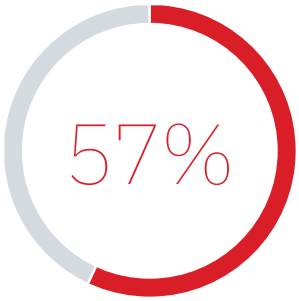
of respondents say that as a result of chasing down false positives and minor vulnerabilities, the most dangerous vulnerabilities continue to expose valuable assets.

The data also shows that instead of taking a programmatic approach to vulnerability management, many organizations take an anecdotal approach. They divvy up and plow through an Excel spreadsheet, which may contain thousands to millions of vulnerabilities. The spreadsheet method may work for one team in the organization, but when it's rolled out across an entire enterprise, chaos can ensue. Millions upon millions of vulnerabilities are piled on, as each team scrolls through the spreadsheet trying to understand which vulnerabilities pose the highest risk of a compromise and should fixed first. And even if they prioritize vulnerabilities accurately, the process of remediation can become a headache as teams try to process the information — who owns the vulnerable asset, is there a patch, what if the patch doesn't work, when is an appropriate time for patching, etc. etc. etc. To be effective, vulnerability management processes must be scalable and repeatable.

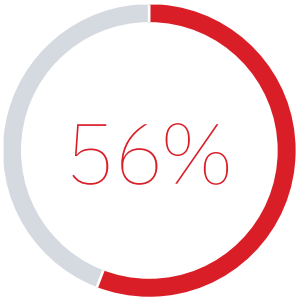
The cloud-related data in this report was also interesting, although not surprising. Organizations tend to have different teams and policies when it comes to cloud security versus on-premises security. Because the cloud footprint can expand so rapidly and have a different governance structure, the cloud security teams are drowning. Often, when applications are moved into the cloud environment, they do not receive the same level of attention — less frequent penetration testing, vulnerability scanning, etc.

Meanwhile, the on-premises applications may not have been glowing bastions of security to begin with. Applications that may have had security problems while on-premises are now moving to the cloud where there is even less oversight. The report reveals that the majority of organizations are uncertain about the security of applications and containers placed in the cloud with 57 percent of respondents saying they don't know if applications in containers are designed securely, and 56 percent of respondents saying they are uncertain if the applications in containers were tested to find and fix high-risk vulnerabilities.

Programmatic testing of cloud-based applications results in more visibility into design-related and other application vulnerabilities. If organizations deploy an ongoing vulnerability management program for their cloud environment, which includes scanning, prioritization, and a repeatable remediation process, they will continuously understand the security posture of their applications and minimize the risk of a compromise.



of respondents say they don't know if applications in containers are designed securely.



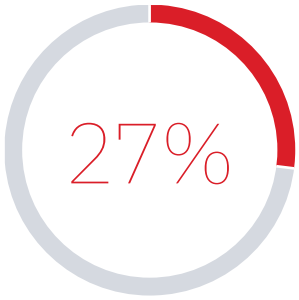
of respondents say they are uncertain if the applications in containers were tested to find and fix high-risk vulnerabilities.

We cannot overlook one more statistic, which speaks to why we built our Red Portal. Only 27 percent of respondents say they have visibility into the vulnerability management lifecycle, which makes it difficult to ascertain how well their organizations are prioritizing and patching vulnerabilities. Every enterprise has an immense amount of data, much of which is siloed, giving each team a different perspective of risk. The fragmented viewpoints prevent seeing the full risk picture, which can also lead to important vulnerabilities being deprioritized or overlooked.

We built our Red Portal to help organizations overcome this challenge. The portal can serve as a clearing house for vulnerability data. It ingests and enriches data from the entire organization and provides remediation recommendations, documentation of risk reduction, and a single view of the vulnerabilities that matter most.

X-Force Red offers penetration testing, adversary simulation, and vulnerability management services for on-premises and cloud environments.

Learn more about X-Force Red Offensive Security Services.



of respondents say they have visibility into the vulnerability management lifecycle.

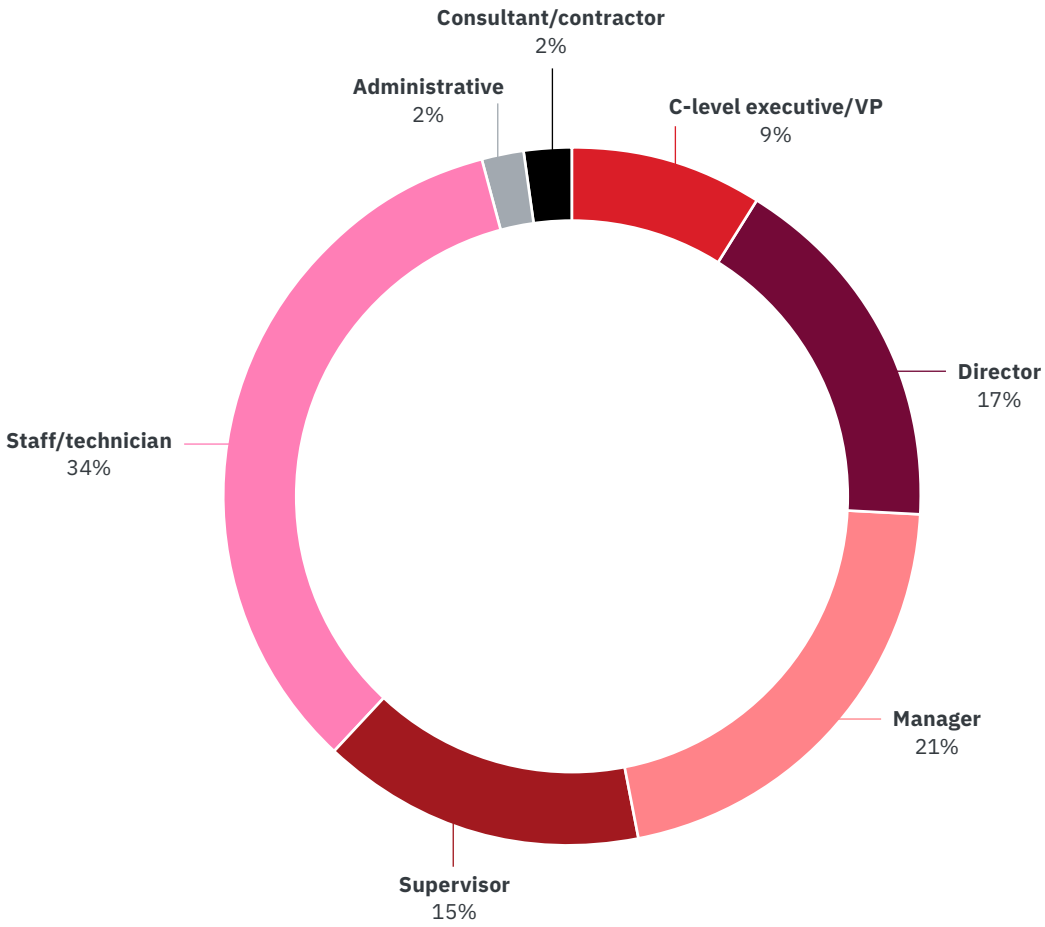
Methods

A sampling frame of 50,068 IT and IT security professionals in North America, EMEA, Asia-Pac and Latin America were selected as participants in this survey. Table 1 shows 2,051 total returns. Screening and reliability checks required the removal of 203 surveys. Our final sample consisted of 1,848 surveys, or a 3.7 percent response rate.

Table 1. Sample response	FY2020	Pct%
Sampling frame	50,068	100.0%
Total returns	2,051	4.1%
Rejected or screened surveys	203	0.4%
Final sample	1,848	3.7%

Pie Chart 1:

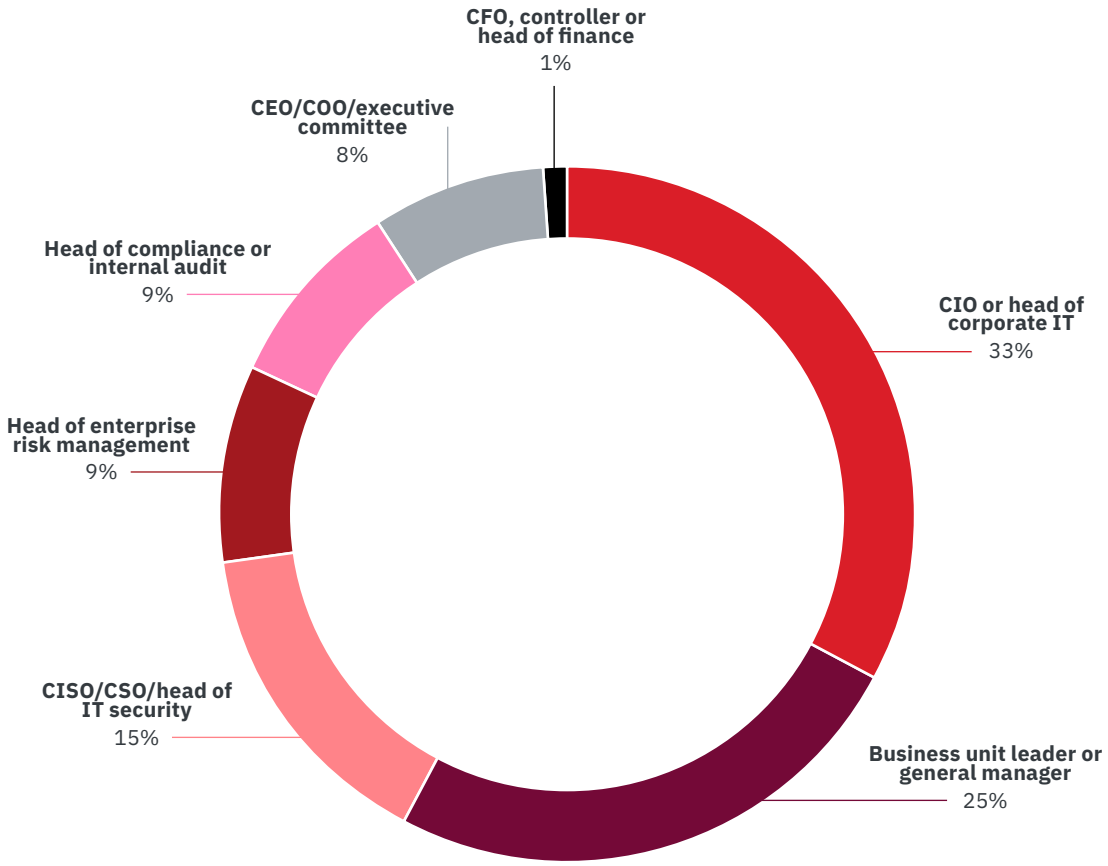
Position level of respondents



The following pie chart summarizes the position level of qualified respondents. At 34 percent, the largest segment contains those who are rank-and-file level employees (e.g., staff/technicians). More than half (62 percent) of respondents are at or above the supervisory level.

Pie Chart 2:

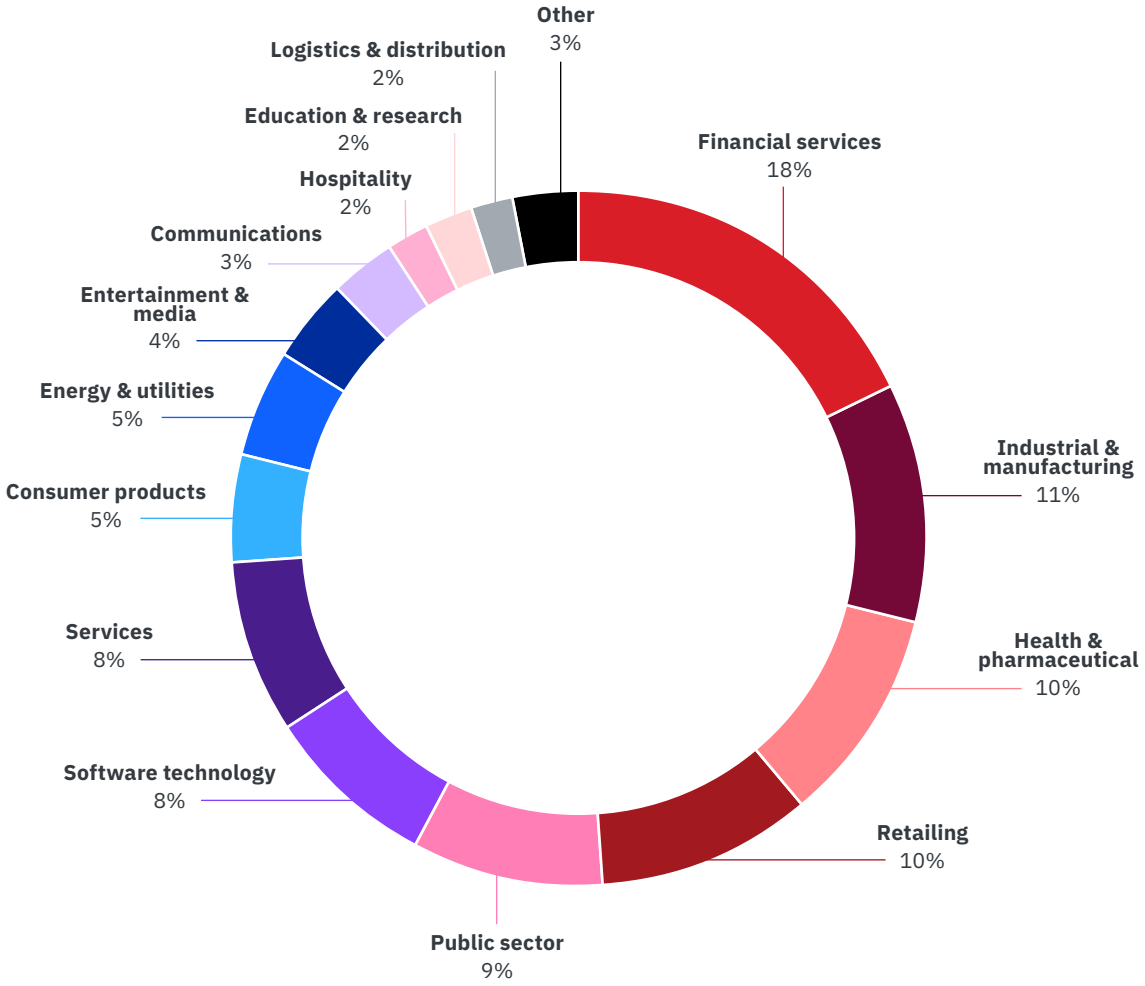
Primary person you or your leader reports to



As shown in Pie Chart 2, 33 percent of respondents report to the CIO or head of corporate IT, 25 percent of respondents report to the business unit leader or general manager, and 15 percent of respondents indicated they report to the CISO/CSO/head of IT security.

Pie Chart 3:

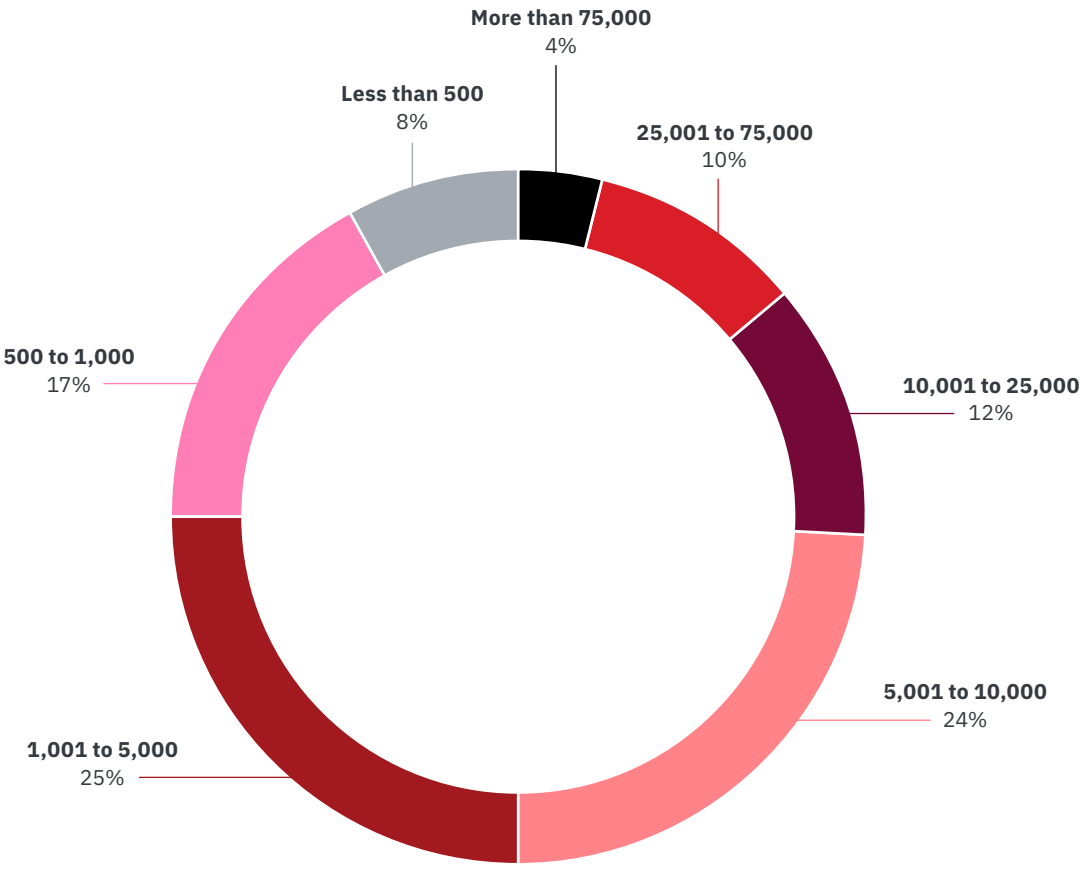
Primary industry focus of respondents' companies



Pie Chart 3 shows the percentage distribution of respondents' companies across 14 industries. Financial services represent the largest industry sector (at 18 percent of respondents), which includes banking, insurance, brokerage, investment management and payment processing. This is followed by industrial and manufacturing (11 percent of respondents), health and pharmaceuticals (10 percent of respondents), and retailing (10 percent of respondents).

Pie Chart 4:

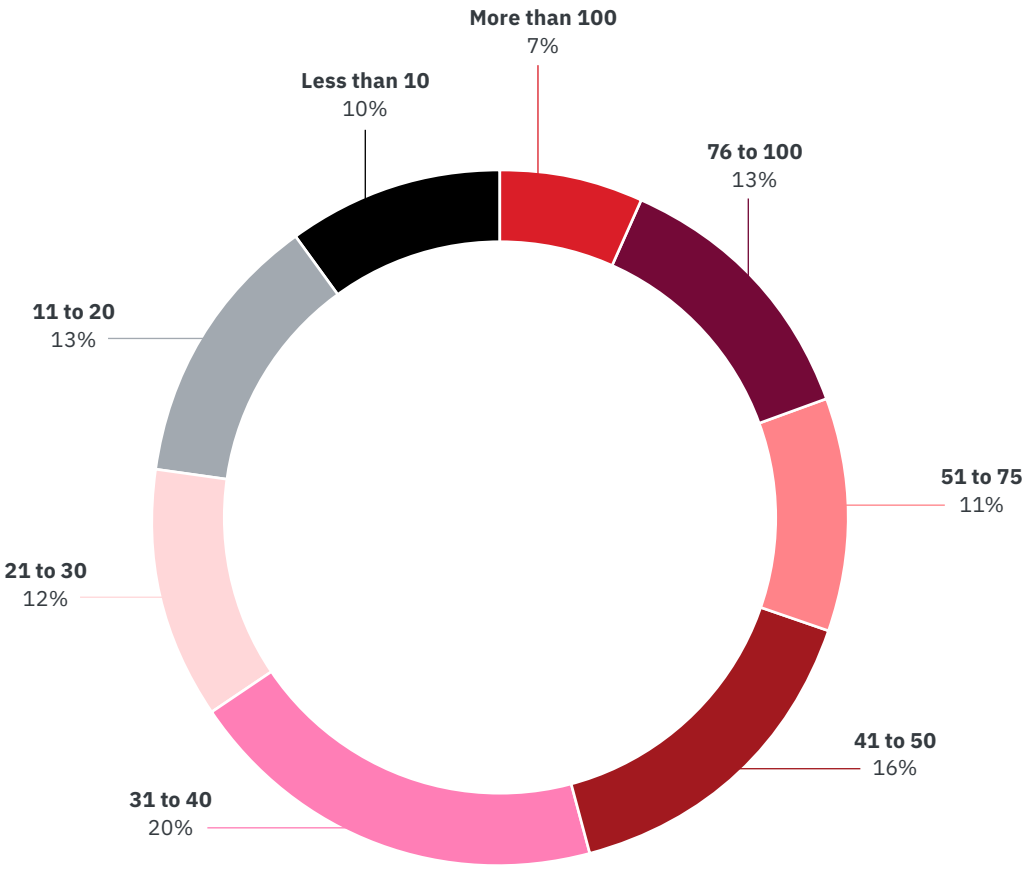
Global headcount of respondents' organization



Pie Chart 4 summarizes the total worldwide headcount of respondents' companies. In the context of this study, headcount serves as an indicator of size. At 25 percent, the largest segment contains organizations with 1,001 to 5,000 full-time equivalent employees. The smallest segment (4 percent) includes larger-sized organizations with 75,000 or more employees. Half of respondents are from organizations with a global headcount greater than 5,000 employees.

Pie Chart 5:

Full-time headcount of your IT security function



Pie Chart 5 summarizes the full-time headcount of the IT security function. At 20 percent, the largest segment contains between 31 and 40 full-time employees. More than half (67 percent) of respondents indicated there are more than 30 full-time employees within the IT security function.

Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security professionals. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2020