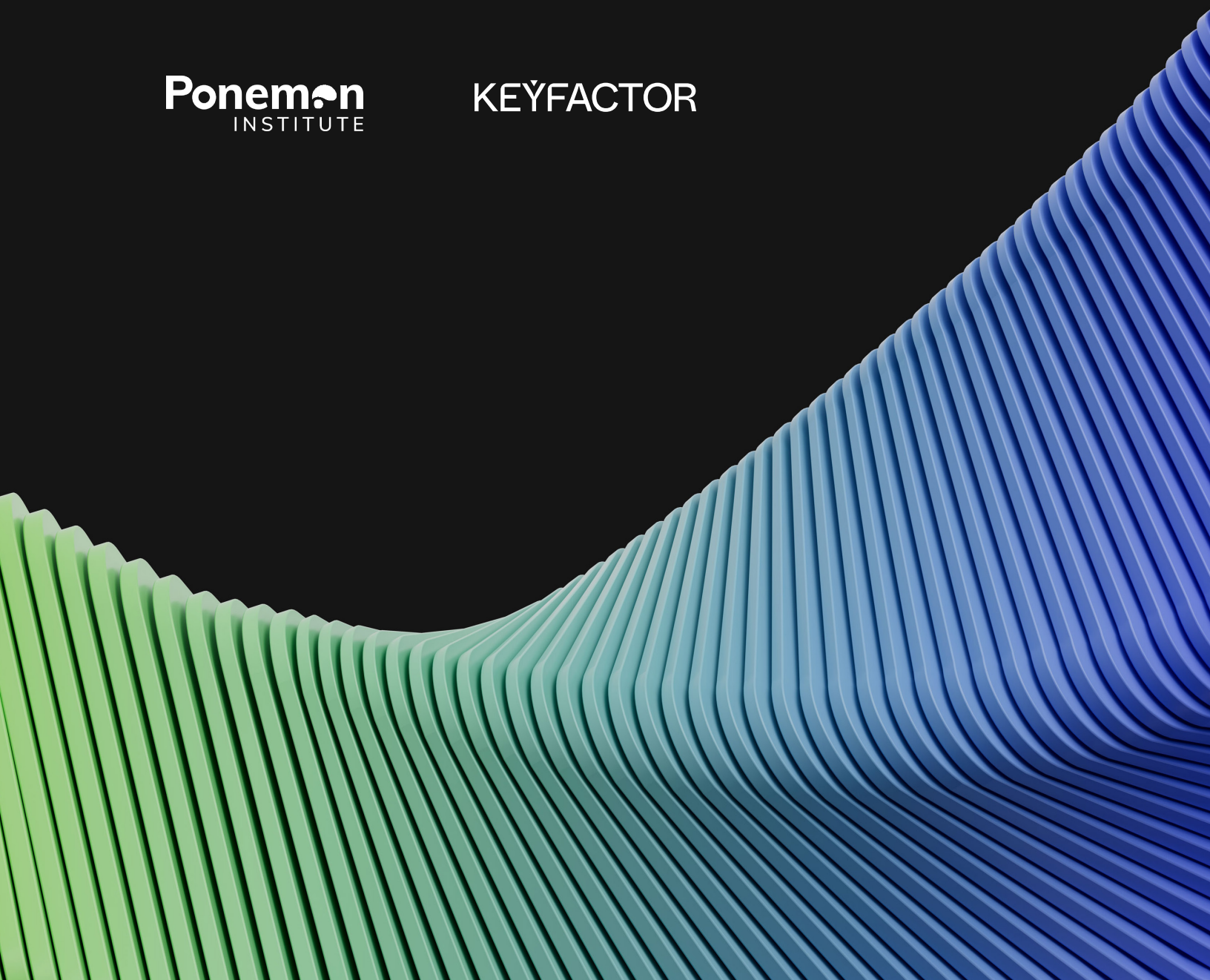
State of Machine Identity Management 2023

Ponemon INSTITUTE

KEYFACTOR



Foreword

The challenges of identity and access management (IAM) continue to grow. The ongoing evolution in the workplace – employees working remotely, high turnover rates, and economic pressures still in place as the pandemic eases – creates a turbulent environment for those tasked with IAM.

One response has been the continued rapid growth of machines as part of the workforce. This has resulted in more servers, IoT devices, containers, applications, and end-user devices as organizations scramble to improve customer responsiveness while improving efficiency.

Last year I observed that the forces driving this growth of the machine workforce were only going to accelerate. I am not prescient; the trends are very clear.

Yet as these organizations incorporate machines into their ecosystems, identifying and providing them with an identity (and then managing it) has become more difficult. More than 60% of respondents to our third annual State of Machine Identity Management Report with the Ponemon Institute said they do not know how many keys and certificates they have – which is 7% more than last year. The embrace of zero trust, whether in a government agency or a corporation, the increased use of IoT devices, and the adoption of cloud-based services are all driving the deployment of keys, PKI, and certificates.

As a result, finding ways to get a handle on the challenge and reducing the complexity of the PKI environment is one of this year's top priorities.

And new challenges are arising. Concerns about a post-quantum world, where quantum computers hold the potential for being able to break current cryptographic algorithms, are increasing, and the understanding that most cryptographic providers will need to migrate to new quantum-resistant ones is driving organizations to rethink PKI and invest in certificate management to address these concerns.

These are just a few of the findings in this year's report. It makes clear that the IAM landscape is continuing to change rapidly, and organizations are struggling to keep up with those changes.

But there are signs of progress. More organizations than ever understand the importance of having an overall MIM strategy that can be applied across their enterprises. Included in that is a recognition of the importance of visibility into PKI use and distribution and an inventory of all assets.

The 2023 State of Machine Identity Management Report reflects many of the day-to-day experiences Keyfactor encounters in engaging security leaders, developers, and engineers to identify organizational obstacles to effective identity management – for both humans and machines. It also illuminates the challenges and possible solutions organizations of all sizes are experiencing. We hope you find it as enlightening and helpful as we find the exciting work and research we are conducting in this field.

Chris Hickman
Chief Security Officer (CSO)

Contents

Executive summary

Introduction

Welcome to the third annual State of Machine Identity Management report, an in-depth look at the role of PKI and machine identities in establishing digital trust and securing modern enterprises.

Within the overarching domain of identity and access management (IAM), machine identity management (MIM) focuses on managing device and workload identities, such as X.509 certificates, SSH credentials, code signing keys, and encryption keys.

In this report, we explore findings from a survey independently conducted by the Ponemon Institute and published by Keyfactor, the identity-first security solution for modern enterprises. The report provides insights into how organizations are deploying and managing PKI and machine identities and what challenges and risks are top of mind as the role of PKI and machine identities continues to evolve and become more complex.

This year, we analyzed survey responses from 1,280 individuals across North America, Europe, the Middle East, and Africa (EMEA). Survey respondents work in all areas of the IT organization, from information security to infrastructure, operations, and development.

The findings from this year's survey show that an effective machine identity management strategy is critical to keeping track of all machines to ensure each one has appropriate access permission. As shown in this research, responsibility for deploying and managing PKI is dispersed throughout organizations. One of the consequences of no clear ownership is that less than half (47 percent) of organizations have an enterprise-wide strategy for managing PKI and machine identities. Only 31 percent of respondents say their organizations have a mature machine identity working group.

1,280
Survey respondents

12
Industries

2
Global regions

The results of this year's survey show that zero-trust strategies, IoT devices, and cloud-based services are driving further use of PKI, keys, and digital certificates in the enterprise. However, shorter certificate lifecycles have made it much more difficult to keep pace with certificate issuance and management. Moreover, 53 percent of respondents say their organizations do not have enough staff and resources dedicated to their PKI deployment. In short, this growth is leading to significant challenges and most organizations do not have enough team members to keep pace with the change and the challenges presented by today's enterprise PKI infrastructure.

A prominent theme throughout the research is the growing need to reduce the complexity of PKI infrastructure. For the first time, the top strategic priority for digital security in organizations is reducing complexity in their PKI infrastructure, an increase from 50 percent in 2021 to 58 percent this year. Seventy-four percent of respondents, an increase from 61 percent in 2021, say their organizations are deploying more cryptographic keys and digital certificates. As a result, this has significantly increased the operational burden on their organizations' teams, according to 72 percent of respondents, up from 62 percent in 2021. A key takeaway from this year's report is that complexity is increasingly recognized as the enemy of a secure PKI infrastructure and makes organizations vulnerable to data breaches. Contributing to complexity is the exponential increase in the number and variety of machines with different keys and certificates required.

The ongoing evolution in the workplace – employees working remotely, high turnover rates, and economic pressures still in place as the pandemic eases – creates a turbulent environment for those tasked with IAM.

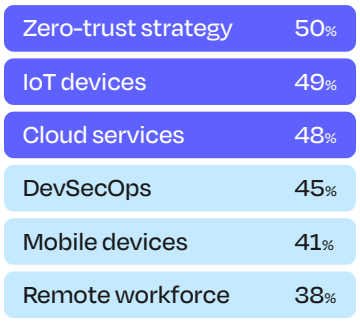
Key findings

The key findings described here are based on Keyfactor's analysis of the research data compiled by the Ponemon Institute.

PKI for IoT and DevOps is on the rise

WFH trend declines post-pandemic

PKI continues to be a critical component in zero-trust strategy and cloud security. However, there's been a notable increase in usage of PKI to secure emerging DevSecOps and IoT environments, with the number of respondents indicating IoT as a top trend increasing from 43 percent in 2021 to 49 percent in 2023. DevSecOps similarly increased in importance, with 40 percent of respondents saying it is a top use case in 2021 compared to 45 percent this year.



Skills shortage is getting worse

PKI experts are hard to find and retain

CISOs and security teams are grappling with a labor shortage, and it's taking a toll on PKI and machine identity strategy. In fact, respondents say that lack of skilled personnel and too much change and uncertainty are the two biggest challenges facing their teams today. It's not just impacting strategy, though, with 53 percent of respondents saying they don't even have enough staff to deploy and maintain their PKI effectively, up from 50 percent in 2022.

▲53%

Say they don't have enough staff to deploy and maintain their PKI

Decentralized PKI is the new norm

CA sprawl is a serious challenge

PKI is everywhere, with different teams leveraging different tools to issue certificates – from internal CAs and self-signed certificates to cloud-based PKI and CAs built into DevOps tooling. On average, respondents estimate they have 9 different CA and PKI solutions in use across the organization. Unsurprisingly, reducing complexity in PKI infrastructure became the top strategic priority for machine ID management in 2023, as teams struggle to regain control and prevent the sprawl of non-compliant and untrusted CAs.

9

Average number of different PKI and certificate authority (CA) solutions used within organizations

▲256k

Average number of internally trusted certificates within organizations

More certificates, more problems

If you can't manage them

For the third consecutive year, the average number of internally trusted certificates (i.e., certificates issued from an internal private PKI) increased significantly, from 231,063 in 2021 to 255,738 in 2023. With more certificates, teams responsible for PKI are struggling to maintain visibility and control. Sixty-two percent of respondents say they don't know exactly how many keys and certificates they have, up from 53 percent of respondents in 2021.

77%

Say their organization experienced at least two significant outages caused by expired certificates in the past 24 months

Outages are hitting organizations hard

What happens when certs expire unexpectedly

If left untracked or ignored, certificates expire unexpectedly, causing applications and services to stop working. Most respondents (77 percent) report experiencing at least two of these incidents in the past 24 months. Certificate-related outages aren't a trivial incident, with 55 percent of respondents saying these outages caused severe disruption to customer-facing services. Another 50 percent say these events caused major disruption to internal users or a subset of customers.

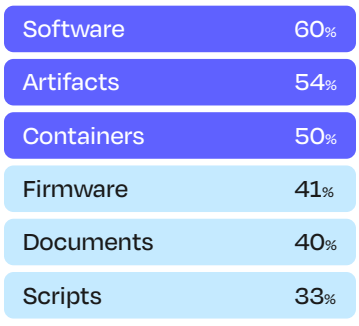
3.79hrs

The average time it takes teams to identify, remediate, and recover from certificate-related outages

Time to recovery (TTR) is slow

Without visibility or automation

So, what happens when an outage strikes? According to respondents, it takes an average of nearly 4 hours to identify and remediate a certificate outage, which involves identifying the root cause, finding the expired certificate, then re-issuing and provisioning it to all affected services. Respondents say an average of 11 staff are directly involved in remediating these outages when they occur, pulling them away from priorities and into incident response tasks.



Code signing usage is expanding

Not just for software anymore

The definition of "code" is changing. As teams shift to developer-driven, software-defined infrastructure, they are signing more than just software deliverables. According to respondents, use cases for signing range from software and firmware to artifacts, scripts, and containers. Virtually every company is signing software in some shape or form, but responses are based on each respondent's individual perspective.

▲68%

Say their organization stores code-signing keys within an HSM

Code signing keys are vulnerable

But security practices are improving

Recent incidents involving the theft and abuse of code signing keys highlight the need to protect them against would-be attackers. Unfortunately, more than half of respondents (56 percent) say they are not confident in their ability to protect keys against theft or misuse. While many organizations still store sensitive keys on build servers or workstations, where they are vulnerable to attack, 68 percent of respondents say they have adopted best practice use of an HSM to generate and store keys, an increase of 17 percent since 2021.

Only

▼22%

Say lack of executive-level support is a serious challenge

Executives are paying attention

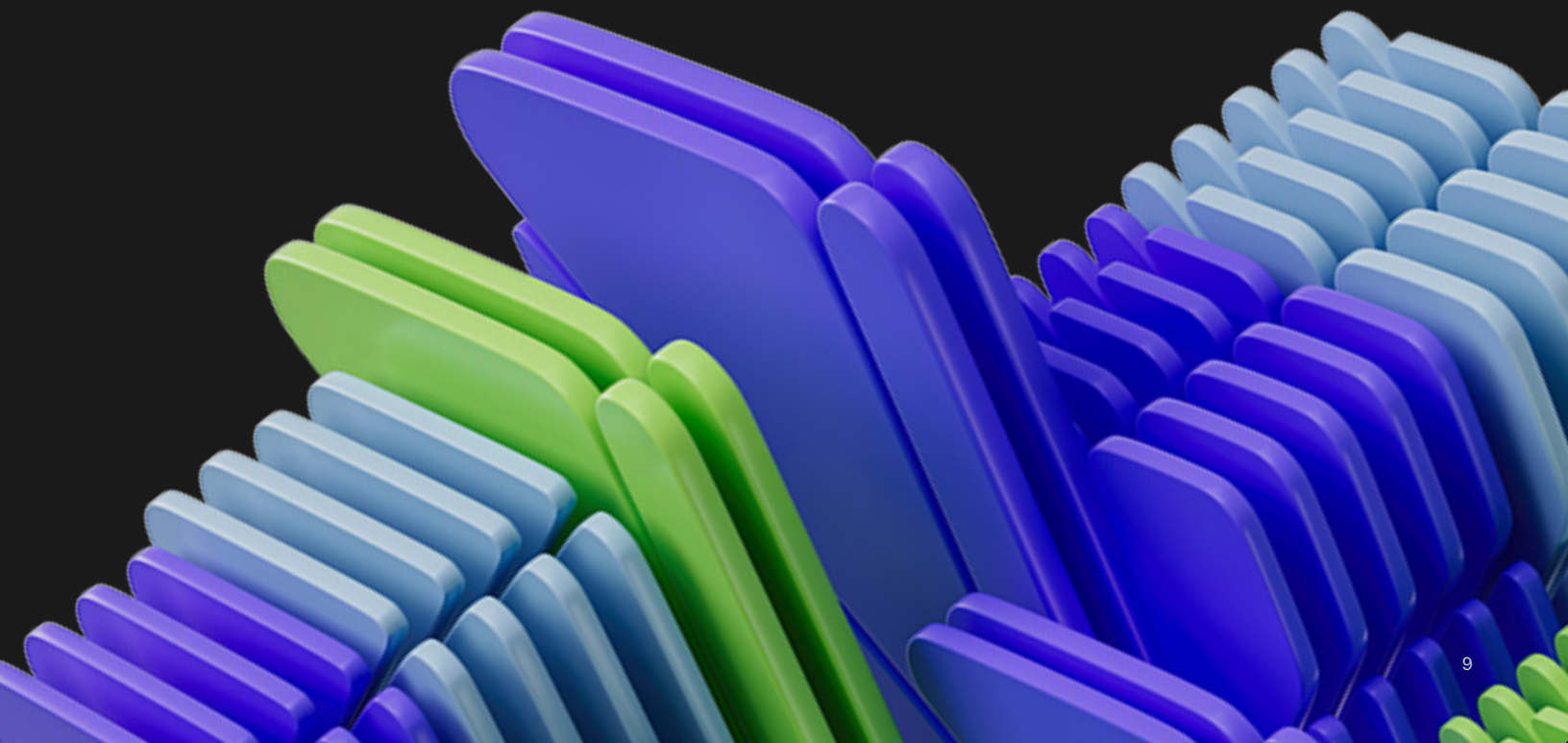
Machine identity isn't just a tech problem

Without support from the C-level, priorities will always fall elsewhere. The good news is that only 22 percent of respondents say lack of executive support was a serious issue in setting an enterprise strategy for PKI and machine identity management, down significantly from 36 percent of respondents in 2021. Bottom line is, executive awareness is growing around the need to invest in the right tools, people, and processes for machine identity management.

Complete findings

In this section, we analyze the complete findings of the research. We have organized the topics in the following order:

1. Strategies and trends in PKI and machine identity management
2. PKI and certificate management practices
3. Code signing practices
4. SSH identity management practices
5. The impact of outages, key misuse, and failed audits



Strategies and trends in PKI and machine identity management

Machine identity management is gaining traction, but organizational hurdles stand in the way. As shown in Figure 1, 47 percent of respondents say they have an overall strategy for managing PKI and machine identities, such as keys, certificates, and secrets, an increase from 40 percent in 2021.

Machine identities, as opposed to human or user identities, are becoming an increasingly important piece of the identity and access management (IAM) landscape. However, Figure 2 shows that it's still unclear who owns identity and access management (IAM) strategy, never mind where machine identities fit in.

Figure 1

Does your organization have an enterprise-wide strategy for managing PKI and machine identities?

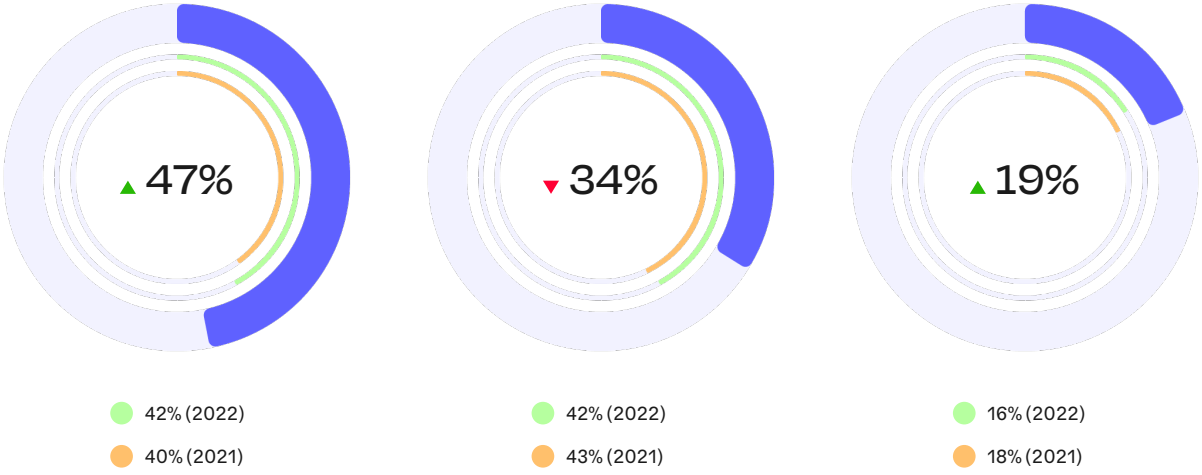
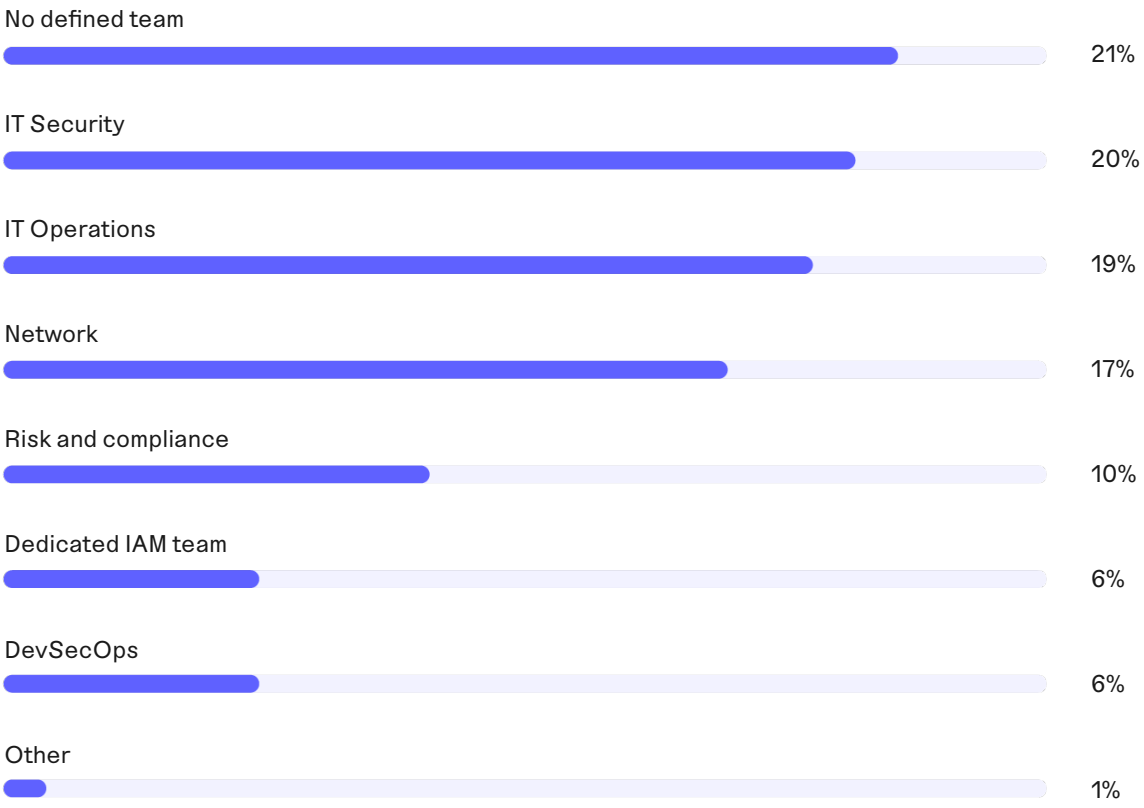


Figure 2

Who is responsible for Identity and Access Management (IAM) within your organization?

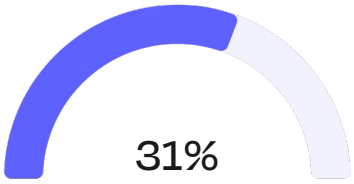


A machine identity working group could be the solution. If a developer or engineer asks how to attain a certificate as they deploy a new service, who do they consult with? The answer is they need insight from several teams to gather the right information and make the right decisions, which could include PKI, I&O, DevOps, and IAM. Bottom line, it requires cross-functional collaboration.

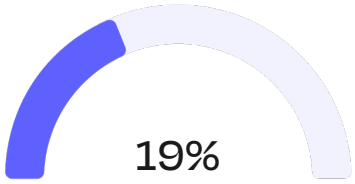
Once formed, a cross-functional machine identity working group can define guidelines and best practices for issuing and managing certificates and other machine IDs, making tooling decisions, and setting clear policies. As seen in Figure 3, 50 percent of respondents say their organization has an established machine identity working group at varying levels of maturity.

Figure 3

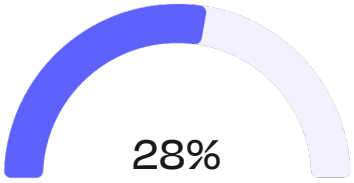
Does your organization have a team or working group dedicated to PKI and machine identity management?



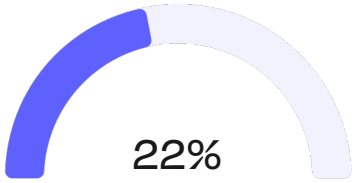
Yes, we have a mature machine identity working group that provides leadership, research, implementation, strategy, ownership and best practices



Yes, but our machine identity working group is still immature



No, but we plan on implementing a machine identity team or working group within the next 6 months



No, and we do not have plans to implement a machine identity team or working group

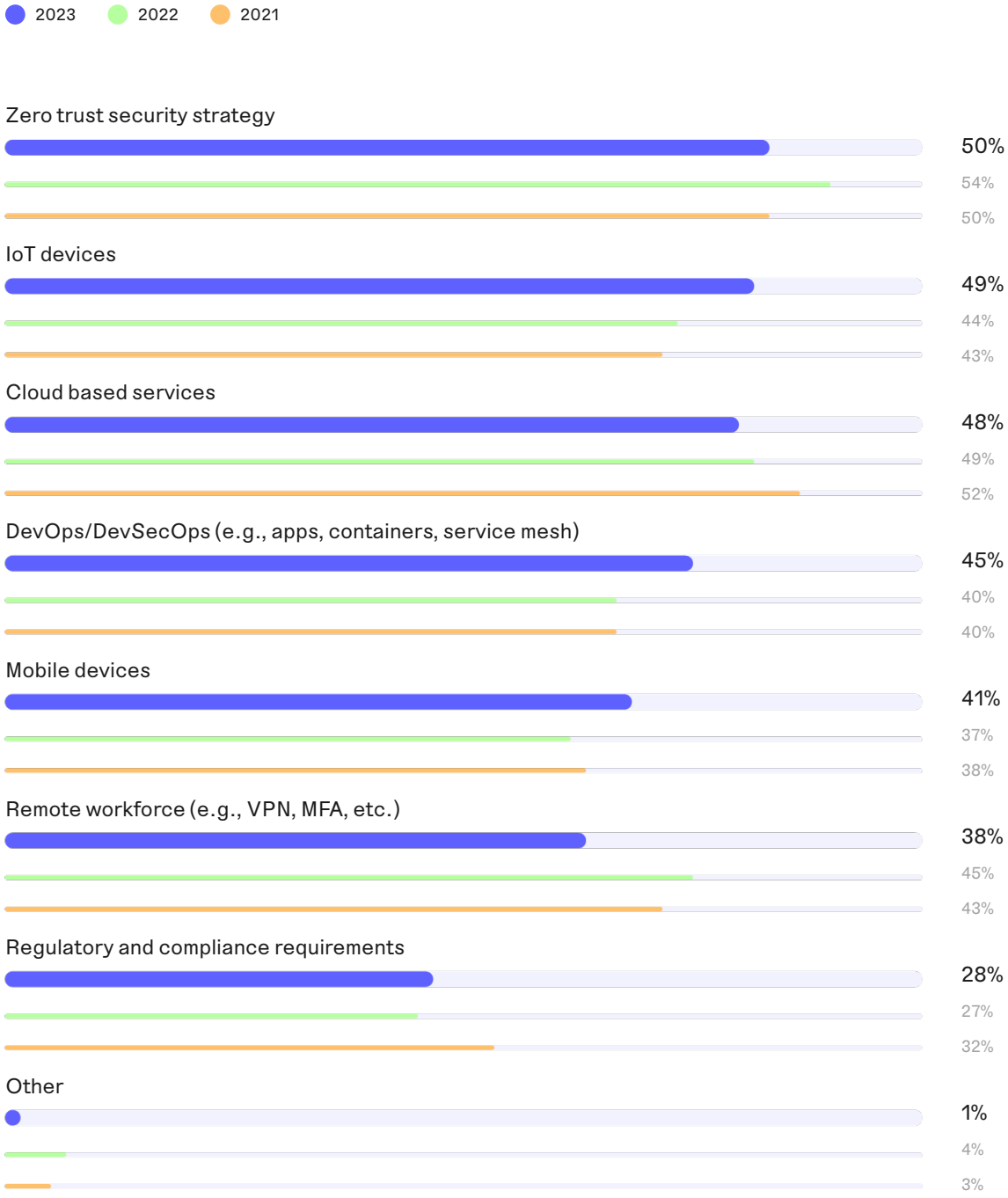
IoT and DevOps are the fastest-growing use cases for PKI and machine IDs. Figure 4 shows the most important trends driving the deployment of PKI, keys, certificates, and other secrets. Zero trust strategy and cloud-based services remain top trends for PKI, consistent with results from previous years.

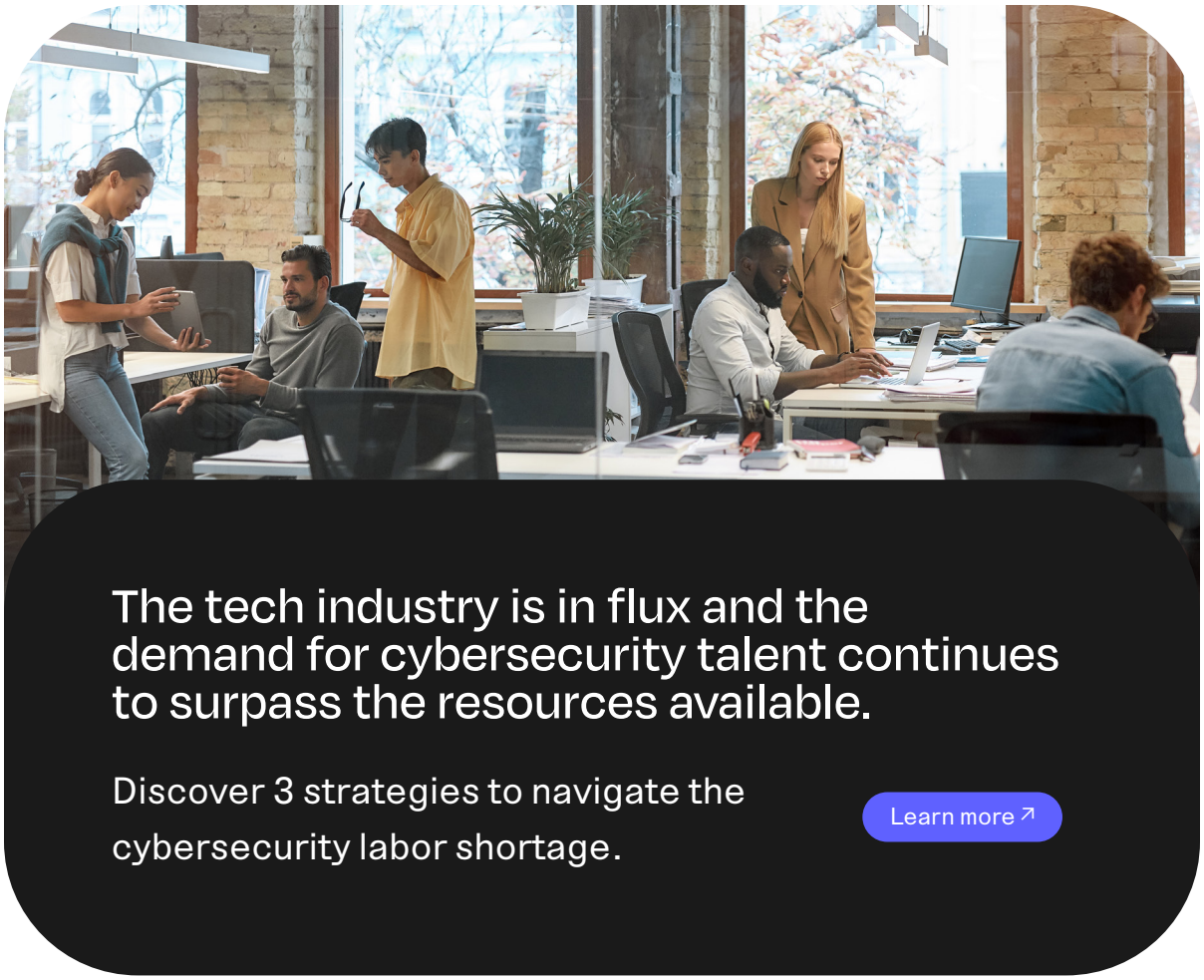
IoT devices (49 percent of respondents) and DevOps/DevSecOps (45 percent of respondents) represent the fastest-growing trends, up from 43 percent and 40 percent of respondents in 2021, respectively. Conversely, the importance of the remote workforce has decreased from 43 percent of respondents in 2021 to 38 percent of respondents in this year's report, likely due to a post-pandemic shift in priorities.

Figure 4

The most important trends and use cases driving deployment of PKI, keys, certificates, and other secrets

Three responses permitted





Skills shortage and uncertainty are still the top challenges facing teams; fragmented tools are becoming a bigger problem. Figure 5 provides a list of six challenges involved in setting an enterprise-wide strategy for PKI and machine identity management. We asked respondents to indicate the top two challenges facing their organization.

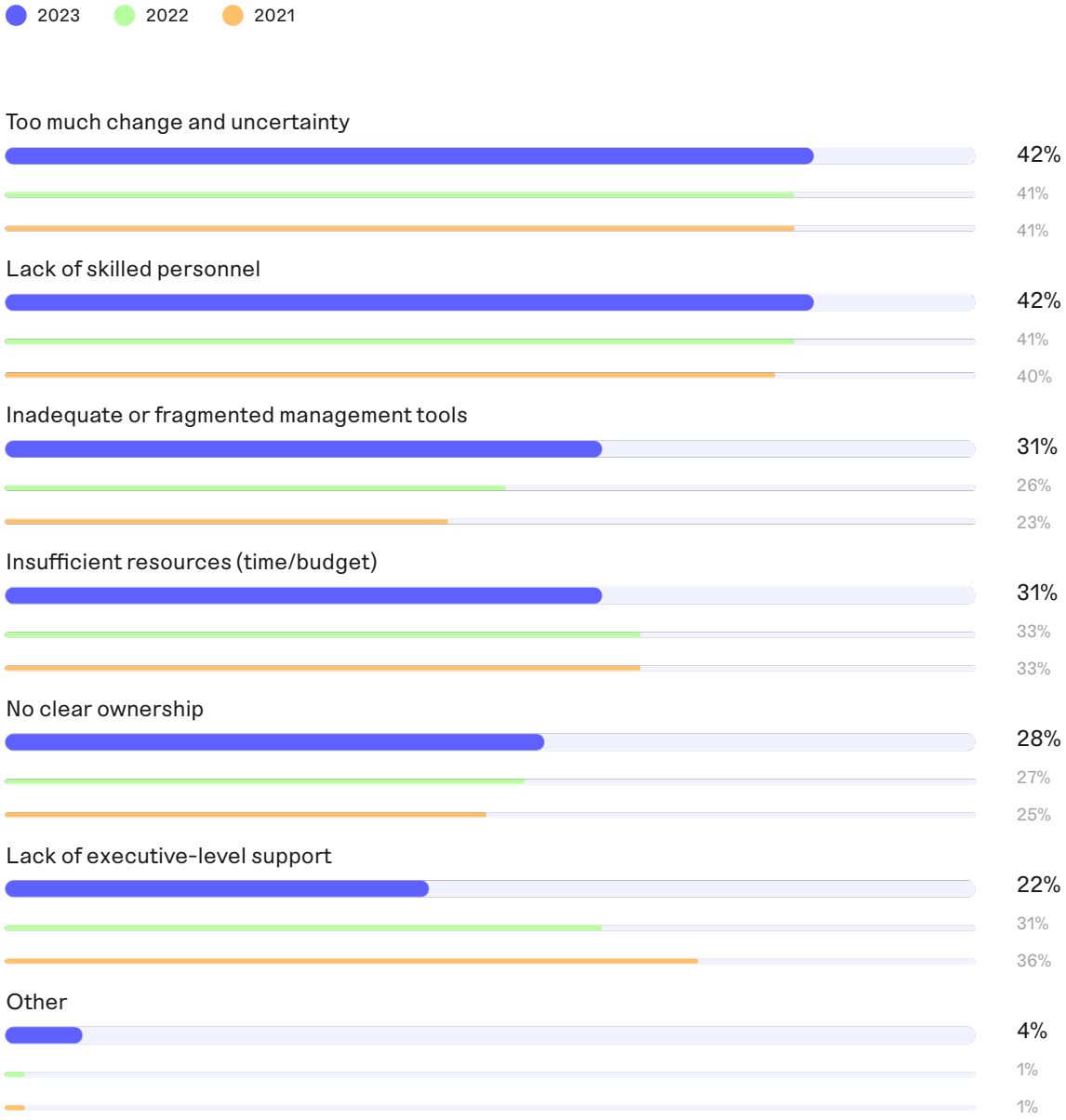
Forty-two percent of respondents say that a lack of skilled personnel and too much change and uncertainty are top challenges, consistent with previous years. However, there is a notable increase in respondents that say inadequate and fragmented management tools are a top challenge, increasing from 23 percent of respondents in 2021 to 31 percent of respondents in this year's report.

On a positive note, it appears executives are becoming more aware and supportive of the need for machine identity management, with only 22 percent of respondents saying lack of executive-level support is a top challenge, compared with 36 percent of respondents in 2021.

Figure 5

Biggest challenges involved in setting enterprise-wide strategy for PKI and machine identity management

Two responses permitted



More certificates create more problems, if organizations can't track or manage them effectively. As shown in Figure 6, 72 percent of respondents say the increasing use of key and certificates has significantly increased their operational burden, up from 62 percent of respondents in 2021.

As the volume of certificates within organizations increases, visibility also becomes a serious challenge. Sixty two percent of respondents say they don't know exactly how many keys and certificates (including self-signed) their organization has, compared to 53 percent of respondents in 2021. Misconfiguration of keys and certificates is also an increasing concern.

In June 2022, NIST chose the first group of algorithms to become part of its post-quantum cryptographic standard, expected to be finalized within two years. Forty-eight percent of respondents say they are concerned about their ability to adapt to these post-quantum algorithms, up from 44 percent last year, before the NIST announcement.

Figure 6

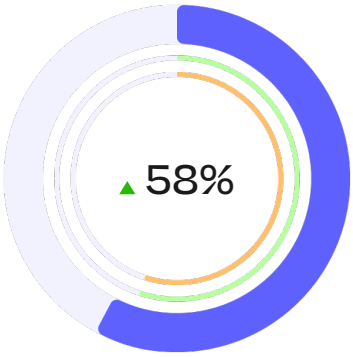
Perceptions and concerns about managing machine identities

Strongly agree and agree responses combined

Increasing use of keys and certificates has significantly increased operational burden on my organization's teams

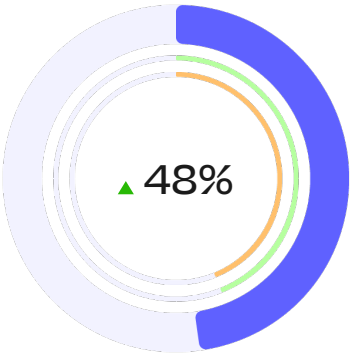
My organization does not know exactly how many keys and certificates (including self-signed) it has

Figure 6 Cont.



55% (2022)
55% (2021)

Misconfiguration of keys and certificates is an increasing concern in my organization



44% (2022)
44% (2021)

My organization is concerned about the ability to adapt to changes in cryptography (i.e. post-quantum algorithms)

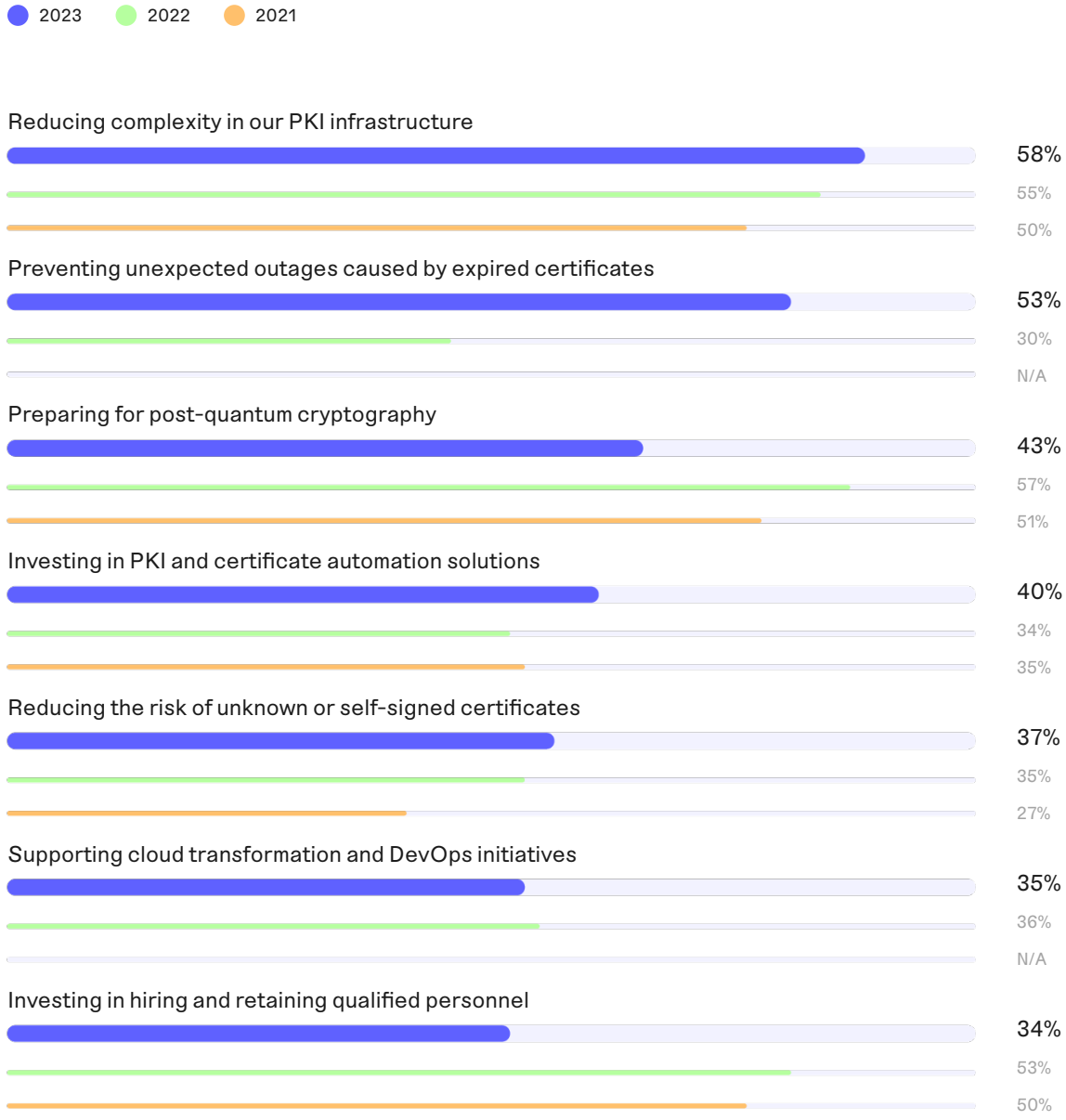
Reducing PKI complexity, preventing certificate-related outages, and preparing for post-quantum cryptography top the list of strategic priorities. Figure 7 provides a list of seven strategic priorities for machine identity management. We asked respondents to indicate the top three priorities.

As organizations increasingly rely on PKI and digital certificates to authenticate workloads and devices, it's clear that teams are struggling to maintain visibility and control. Unsurprisingly, respondents say their top priorities are to reduce complexity in PKI infrastructure (58 percent) and prevent outages caused by expired certificates (53 percent). Forty-three percent of respondents say preparing for post-quantum cryptography is also a top priority.

Figure 7

Strategic priorities for PKI and machine identity management in 2023

Three responses permitted



*Note: additional response options were included in the 2022 and 2023 survey

PKI and certificate management practices

Decentralized PKI is the new normal. According to respondents, there are an average of 9 different certificate authorities (CA) and PKIs being used within organizations.

As seen in Figure 9, respondents say that their PKI commonly includes a mix of internal private PKI (50 percent), CAs built into DevOps tools (35 percent), self-signed certificates (33 percent), managed PKI services (33 percent), private CA services in the cloud (31 percent), as well as public CA services (25 percent).

Gone are the days of one or two CAs behind the four walls of the datacenter. Today, different teams are using multiple CA and PKI deployments to support various levels of trust, use cases, and requirements for security and performance. While necessary, this results in new risks and challenges as PKI becomes more fragmented and complex, creating the need for control and consolidation, wherever possible.

Figure 8

How many different PKIs and Certificate Authorities (CAs) are in use within your organization?

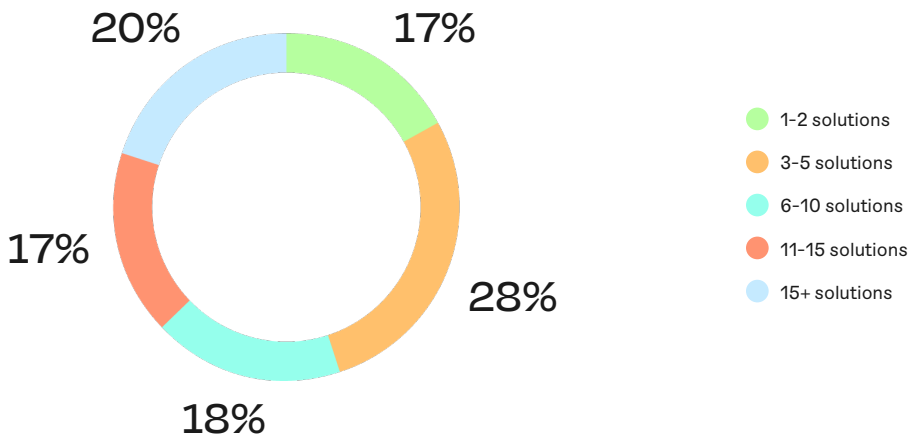
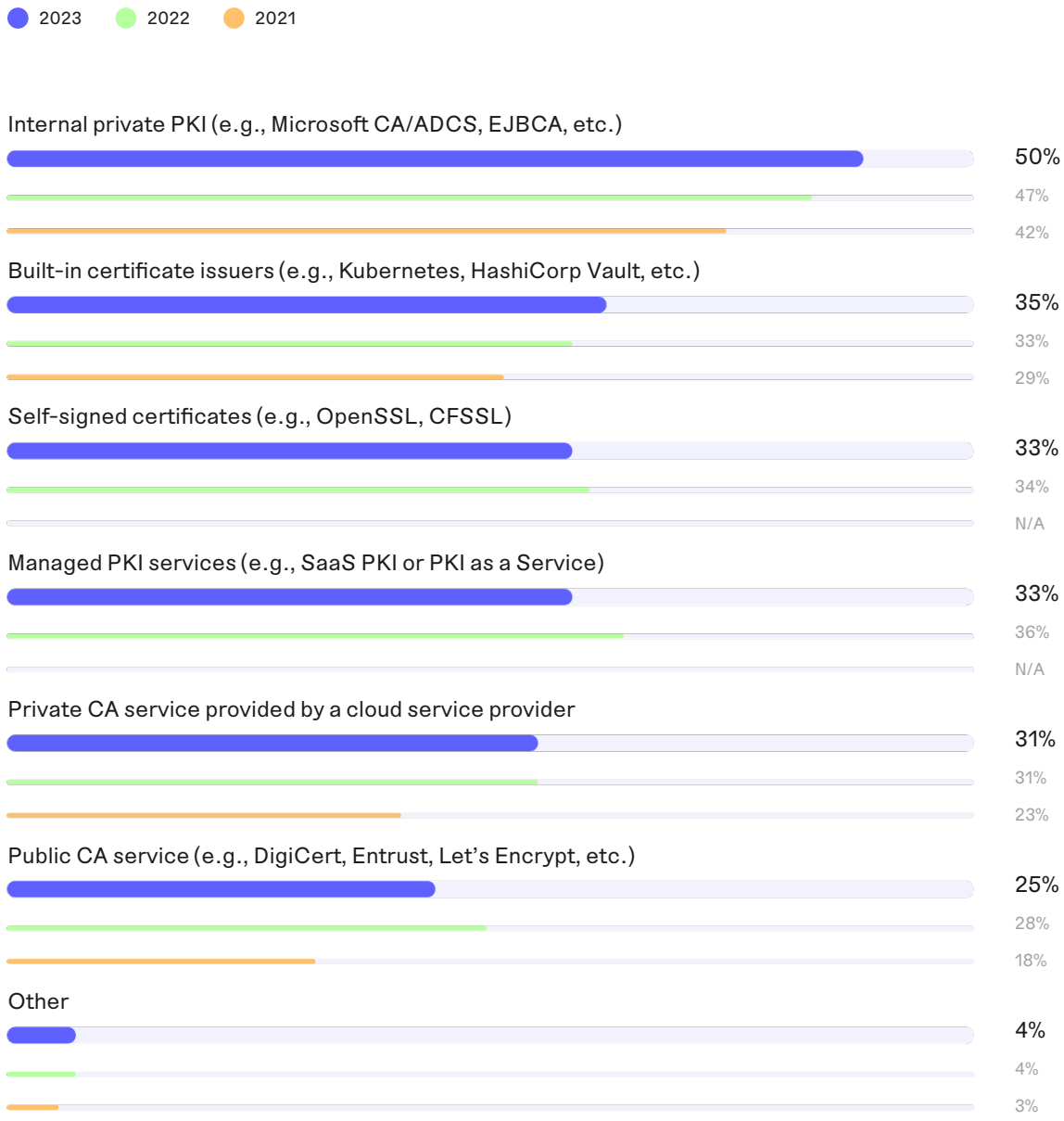


Figure 9

Which of the following PKI and certificate authority (CA) solutions are deployed in your organization?

More than one response permitted

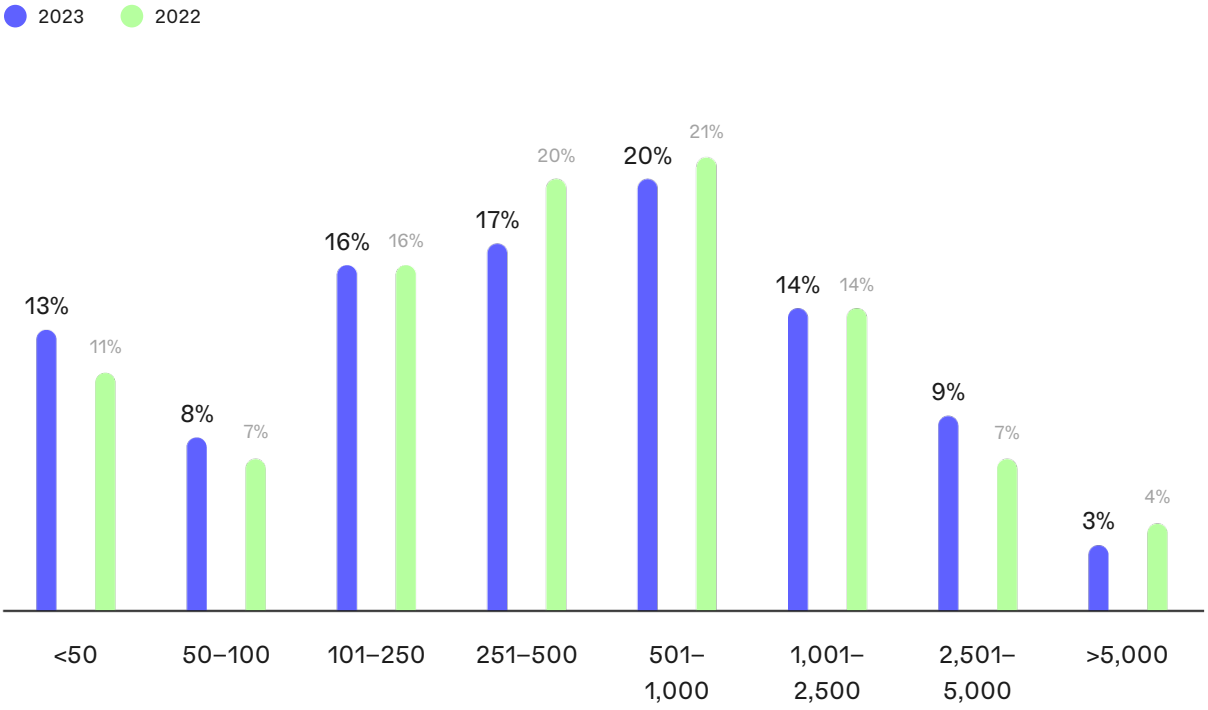


*Note: additional response options were included in the 2022 and 2023 survey

The volume of internally trusted certificates is growing fast. According to respondents, organizations represented in this study have an average of 255,714 internally trusted certificates (i.e. issued from an internal PKI) and 1,024 publicly-issued SSL/TLS certificates (i.e. issued from an SSL/TLS provider or public CA). The average number of internally trusted certificates grew significantly over the past year, with an average of 235,084 reported in 2022.

Figure 10

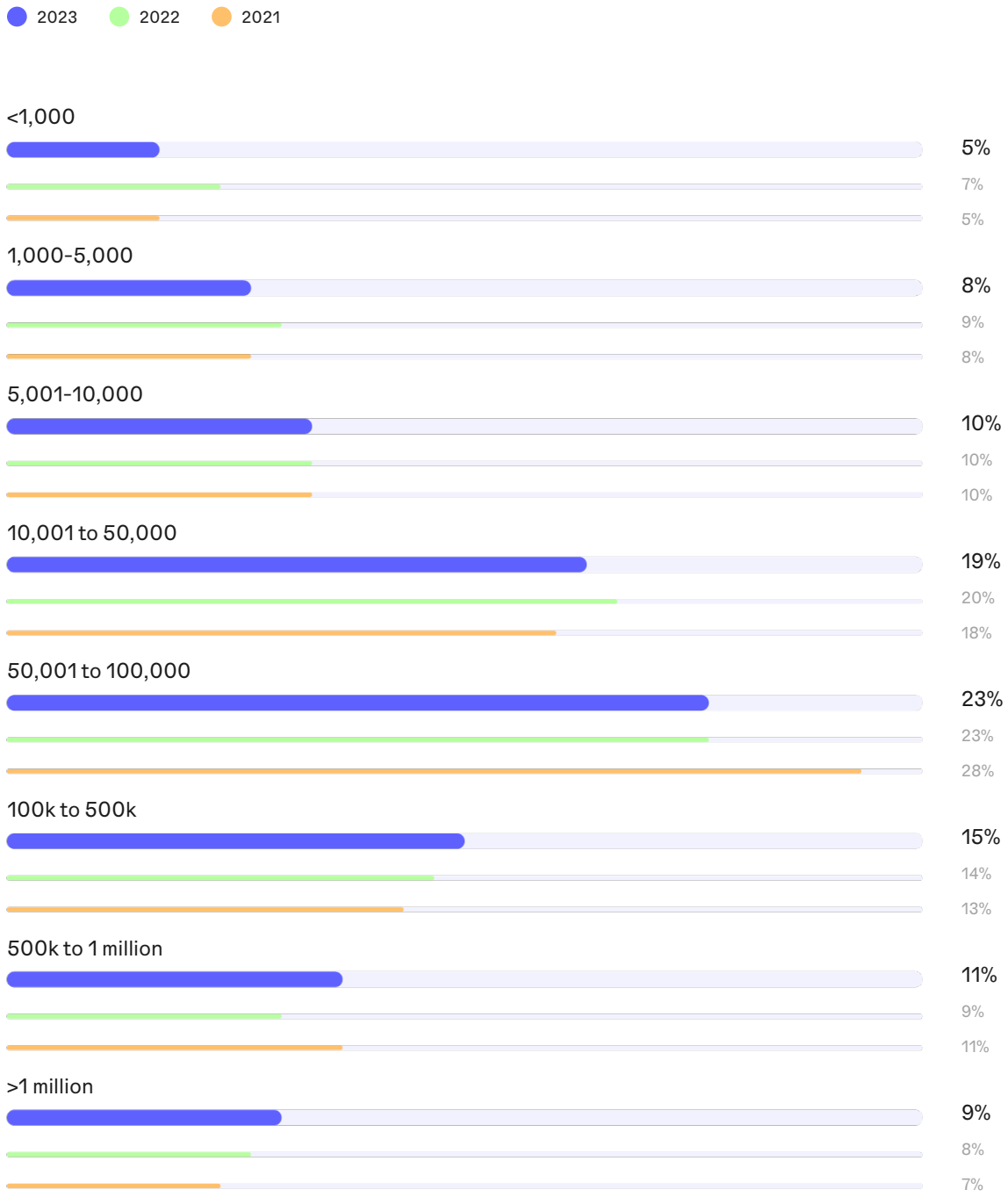
How many public SSL/TLS certificates does your organization have?



*Note: this question was not included in the 2021 survey

Figure 11

How many internally-trusted certificates does your organization have?



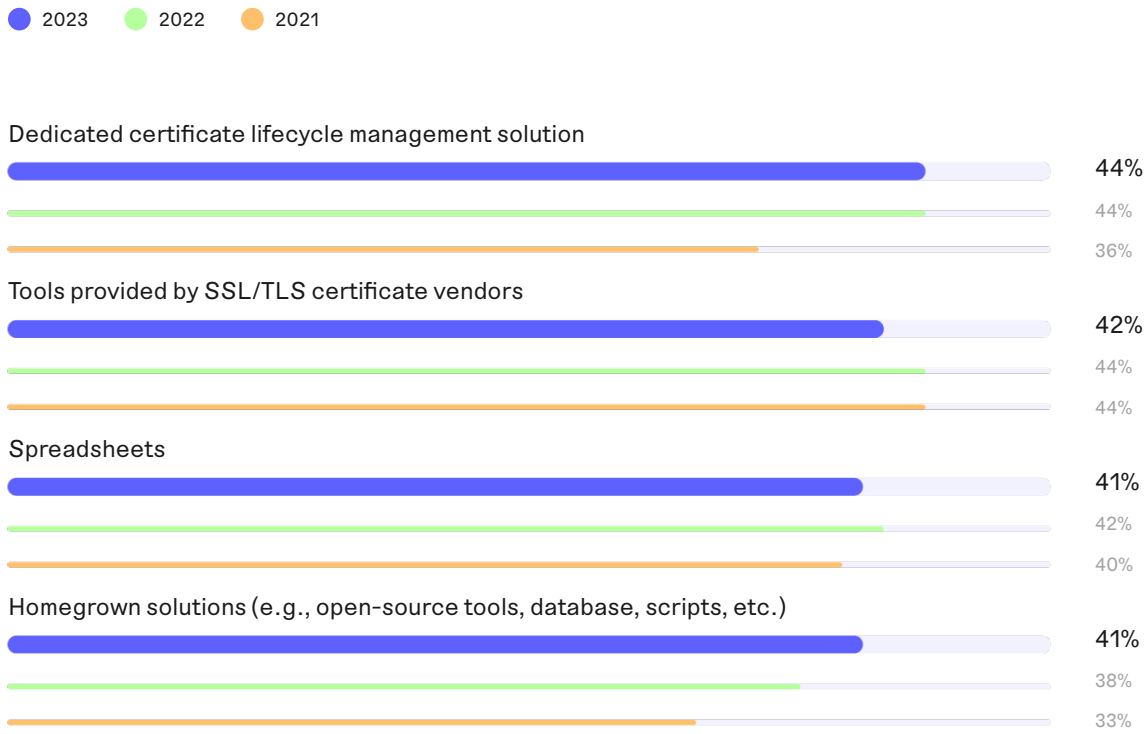
*Note: the extrapolated average value from 2022 has been corrected. The average number of internally trusted certificates within organizations was 235,084 in 2022, not 267,620, as previously reported.

How are certificates being managed? Figure 12 shows that many organizations still rely on a patchwork of disparate and manual solutions to manage digital certificates. Forty-one percent of respondents use spreadsheets and/or homegrown tools, and another 42 percent of respondents use tools provided from their SSL/TLS certificate provider. Use of homegrown solutions to manage certificates has increased consistently year-over year, from 33 percent of respondents in 2021 to 41 percent in 2023.

Figure 12

How does your organization track and manage certificates?

More than one response permitted



Lack of PKI staffing and resources still a problem. PKI isn't just software, it's critical infrastructure. Without the right skills and expertise, it's difficult to configure, deploy, and most importantly, maintain properly over its lifespan. As seen in Figure 13, more than half of respondents say they do not have enough staff and resources to deploy and maintain PKI effectively, showing a relatively consistent year-over-year trend over the past three years.

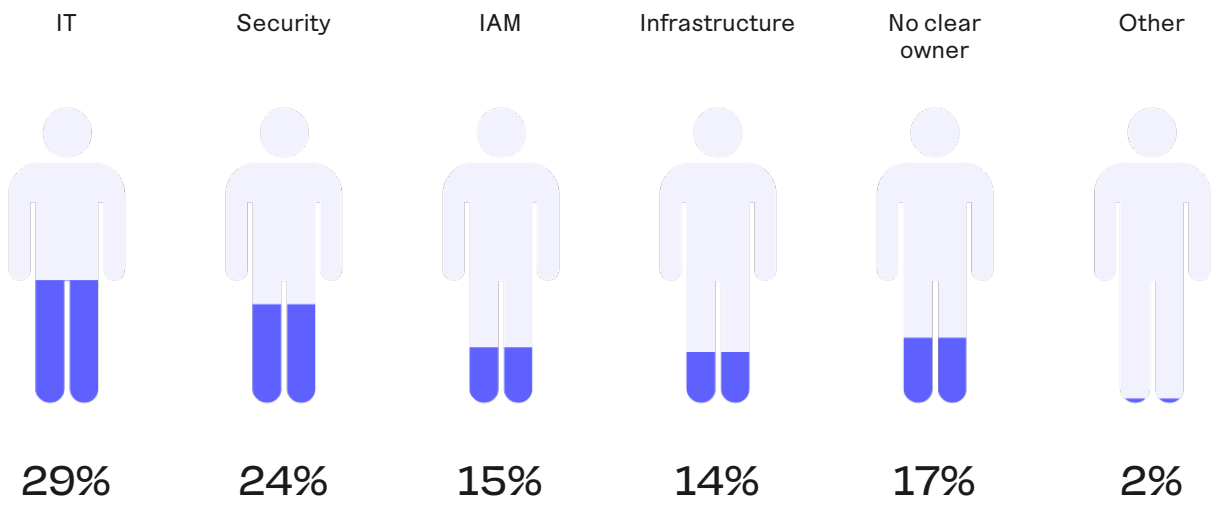
Figure 13

In your opinion, does your organization have enough resources and staff to deploy and maintain PKI effectively?

Who is responsible for PKI? Figure 14 shows the different teams responsible for deploying and managing PKI within organizations represented in this study. IT and security teams are more commonly responsible for PKI, but IAM and infrastructure teams aren't uncommon owners of PKI either. Seventeen percent of respondents say that there is no clear owner.

Figure 14

Who is currently responsible for deploying and managing PKI at your company?



*Note: this question was not included in the 2021 or 2022 survey

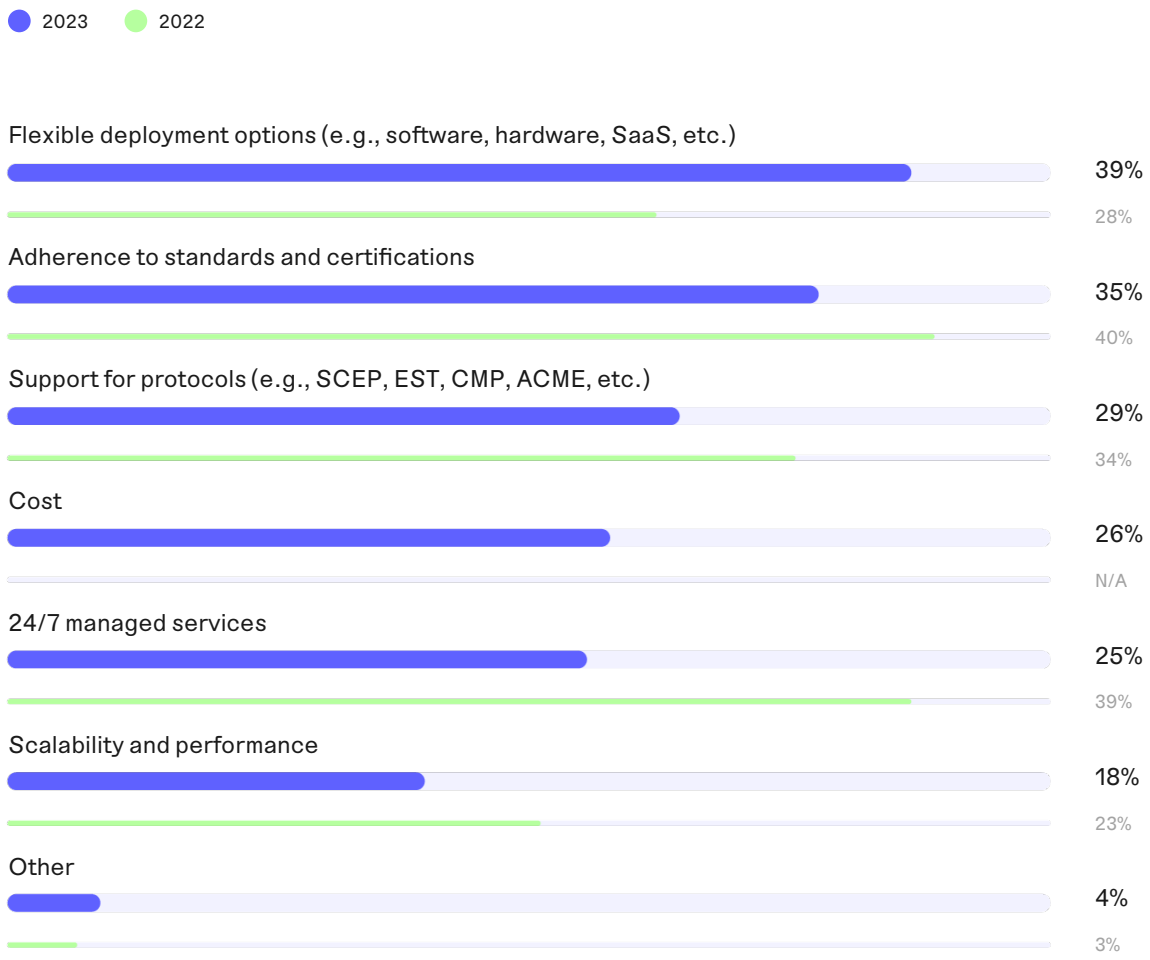
Flexibility and visibility are critical to PKI and certificate management. Figure 15 lists six features or factors considered important when evaluating PKI solutions. Thirty-nine percent of respondents say that flexible deployment options, such as software, hardware, and SaaS-delivered PKI, are a critical feature, followed by adherence to standards and certifications (35 percent of respondents) and support for protocols (29 percent of respondents).

Similarly, Figure 16 shows the most important features or capabilities of certificate management solutions. Sixty-two percent of respondents say complete visibility and inventory of all certificates is an important capability. This comes as no surprise, considering 62 percent of organizations do not know how many keys and certificates they have, as shown previously in Figure 6.

Figure 15

The most important features when evaluating PKI solutions

Three responses permitted

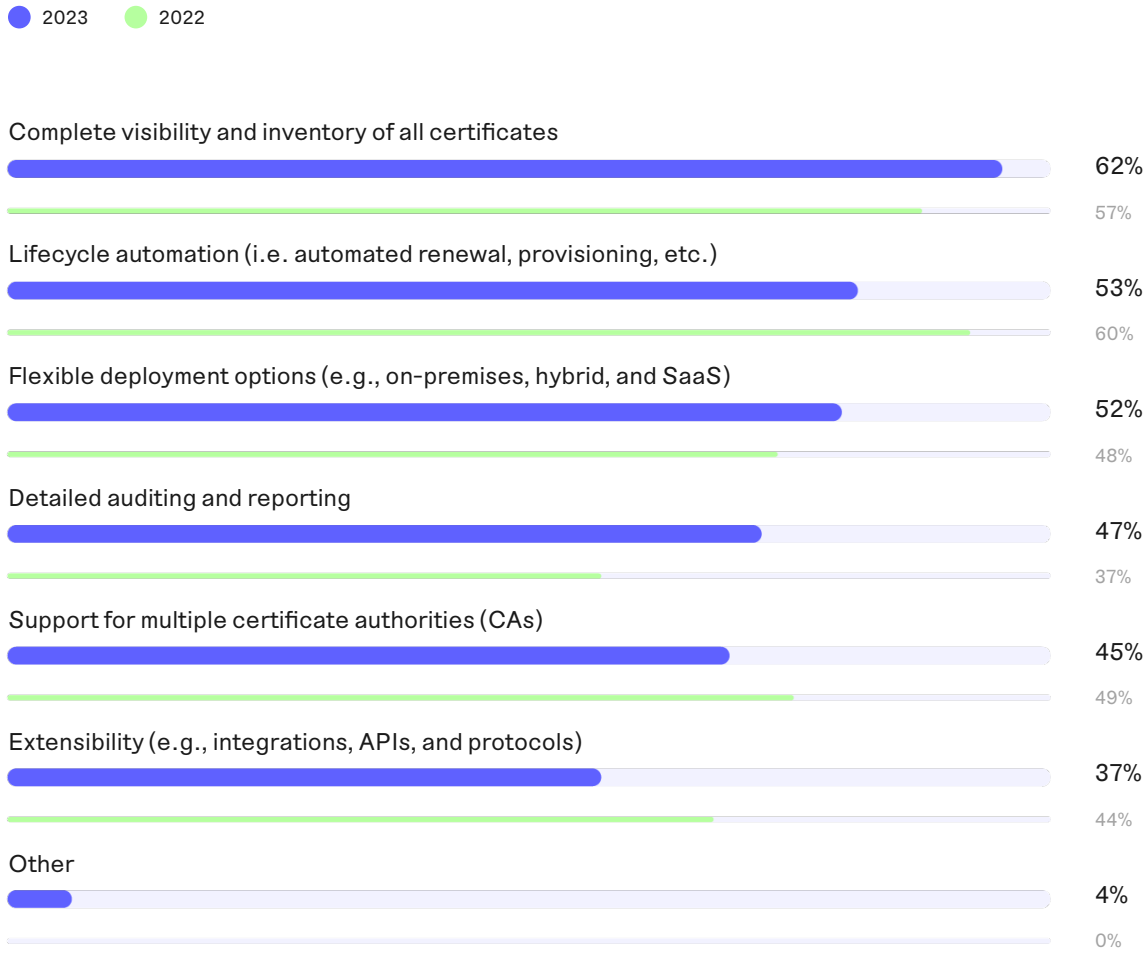


*Note: this question was not included in the 2021 survey

Figure 16

The most important features when evaluating certificate management solutions

Three responses permitted



*Note: this question was not included in the 2021 survey

Code signing practices

In this section, we asked respondents if they are involved in code signing operations. Responses from individuals who said they are not involved were excluded from the following analysis.

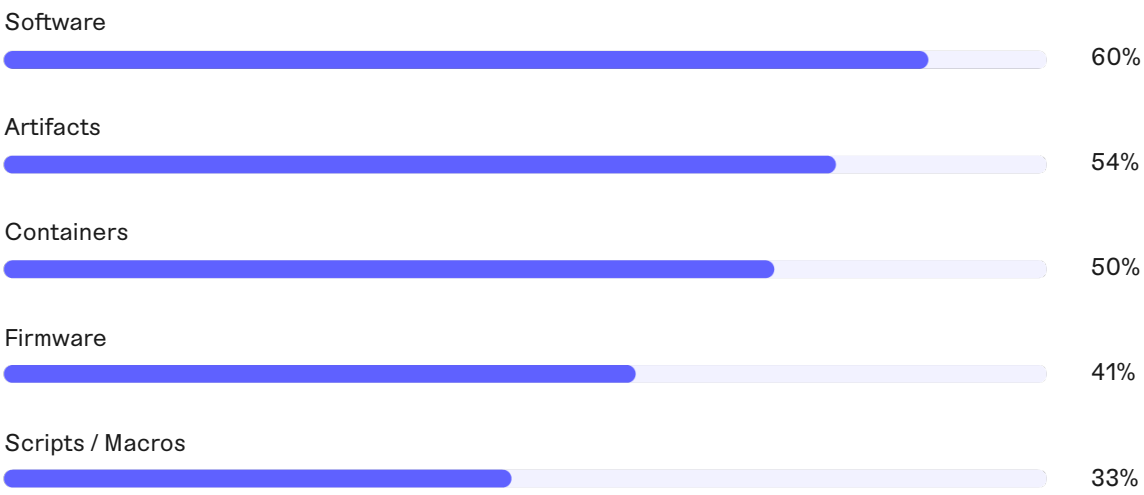
Code signing use cases are expanding. The definition of "code" has changed. As organizations shift toward a "Trust nothing, sign and verify everything" approach, DevOps and security teams are leveraging code signing not just for the software they deliver to end-users, but also for scripts, containers, artifacts, and infrastructure as code used throughout the software development lifecycle (SDLC).

Figure 17 shows that code signing is most often used for software (60 percent of respondents), artifacts (54 percent), and containers (50 percent). For organizations that manufacture hardware or develop firmware, signing and verification are also critical to enable security features such as secure boot and secure over-the-air (OTA) updates.

Figure 17

What are the current use cases for signing within your organization?

More than one response permitted



Responsibility to protect and manage code signing keys varies. Figure 18 reveals that organizations represented in the 2023 study use an average of 23 code signing certificates to digitally sign software, artifacts, containers, and other digital assets.

Sensitive private keys associated with code signing certificates must be securely managed and protected to avoid misuse or theft. As seen in Figure 19, the responsibility to manage and protect these assets is divided between senior developers and management (12 percent of respondents), developers (24 percent), IT operations (29 percent), and IT security (24 percent). Another 11 percent of respondents say no one function is responsible.

Figure 18

How many code signing certificates do you have in your organization?

Figure 19

Who is most responsible for managing and protecting code signing keys?

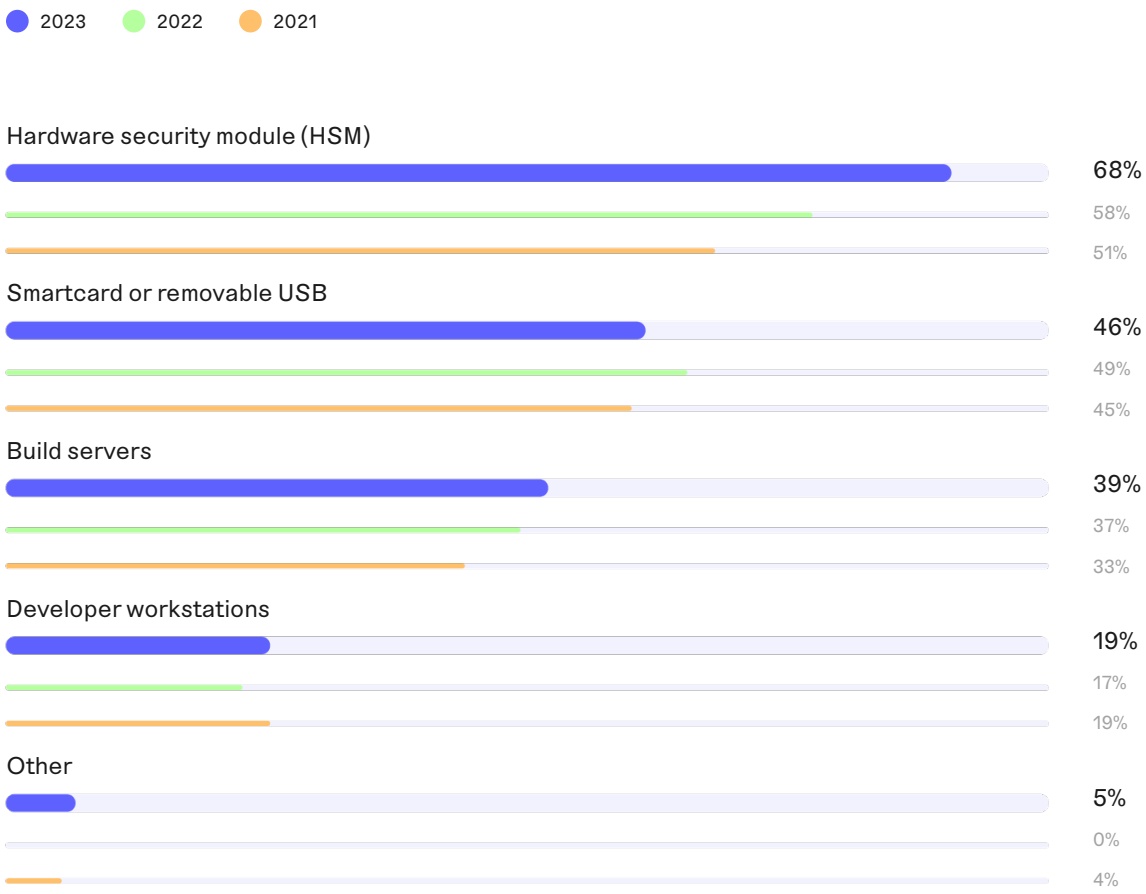
Where are code signing keys stored? Code signing without protecting private keys exposes organizations to serious risk. The problem is that developers and the tools they use need access to these keys to sign code. As a result, private keys are often stored in easily accessible locations, such as servers or workstations, where they are inadvertently exposed to attackers that steal keys to sign and distribute malicious code masked as legitimate software.

As shown in Figure 20, sixty-eight percent of respondents say they follow best practices by storing code signing keys within a hardware security module (HSM), a significant improvement. Another 46 percent of respondents say they store code signing keys in a smartcard or removable USB, which may or may not be encrypted. Many respondents say that code signing keys are stored insecurely on build servers (39 percent) and developer workstations (19 percent).

Figure 20

Where are code signing keys stored in your organization?

More than one response permitted

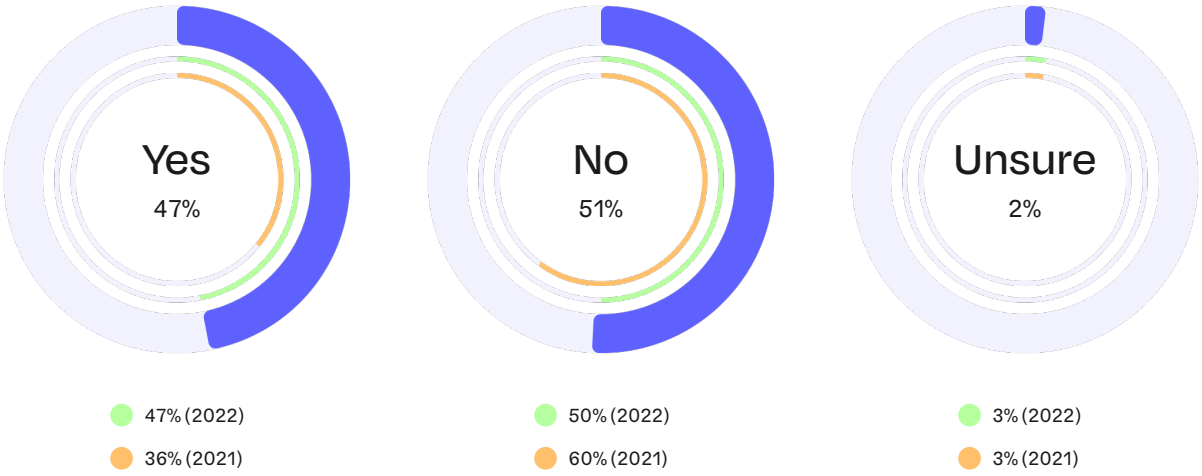


Organizations lack formal code signing access controls. It's not enough to securely generate and store code signing keys. To prevent code signing abuse or misuse in todays dispersed and automated CI/CD environments, organizations must implement policies and access controls that ensure only specific people, machines, and tools with the right permissions have the authorization to sign code.

However, Figure 21 shows that less than half of respondents (47 percent) say their organization has formal access control and approval processes in place for code signing keys.

Figure 21

Does your organization have formal access control and approval processes in place for code signing keys?

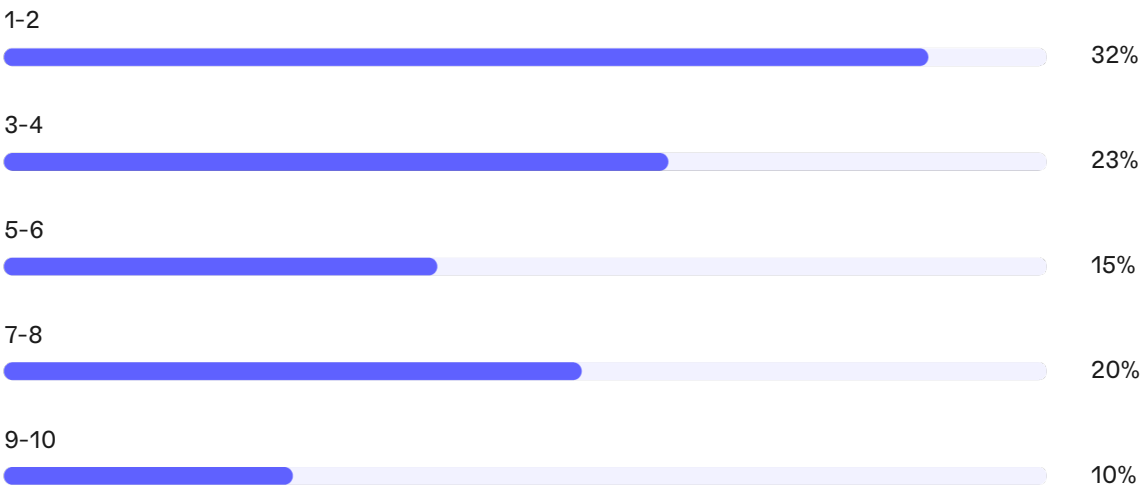


Organizations are not confident in their ability to protect code signing keys. Unsurprisingly, only 30 percent of respondents say they are confident in their organization's ability to protect code signing keys against theft or misuse (7+ responses combined), while 55 percent say they have little to no confidence (<4 responses combined).

Figure 22

How confident are you in your organization's ability to protect code signing keys from theft or misuse by cybercriminals?

On a scale from 1 = no confidence to 10 = high confidence



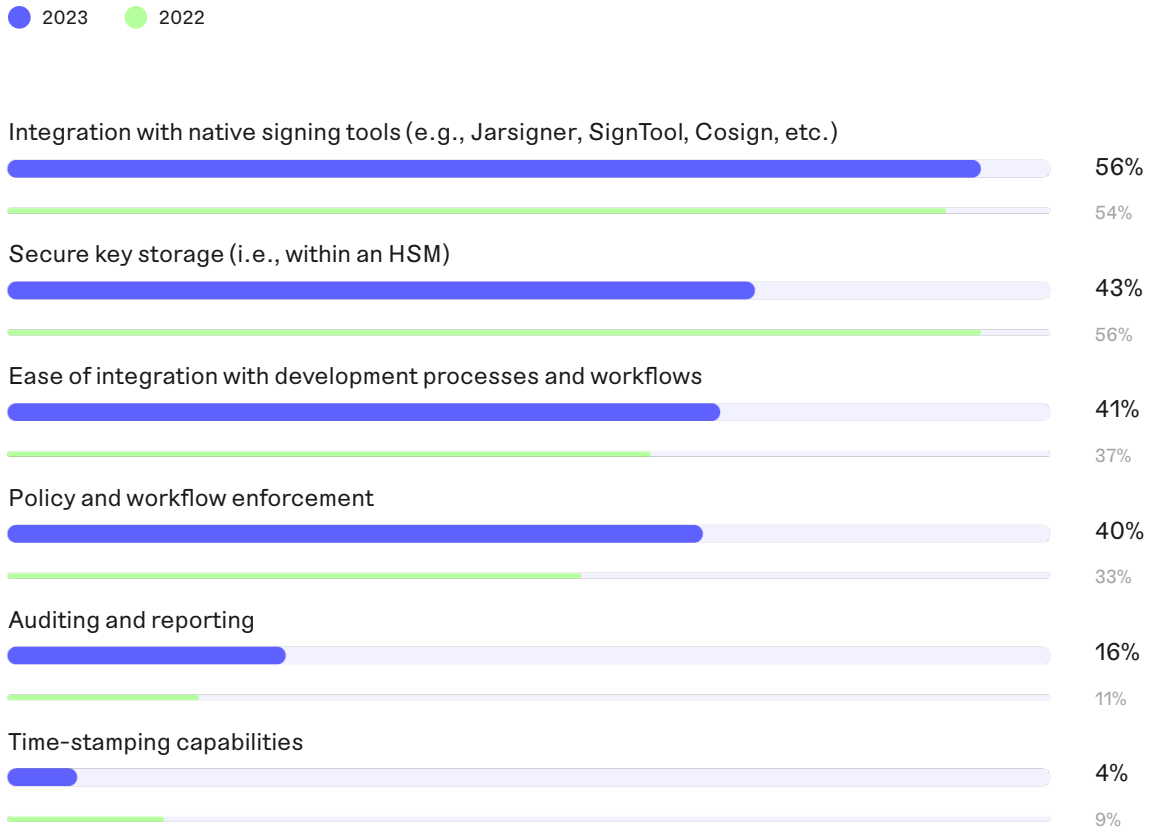
Code signing solutions must integrate with existing tools and processes. Security is a must, but if signing solutions cannot integrate with existing tools and processes, developers won't adopt them.

Figure 23 lists six features considered important when evaluating code signing solutions. According to respondents, the most important features in a code signing solution are integration with native signing tools (56 percent), secure key storage (43 percent), and ease of integration with development processes and workflows (41 percent).

Figure 23

The most important features when evaluating code signing solutions

Two responses permitted



*Note: this question was not included in the 2021 survey

SSH identity management practices

In this section, we asked respondents if they are familiar with their organizations' use of SSH identities. Responses from individuals who said they are not familiar were excluded from the following analysis.

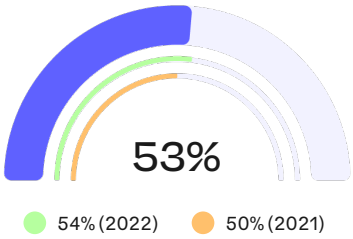
Responsibility for managing SSH identities increasingly falls on administrators. When asked who is responsible for managing SSH credentials, such as SSH keys, SSH certificates, and password-based authentication, respondents generally agreed that it is a shared responsibility, providing more than one response in many cases.

That said, as shown in Figure 24, responsibility for managing SSH credentials is shifting toward network and cloud administrators, both increasing consistently year-over-year.

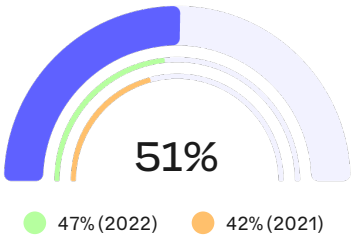
Figure 24

Who is responsible for managing SSH credentials?

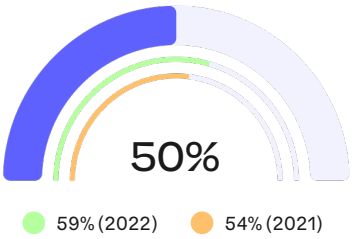
More than one response permitted



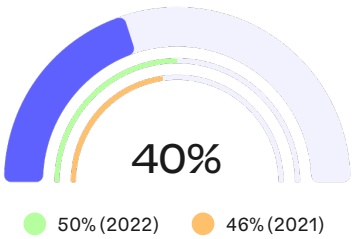
IT Security



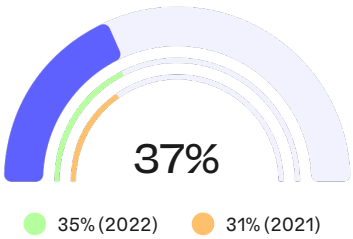
Network Administrators



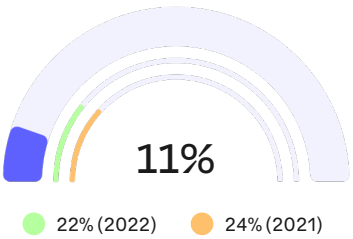
IT Operations



Identity and Access Management (IAM)



Cloud Administrators



No one function is responsible

How are SSH identities managed? Fifty-four percent of respondents say their organization has no centralized management for SSH identities, leaving admins to manage their own SSH keys, certificates, or passwords. Another 54 percent say they use some form of manual tracking. Only a few respondents use a privileged access management (PAM) solution (26 percent) or a dedicated SSH key management solution (27 percent).

Figure 25

How does your organization manage SSH credentials?

More than one response permitted

Most organizations are in the dark when it comes to SSH identities. Despite their widespread use and high-privilege access, SSH credentials are often left untracked, sitting dormant on servers where attackers can exploit them to gain access to critical systems and move laterally without detection.

More respondents say they do not have an accurate inventory of SSH credentials (53 percent) than those that say they do (41 percent). Another 6 percent say they are unsure. As seen in Figure 27, only 51 percent of respondents say their organization rotates SSH identities regularly (at least annually), while 44 percent say that their organization rotates them less frequently or not at all.

Figure 26

Do you have an accurate inventory of SSH credentials in your organization?

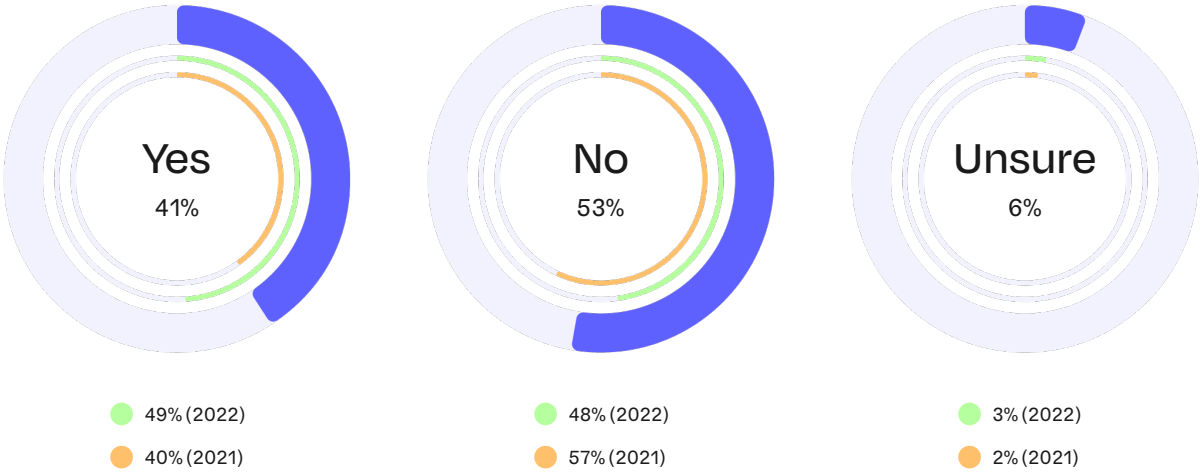


Figure 27

How often does your organization rotate SSH credentials?

The impact of outages, machine identity compromise, and audit failures

Every machine needs an identity to authenticate and securely communicate with other devices, workloads, and people within and outside the organization. But as the number of machines grows rapidly with adoption of cloud, IoT devices, and the remote workforce, the burden to issue and manage machine identities weighs heavy on IT and security teams.

Without the right tools and processes, teams lose control over machine identities. Certificates expire unexpectedly, causing disruptive outages to services and applications. Sensitive keys used to sign code or gain privileged access to backend systems are misused by attackers. Internal or external auditors discover gaps in systems and policies that lead to weeks or even months of remediation.

In this section, we analyze the frequency, seriousness, and risk impact of these incidents. Here, we've provided a quick breakdown of these incidents with examples of recent high-profile events.

Certificate outages

If an unknown or untracked certificate is left to expire, the systems or applications it is installed on stop working, causing downtime and disruption for internal users or customer-facing services.

Megaphone goes silent

On May 31, 2022, millions of listeners on a popular Spotify-owned podcast-hosting platform, Megaphone, could not access their favorite shows for more than eight hours after a single SSL certificate expired, taking down critical systems.[1] For every outage like this one that makes the headlines, there are thousands more that no one hears about.

1 Massive podcast outage caused by Spotify's failure to renew security certificate

Machine ID compromise

Machine identities, such as SSH keys, TLS certificates, and code signing keys, are high-value targets for cybercriminals that use them to sign and distribute malicious code, gain privileged access to systems, or even impersonate legitimate companies.

Signing keys exposed

On December 6, 2022, the popular code-hosting platform, GitHub, reported an unauthorized user gained access to a repository containing three password-protected code signing certificates used for its legacy Atom and Desktop applications. Fortunately, GitHub detected the breach quickly and were able to take corrective action before any damage had been done.[2]

Failed audits

Unexpected audit findings and non-compliance with regulatory mandates related to PKI, signing, and certificate management can result in potential fines or costly remediation efforts.

New mandates increase pressure

On March 2, 2023, the Biden-Harris Administration released the National Cybersecurity Strategy, which, among other items, placed more responsibility on IoT device manufacturers and software companies to ensure the security and integrity of their products. This mandate and others like it will undoubtedly put increased requirements on companies to issue and manage unique identities for devices and digitally sign software to ensure integrity.[3]

2 Action needed for GitHub Desktop and Atom users

3 Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy

What keeps IT and security teams up at night? Respondents were asked to rate the perceived seriousness (Figure 28) and financial impact (Figure 29) of each incident on a scale from 1 (not serious/very serious impact) to 10 (very serious/very serious impact).

Overall, the perceived seriousness and financial impact of machine identity-related incidents have stabilized in this year's study after significant increases from 2021 to 2022.

Failed audits remain the most costly and serious incident, with 66 percent of respondents saying audit failures are a very serious concern, and 57 percent saying these incidents have a very serious financial impact on the organization.

Figure 28

The seriousness of machine identity-related incidents

On a scale of 1 = not serious to 10 = very serious. 7+ responses presented.

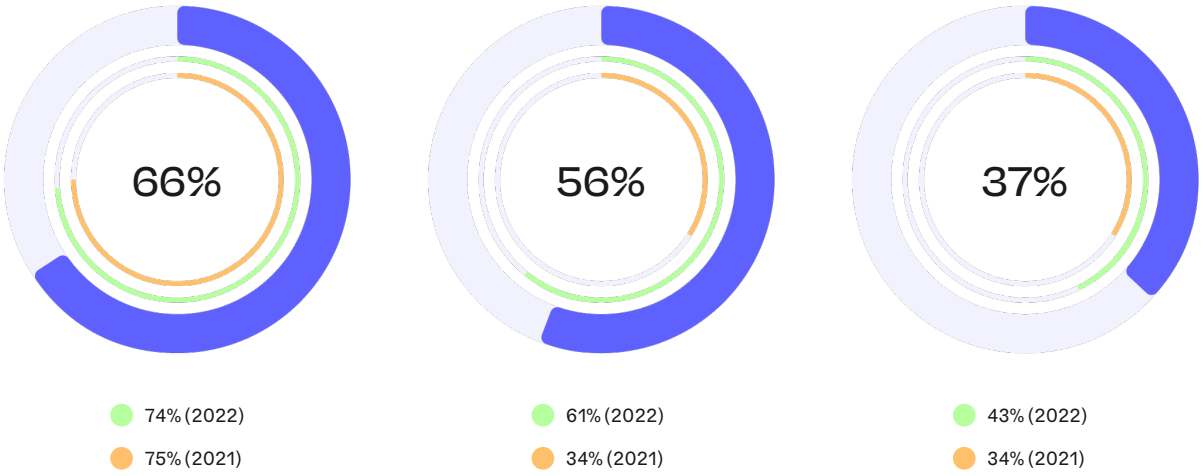
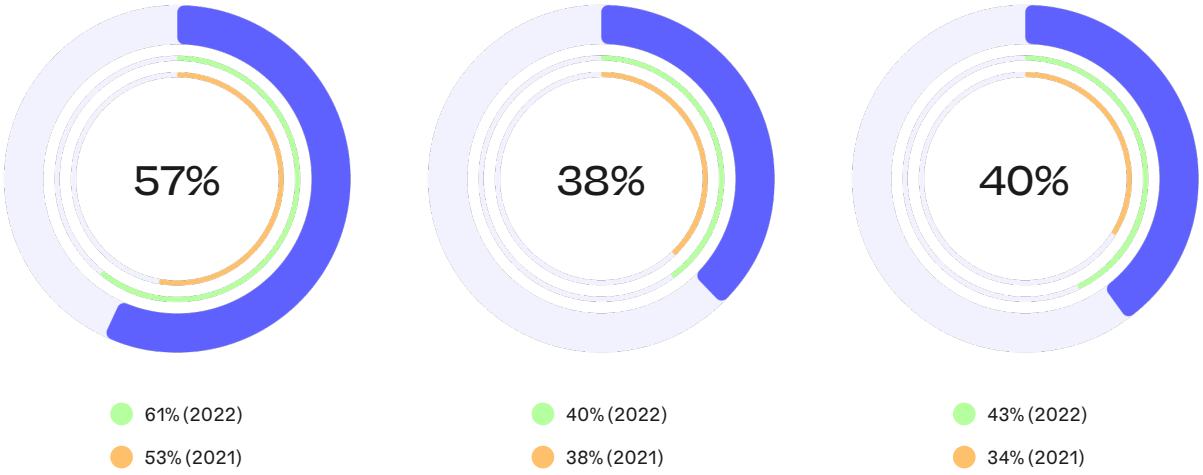


Figure 29

The financial impact of machine identity-related incidents

On a scale of 1 = no impact to 10 = very serious impact. 7+ responses presented.

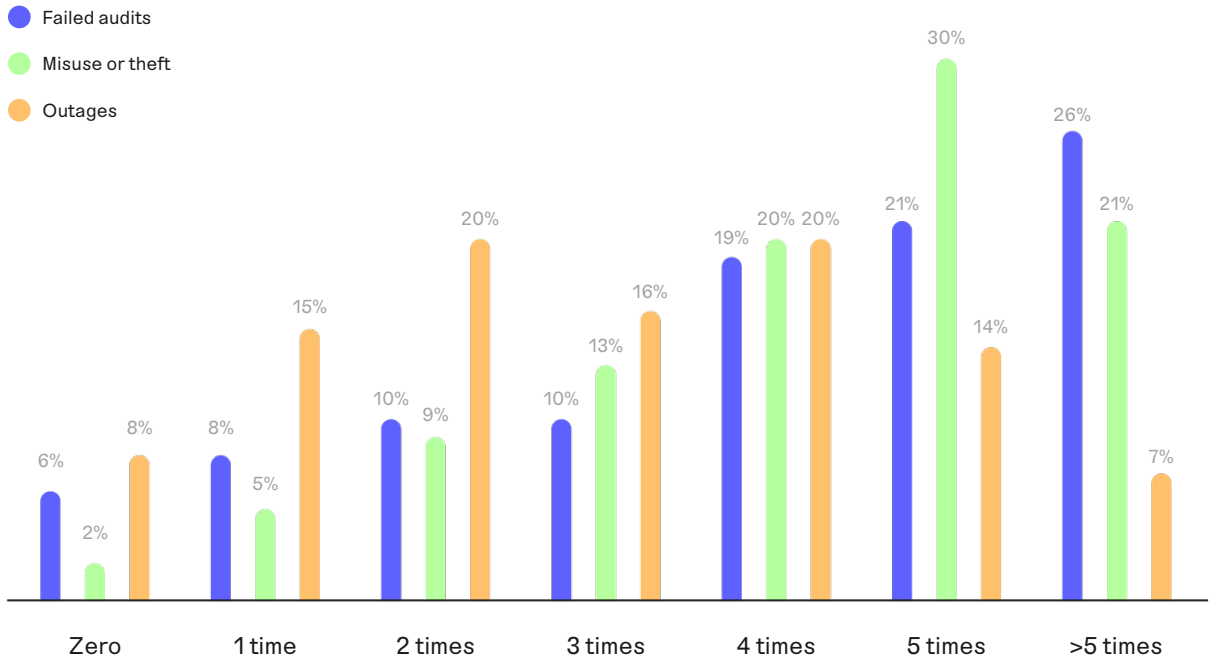


How often do these incidents occur? Respondents were asked to estimate the number of times each incident occurred within the past 24 months. As shown in Figure 30, misuse or theft of keys and certificates is the most frequently reported incident, with 93 percent of respondents say their organization experienced at least two such incidents in the past 24 months.

On average, respondents estimate their organization experienced 4.37 incidents involving theft or misuse of keys and certificates in the past 24 months, followed by failed audits (4.19 incidents) and outages caused by expired certificates (3.00 incidents).

Figure 30

The frequency of machine identity-related incidents in the past 24 months



Average number of incidents in the past 24 months

4.19
Failed Audits

4.37
Misuse or theft

3.00
Outages

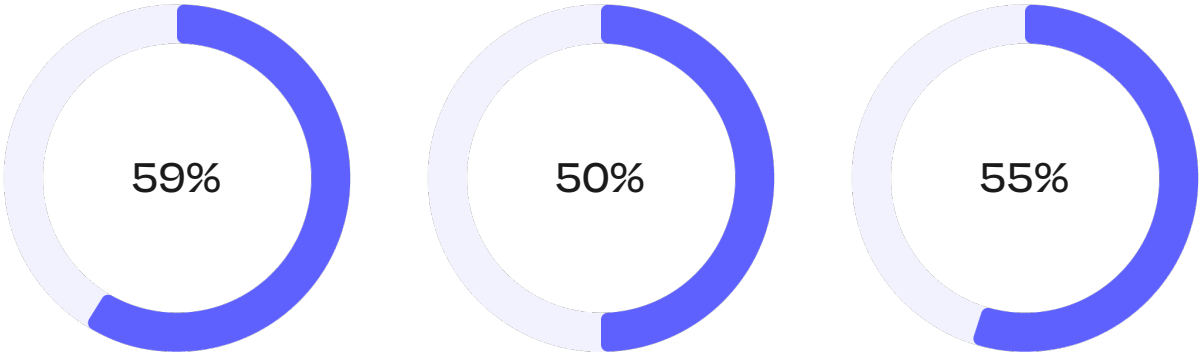
Certificate-related outages disrupt critical systems. Outages caused by unexpected certificate expiration can wreak havoc on critical infrastructure – from customer-facing applications and online storefronts to internal devices and networks.

As shown in Figure 31, fifty-five percent of respondents say that certificate outages in the past 24 months resulted in severe incidents that caused major disruption to customer-facing services. Another 50 percent say outages triggered major incidents disrupting a subset of customers or internal users, while 59 percent say outages caused minor inconvenience to customers and internal users.

Figure 31

Which of the following incidents have occurred due to certificates unexpectedly expiring in the past 24 months?

More than one response permitted



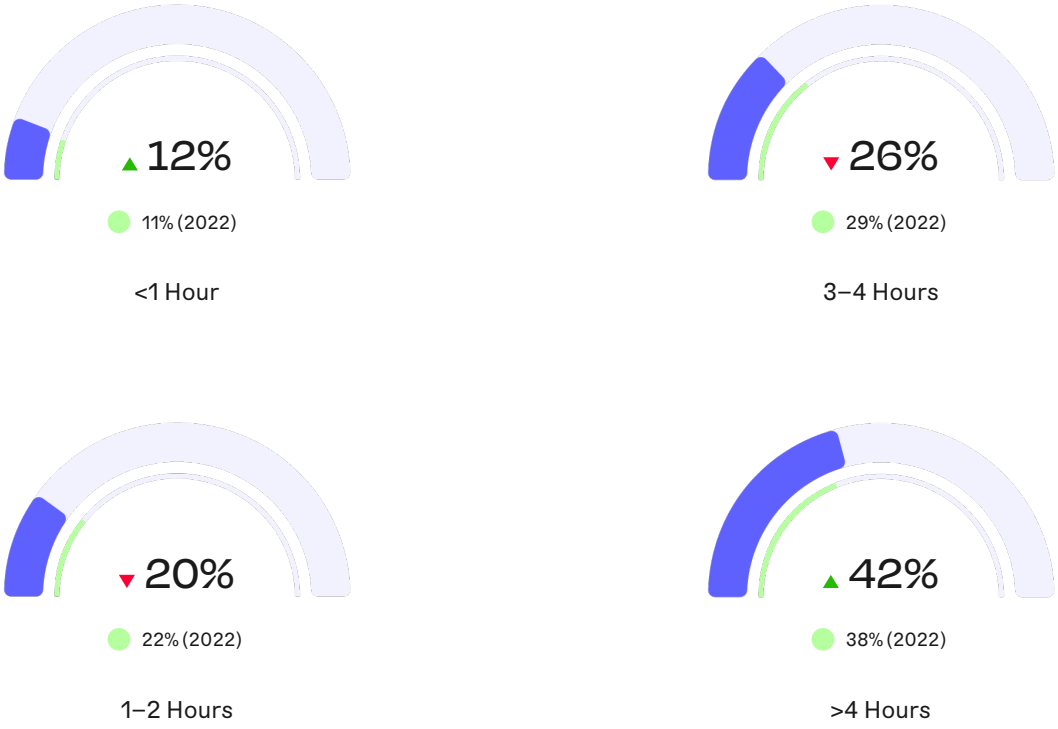
Time to recovery (TTR) from a certificate-related outage is slow. Remediating a certificate-related outages isn't as simple as renewing the expired certificate; it involves identifying the root cause, locating the expired certificate, and then renewing, re-issuing, and provisioning the certificate to all affected systems before they can be restarted.

Respondents were asked how long it takes their teams to identify and remediate certificate-related outages. As seen in Figure 32, forty-two percent of respondents say it takes their teams more than 4 hours to recover, while another 26 percent of respondents say it takes 3 to 4 hours. On average, it takes organizations 3.79 hours to fully recover, compared to an average of 3.28 hours in last years study.

Without visibility of certificates and their locations, or the ability to automate renewal and provisioning, it can take teams hours, rather than minutes, to recover from these incidents, not to mention preventing these incidents from occurring in the first place.

Figure 32

On average, how much time does it take your teams to identify and remediate a certificate-related outage?



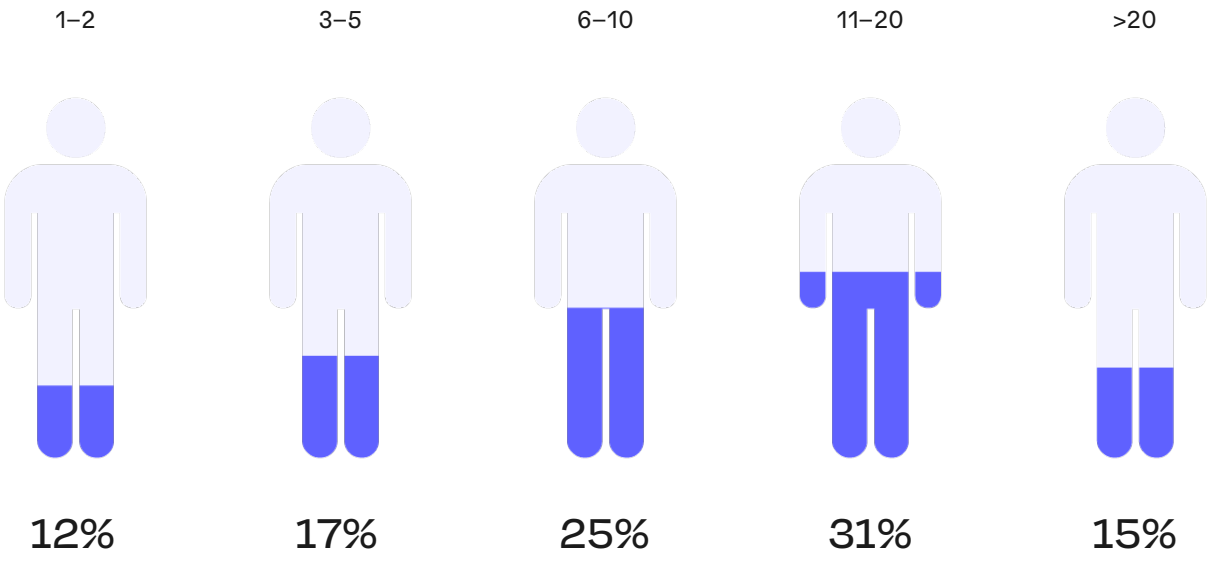
*Note: this question was not included in the 2021 survey

Outages pull multiple IT staff away from their day-to-day priorities. Respondents were asked, on average, how many staff members are directly engaged during a certificate-related outage, including those involved in diagnosing, resolving, and remediating the incident.

According to respondents, an average of 11 staff are directly involved in remediating a typical certificate outage, with 46 percent saying it requires more than 11 staff.

Figure 33

How many staff members, on average, are directly involved during a typical outages caused by an expired certificate?



*Note: this question was not included in the 2021 or 2022 survey

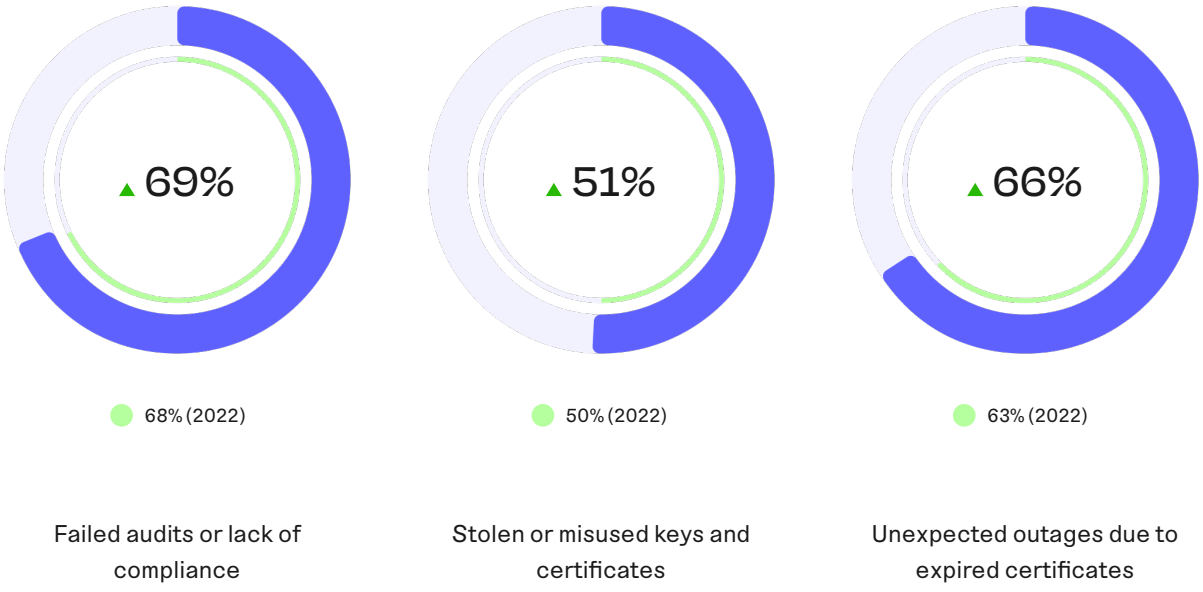
Machine identity-related incidents expected to continue. Respondents were asked about the likelihood of audit failures, misuse or theft of keys and certificates, and certificate-related outages occurring within the next 24 months on a scale from not likely, somewhat likely, likely, and very likely.

As seen in Figure 34, a majority of respondents predict that these incidents are likely or very likely to continue in the next 24 months. The most likely incident to occur is failed audits or lack of compliance, followed by certificate outages, and misuse or theft of keys and certificates.

Figure 34

The likelihood of these incidents occurring in the next 24 months

Likely and very likely responses combined



*Note: this question was not included in the 2021 survey

Five steps to successful machine identity management

In this section, Keyfactor provides steps that organizations can take to improve their machine identity management strategy and recommended resources to support these efforts.

Establish ownership of Machine Identity.

Clear ownership is imperative. In the study, 78% of respondents said they have an immature or no machine identity management working group or team. Technology is an obvious consideration for machine identity management. However, properly implementing technology relies on the right foundation of people, processes, and practices.

According to Gartner, organizations should "Define ownership of tools, keys, secrets and certificates respectively. Use the guidance to move the PKI team from an 'in the way management' structure to a 'delegated management' structure by focusing on the guardrails and policies more than the centralization of tools."*

Invest in your machine identity management.

Investing in your machine identity management platform can help your organization improve visibility and accelerate incident response and productivity. Automate and standardize security controls by integrating them with existing tools, workflows, and applications.

Use best practices established by your working group to audit your machine identity landscape, determine where gaps exist, and find tools and processes that fit the unique requirements of different teams within your organization, including:

- PKI and certificate management
- SSH key management
- Privileged access management (PAM)
- Enterprise code signing
- Secrets managers
- Key management systems (KMS)
- Hardware security modules (HSMs)
- Managed PKI services

* Gartner, Solution Comparison for PKI and Certificate Management Tools, 2 March 2021, Erik Wahlstrom, Paul Rabinovich

Reduce complexity in your PKI infrastructure.

For the first time, the top strategic priority for digital security in organizations is reducing complexity in the PKI infrastructure, an increase from 50 percent in 2021 to 58 percent in this year's research. More organizations are making the prevention of unexpected outages caused by expired certificates a priority (53 percent of respondents vs. only 30 percent of respondents in 2022).

Notably, 74 percent of respondents, an increase from 61 percent in 2021, say their organizations are deploying more cryptographic keys and digital certificates. As a result, this has significantly increased the operational burden on their organizations' teams, according to 72 percent of respondents, an increase from 62 percent in 2021.

Reducing complexity is hindered by not having a mature machine identity working group supported by enough resources. Only 31 percent of respondents say their organizations have a mature machine identity working group that provides leadership, research, implementation strategy, ownership, and best practices. Further, 53 percent of respondents say their organizations do not allocate enough resources and staff dedicated to PKI deployment.

Use managed services to help close the skills gap and alleviate the effects of the cybersecurity labor shortage.

Forty-two percent of respondents in the study identified skills shortages as barriers to setting an enterprise-wide cryptography and machine identity strategy. Another 31% cite insufficient resources — time and money — as an obstacle.

PKI and cryptography experts are hard to find and even harder to retain. A managed PKI or crypto-services provider can help significantly reduce infrastructure costs, mitigate risks, and eliminate the operational burden associated with running PKI in-house, especially during a global labor shortage.

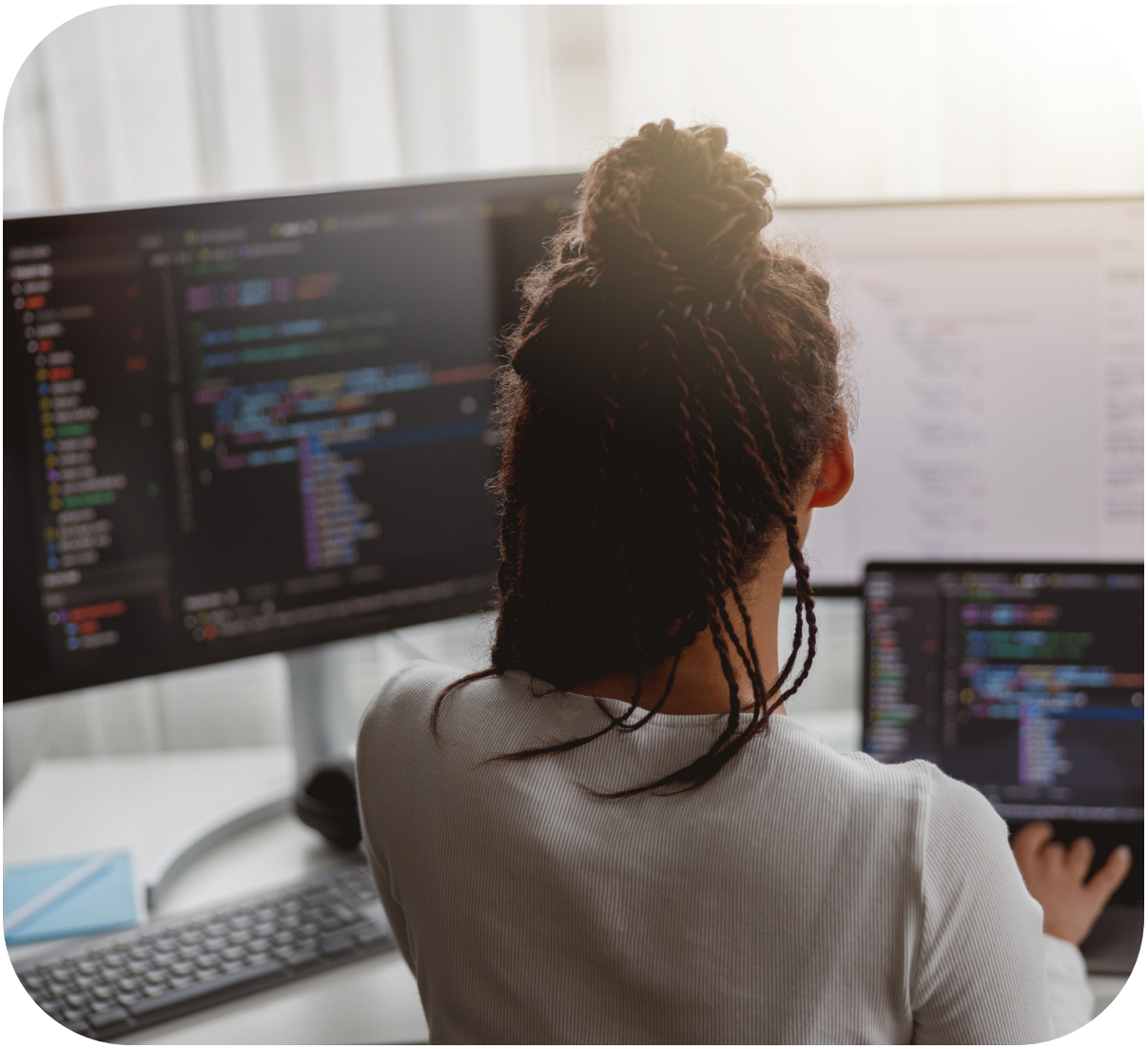
Code signing security should be an important part of machine identity management strategies.

Code signing without securing private keys can expose organizations to significant risks. Software developers are often required to sign code to support installation. Without secure code signing, attackers can compromise these keys to sign and distribute malicious code to an organization's customers masked as legitimate software or firmware.

Respondents were asked how they are involved in code signing, and 71 percent said it is to sign code and software digitally. Sixty-one percent said they are responsible for managing these keys, and 50 percent of respondents audit and protect access to code signing keys. According to the research, the respondents most responsible for managing and protecting code signing keys are IT operations (29 percent), developers (24 percent), and IT security (24 percent).

Code signing use cases are expanding: Organizations often use code signing for software, artifacts, and containers. Best practices in code signing include having a formal code signing process, enabling developers to sign code from everywhere while ensuring the keys remain safe. However, security and development teams need to work collaboratively and integrate code-signing processes with existing tools and workflows without the burden of extra steps to access keys that are securely stored. Leveraging a signing solution can help to ensure that proper security is adhered to while maximum flexibility is available to sign artifacts when and as required, all while maintaining an auditable trail to ensure compliance.

In our software-driven world, trust is everything. Ensuring that an organization's security and development teams are working together to protect the digital certificates and keys used for code signing is key to ensuring their software remains secure and trusted – making code signing a critical part of a secure software supply chain.



Recommendations

Helpful resources

Three Strategies to Navigate the Cybersecurity Labor Shortage

Find out how to navigate the cybersecurity labor shortage and its impacts with strategies to help your team do more with less, plus tips on building a business case to modernize and automate your PKI.

Learn more ↗

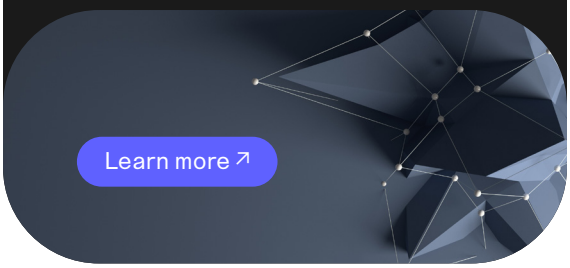
The Definitive Roadmap to Secure Code Signing

Learn about the importance of secure code signing and the risks of poor implementation. Discover four practical steps to overcome security challenges and the solutions to put you on the right track.

Learn more ↗

Planning Ahead for Post-Quantum Cybersecurity

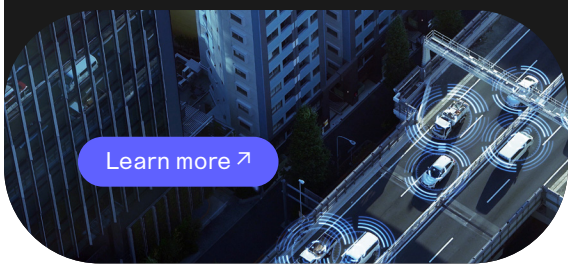
Find out why now is the time for organizations to plan how to protect their data and identities from the future threat of quantum computing.



Learn more ↗

Outlook of IoT Cybersecurity in 2023 and beyond

Watch this on-demand webinar with Admir Abdurahmanovic, SVP of Strategy, Keyfactor, to learn how to prepare for the changing IoT security landscape in 2023.

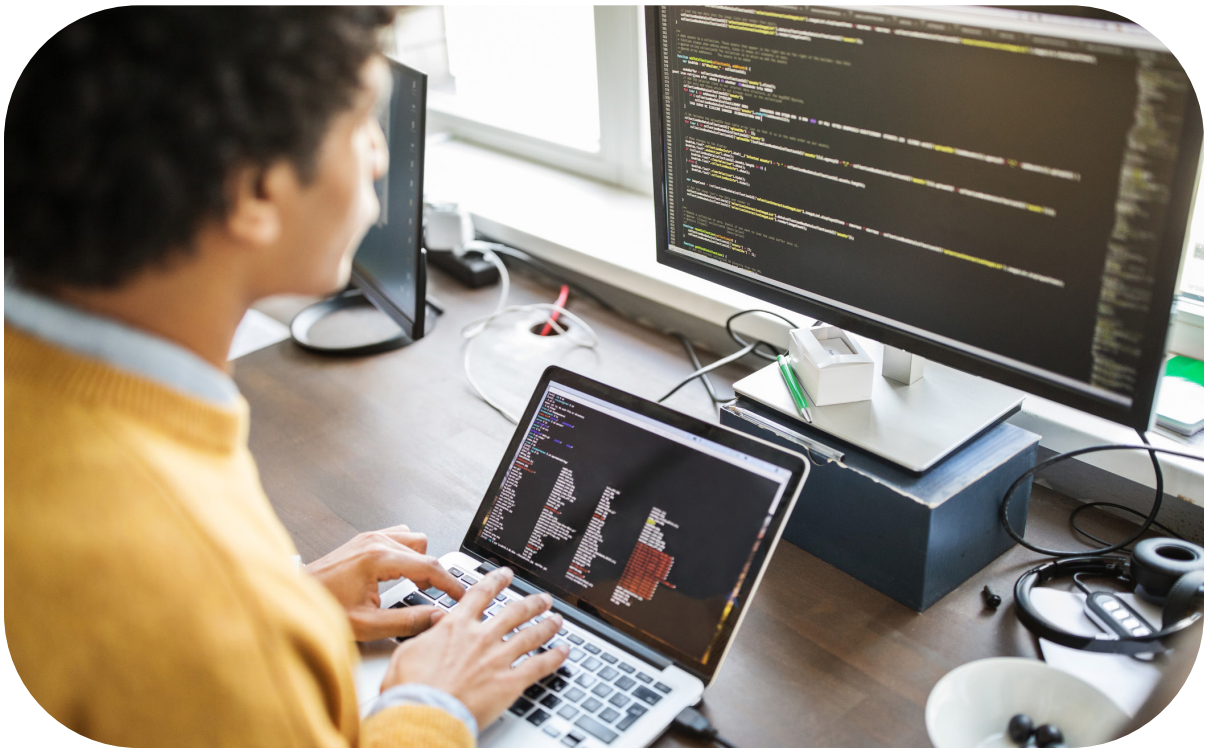


Learn more ↗

Research methodology

A sampling frame of 31,817 IT security professionals in North America and EMEA and organizations with a PKI were selected as participants in this survey. Table 1 shows 1,411 total returns. Screening and reliability checks required the removal of 131 surveys. Our final sample consisted of 1,280 surveys or a 4.0 percent response. All respondents are familiar with their organization's PKI.

Sample Response	Frequency
Sampling frame	31,817
Total returns	1,411
Rejected or screened surveys	131
Final sample	1,280
Response rate	4%



Survey respondents

Here's a closer look at the 1,280 individuals who completed the survey in January 2023.

Figure 35

Current position within the organization

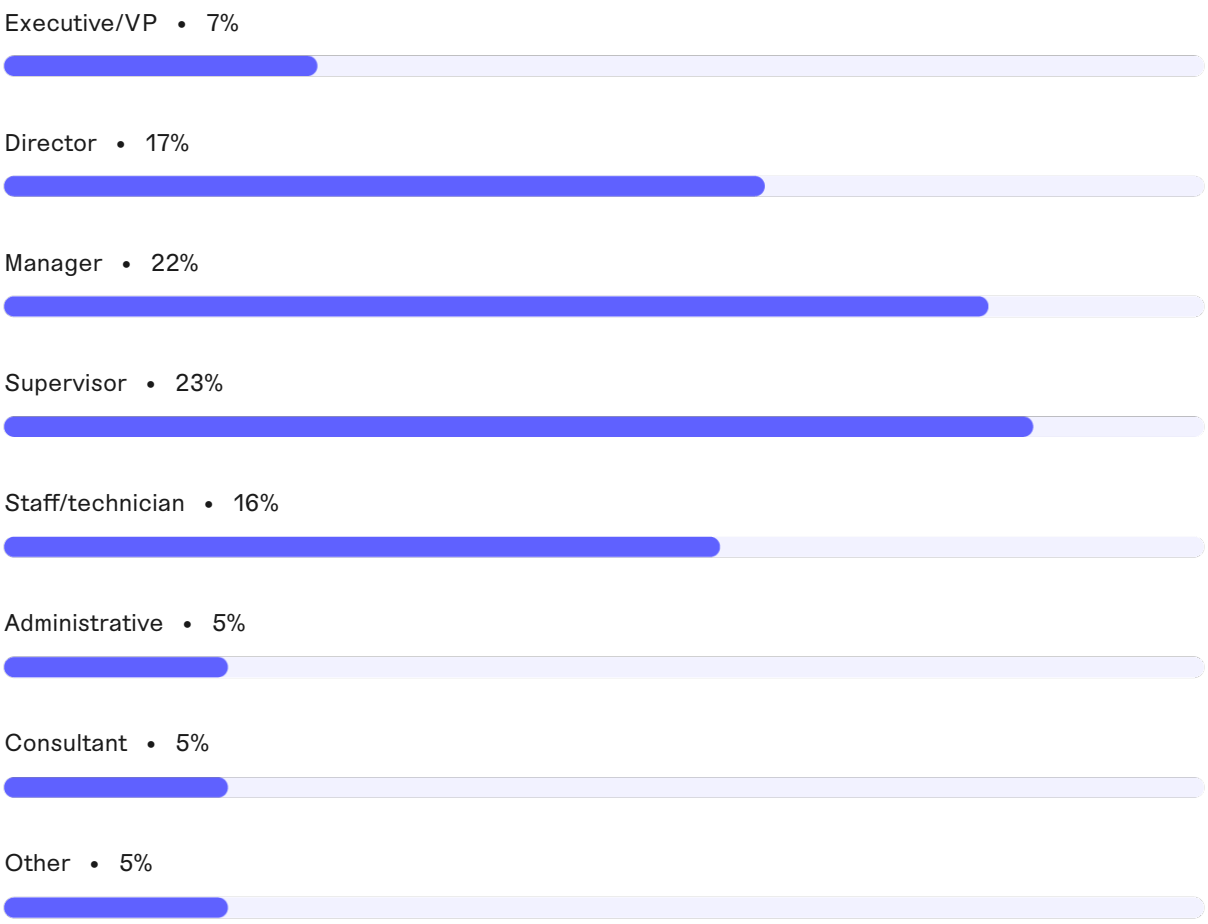
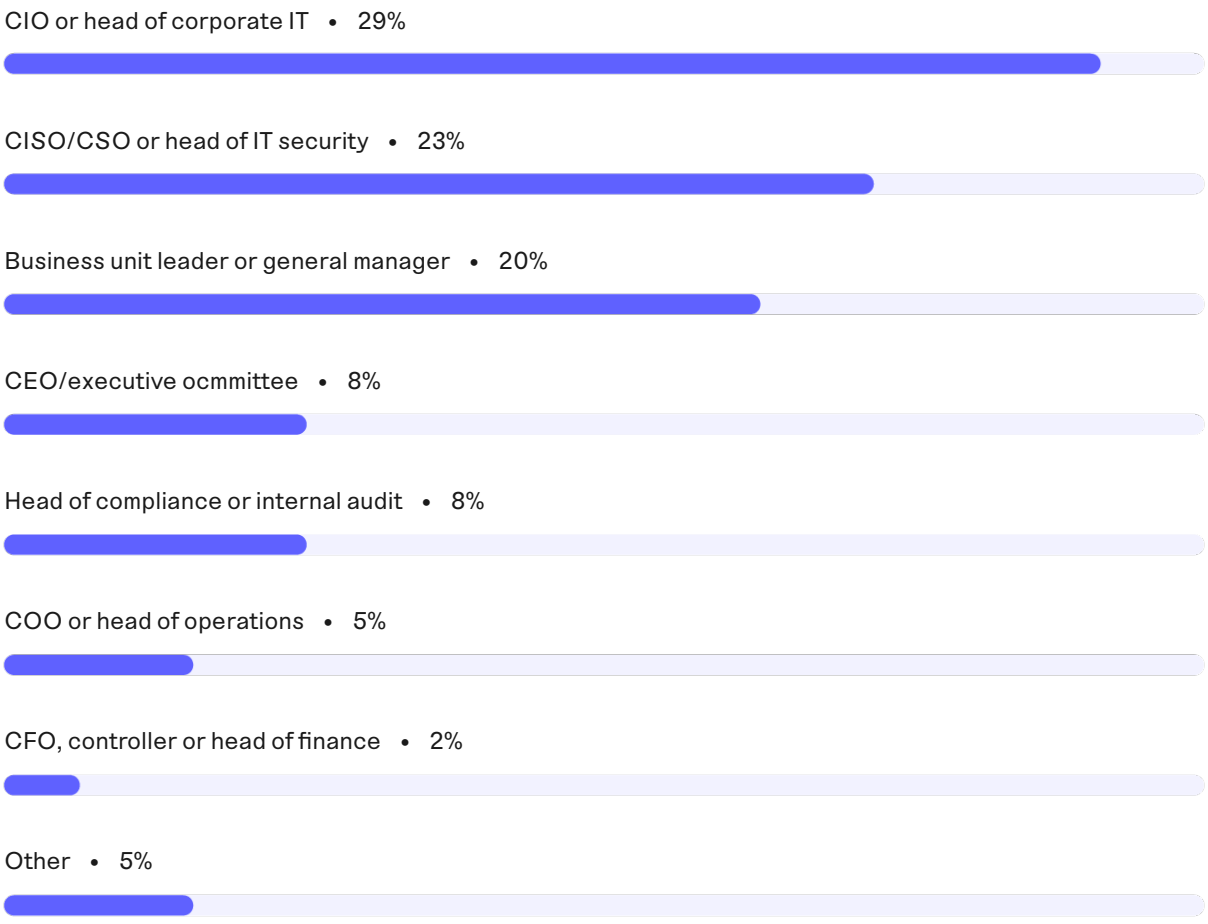


Figure 35 reports the respondent's organizational level within participating organizations. By design, more than half (69 percent) of respondents are at or above the supervisory levels. The largest category at 23 percent of respondents is supervisor.

Figure 36

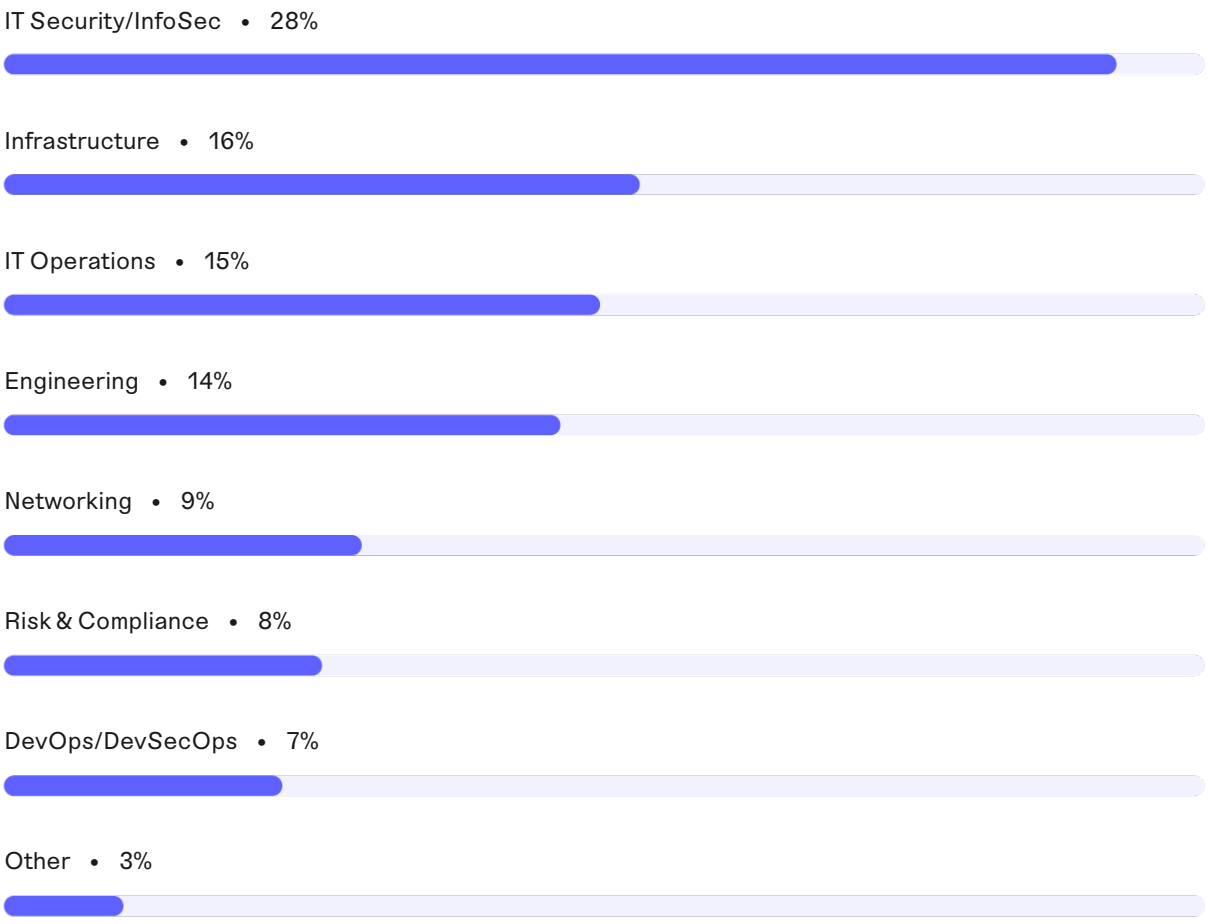
Direct reporting channel



As shown in Figure 36, 29 percent of respondents report to the CIO or head of corporate IT, 23 percent of respondents report to the CISO/CSO or head of IT security, 20 percent of respondents report to the business unit leader or general manager.

Figure 37

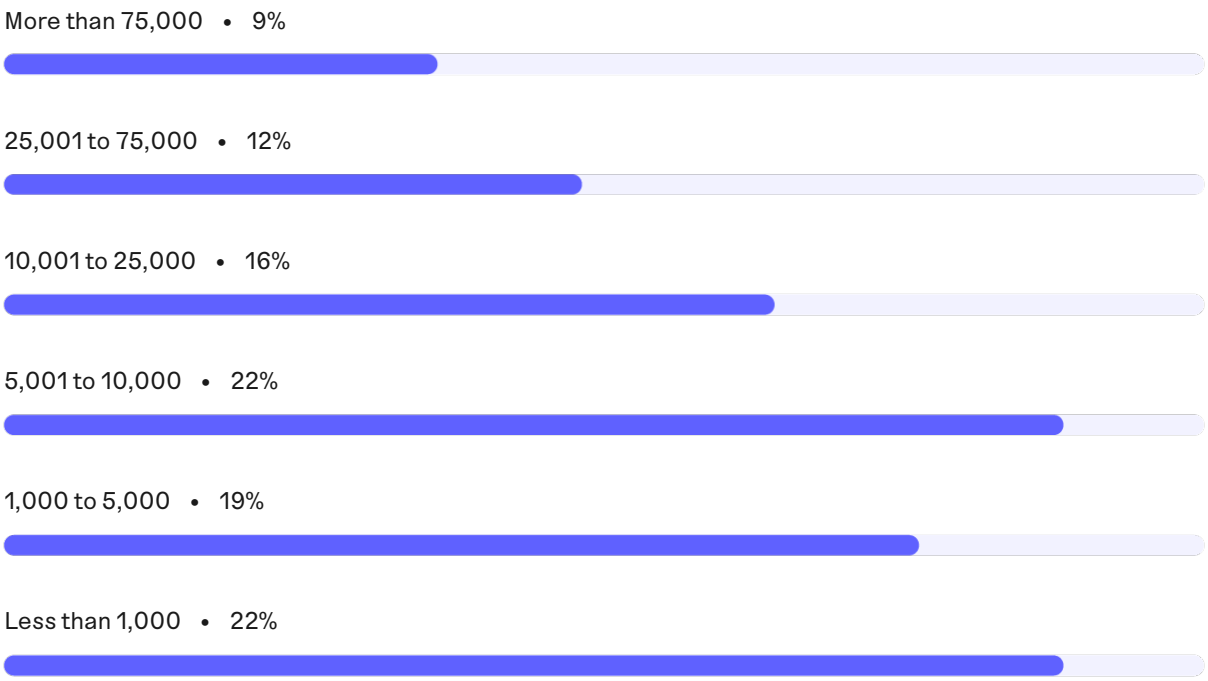
Respondents' department or team



According to Figure 37, 28 percent of respondents are located within the IT security/Info sec department. This is followed by infrastructure (16 percent of respondents), IT operations (15 percent of respondents), engineering (14 percent of respondents), and networking (9 percent of respondents).

Figure 38

Global full-time headcount



As shown in Figure 38, 59 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Figure 39

Distribution of sample by industry

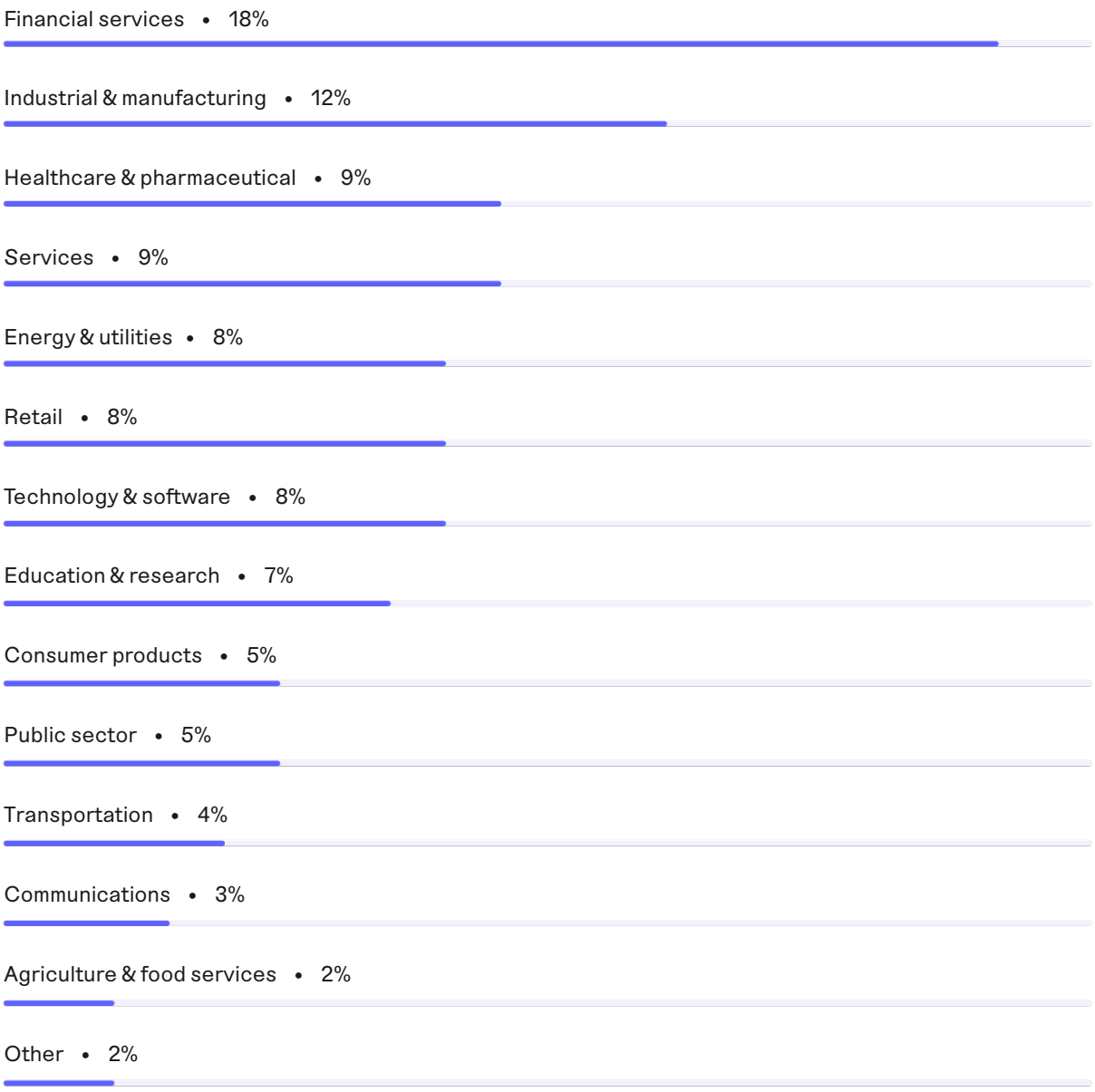


Figure 39 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial and manufacturing (12 percent of respondents), healthcare and pharmaceuticals (9 percent of respondents), services (9 percent of respondents), energy and utilities, retail and technology and software (each at 8 percent of respondents).

Limitations

There are inherent limitations to survey research that must 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 familiar with their organization's PKI. We also acknowledge that the results may be biased by external events such as media coverage. Finally, 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, there is always the possibility that a subject did not provide accurate responses.

About Ponemon Institute and Keyfactor

The 2023 State of Machine Identity Management Report was a joint effort between Ponemon Institute and Keyfactor. The research is conducted independently by Ponemon Institute, and results are sponsored, analyzed, and published by Keyfactor.

Ponemon INSTITUTE

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter, and advocate of growing a trusted, secure, diverse, and inclusive workplace.