State of Machine Identity Management 2021

Ponemon INSTITUTE

KEYFACTOR

Contents

Executive Summary

Introduction

Ponemon Institute and Keyfactor kicked off the first-ever *State of Machine Identity Management Report* with one purpose:

Drive industry awareness around the importance of managing and protecting machine identities, such as keys, certificates, and other secrets, in digital business.

For the *2021 State of Machine Identity Management Report*, Ponemon Institute surveyed 1,162 respondents across North America and EMEA who work in IT, information security, infrastructure, development, and other related areas.

We hope that IT and security leaders can use this research to drive forward the need for an enterprise-wide machine identity management strategy. No matter where you are in the business – IT, security, or development – and no matter the size of your company, this report offers important insights into why machine identities matter, and how they impact your team.

1,162
Survey respondents

12
Industries

2
Global regions

The rise of machine identities

In recent years, we've witnessed the rapid growth of internet-connected devices and machines in the enterprise. From IoT and mobile devices to software-defined applications, cloud instances, containers, and even the code running within them, machines already far outnumber humans.

Much like the human identities we rely on to access apps and devices we use every day (e.g., passwords, multi-factor, etc.), machines require a set of credentials to authenticate and securely connect with other devices and apps on the network. Despite their critical importance, these "machine identities" are often left unmanaged and unprotected.

In the 2020 Hype Cycle for Identity and Access Management Technologies, Gartner introduced a new category: Machine Identity Management. The addition reflects the increasing importance of managing cryptographic keys, X.509 certificates, SSH keys, and other non-human identities.

"This is a new profile that reflects an increased need to manage cryptographic keys, X.509 certificates and other credentials that are used to establish trust in the identities of machines, such as IoT devices, virtual machines, containers and RPA bots."

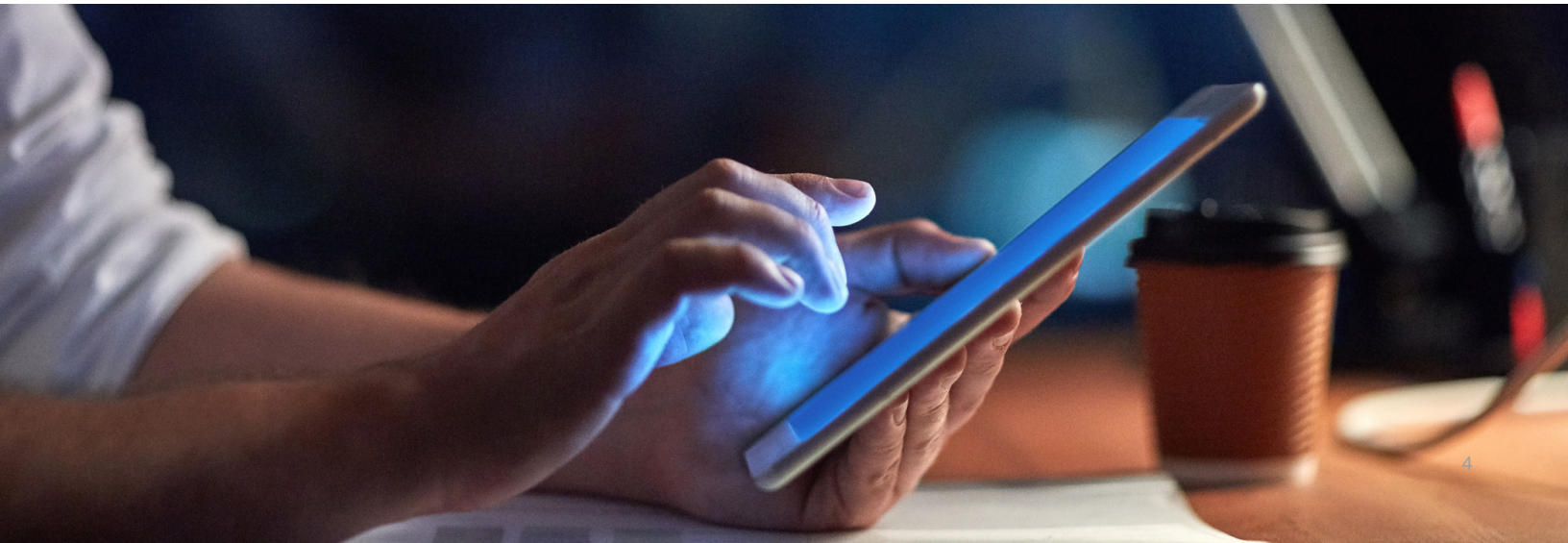
Gartner, Hype Cycle for Identity and Access Management Technologies, 2020, Ant Allen, 16 July 2020

Machine identity management is emerging as an industry-recognized term.

Machine identities have undoubtedly become a critical piece in enterprise IAM strategy, and awareness has reached even the highest levels of the organization. Sixty-one percent of respondents say they are either familiar or very familiar with the term *machine identity management*.

61%

of respondents are familiar with machine identity management



Key findings

In this section, we highlight key findings based on Keyfactor's analysis of the research data compiled by Ponemon Institute. For more in-depth analysis, see the complete findings.

Strategies for crypto and machine identity management are a work in progress.

Despite growing awareness of machine identity management, the majority of survey respondents said their organization either does not have a strategy for managing cryptography and machine identities (18 percent of respondents), or they have a limited strategy that is applied only to certain applications or use cases (42 percent of respondents).

The top challenges that stand in the way of setting an enterprise-wide strategy are too much change and uncertainty (40 percent of respondents) and lack of skilled personnel (40 percent of respondents).

40%

of companies have an enterprise-wide strategy for managing cryptography

Shorter certificate lifespans, key misconfiguration, and limited visibility are top concerns.

Challenges in managing machine identities include the increased workload and risk of outages caused by shorter SSL/TLS certificate lifespans (59 percent of respondents), misconfiguration of keys and certificates (55 percent of respondents), and not knowing exactly how many keys and certificates the organization has (53 percent of respondents).

A significant driver of these challenges is the recent reduction in the lifespan of all publicly-trusted SSL/TLS certificates by roughly half, from 27 months to 13 months, on September 1, 2020. It is worth noting that the real impact of this change will likely not be realized until the months and years ahead.

61%

of companies are deploying more cryptographic keys and digital certificates

1/2

of respondents say crypto-agility is a top strategy priority

1. Cloud-based services
2. Zero Trust strategies
3. Remote workforce
4. IoT devices
5. DevOps/DevSecOps
6. Mobile devices
7. Regulatory requirements

Crypto-agility emerged as a top strategic priority.

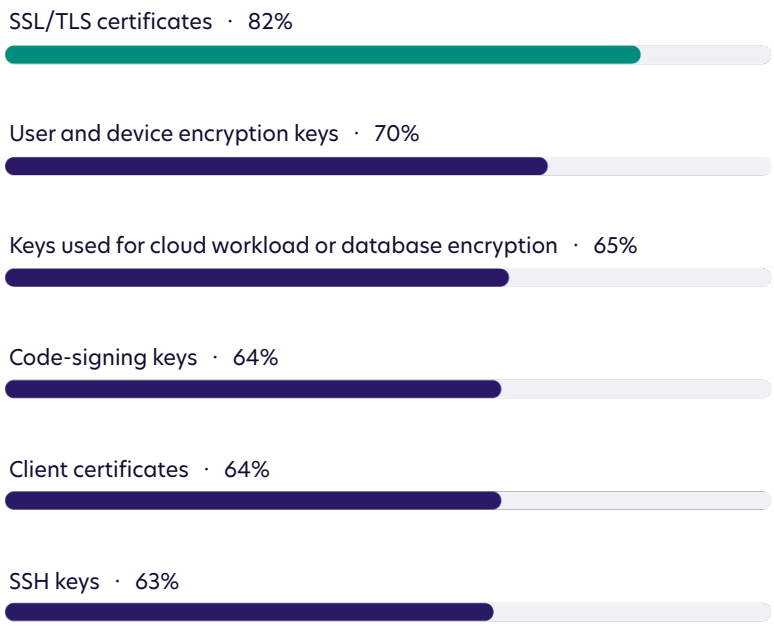
Moving into the top position on the list, more than half of respondents (51 percent) identified crypto-agility as a strategic priority for digital security, followed by reducing complexity of IT infrastructure and investing in hiring and retaining qualified personnel (both 50 percent of respondents).

Cloud and Zero-Trust strategies are driving the deployment of PKI and machine identities.

While many trends are driving the deployment of PKI, keys, and certificates, the two most important trends are cloud-based services (52 percent of respondents), and Zero-Trust security strategy (50 percent of respondents). Other notable trends include the remote workforce and IoT devices (both 43 percent of respondents).

SSL/TLS certificates take priority, but every machine identity is critical.

Overall, respondents agree that managing and protecting every machine identity is critical. That said, SSL/TLS certificates were widely considered the most important machine identities to manage and protect, according to 82 percent of respondents.



Only

45%

of companies have enough staff dedicated to their PKI

PKI deployments are everywhere — most are understaffed.

The most common method for deploying enterprise PKI is an internal privately-rooted certificate authority (CA) (42 percent of respondents). However, many organizations also leverage built-in issuing CAs such as Kubernetes or HashiCorp Vault (29 percent of respondents), private CAs running in a public cloud (23 percent of respondents), and externally-hosted managed PKI services (23 percent of respondents).

40%

say they still use spreadsheets to track certificates

Most organizations still rely on spreadsheets and CA-provided tools to track certificates.

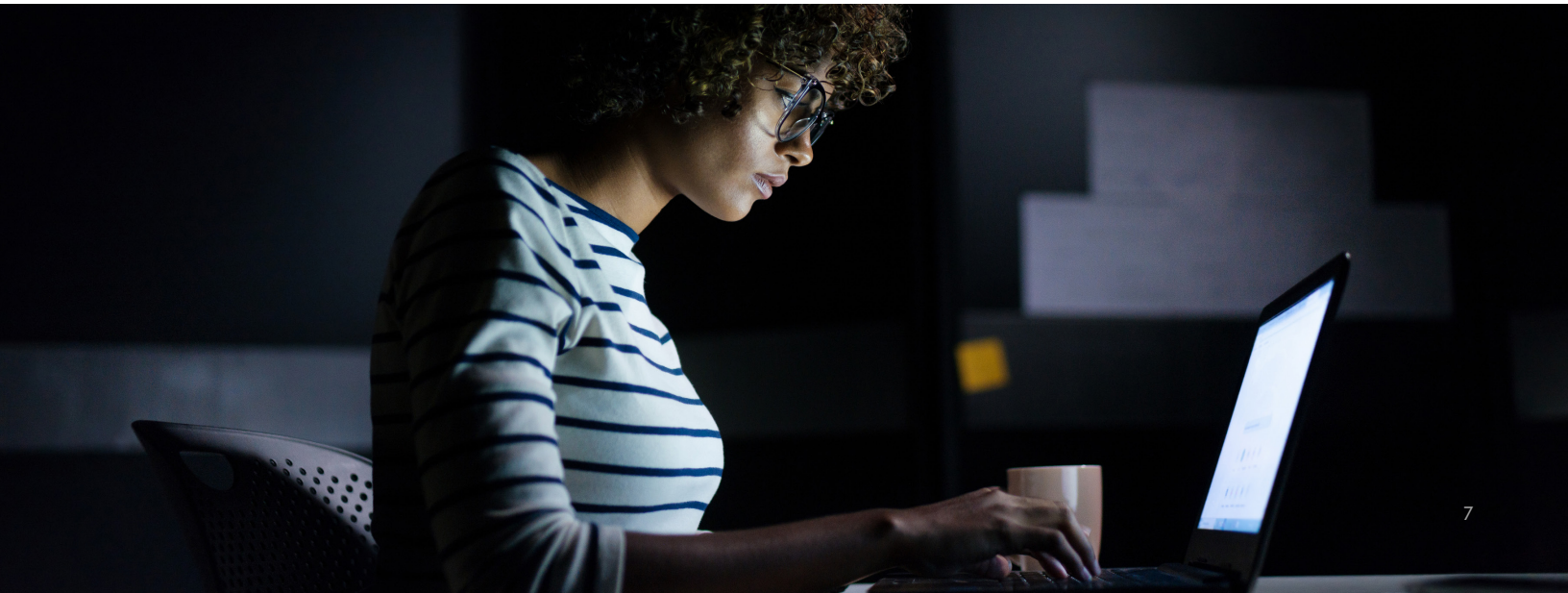
Despite the increasing volume of machine identities, many organizations still rely on a patchwork of CA vendor-provided tools (44 percent of respondents), spreadsheets (40 percent of respondents), and in-house built solutions (33 percent of respondents) to manage digital certificates. Only about one-third (36 percent of respondents) use a dedicated certificate lifecycle management solution.

3.1

The average number of outages in companies caused by expired certificates in the past two years

Disruptive certificate outages are widespread and likely to increase.

Eighty-eight percent of organizations reported experiencing at least one unplanned outage due to expired certificates in the past 24 months. Another 41 percent report experiencing four or more outages. According to respondents, the likelihood of these unplanned outages occurring in the next 24 months is 40 percent, up from just 25 percent in the 2020 study.



57%

say they do not have an accurate inventory of SSH keys

SSH credentials are frequently overlooked and unmanaged.

According to the findings, SSH credentials, such as passwords, keys, and certificates, are widely used by organizations. However, 53 percent have no centralized management process, leaving administrators to manage their own credentials. As a result, less than half of organizations have an accurate inventory of SSH credentials across their infrastructure (40 percent of respondents).

25

The average number of code signing keys used within organizations

Code signing keys are still found on build servers and developer workstations.

Almost half (48 percent) of respondents rank the importance and risk associated with code-signing keys as very high. However, only 36 percent of respondents say their organization has formal access controls and approval processes for code signing. Many still report that these sensitive code-signing keys are stored on build servers (33 percent of respondents) and developer workstations (19 percent of respondents).

4.9

The average number of failed audits due to insufficient key management in the past 2 years

Failed audits are all too common.

Compared to other machine identity-related incidents, such as unplanned certificate outages or theft and misuse of keys and certificates, audit failures are considered the most frequent and serious, according to 75 percent of respondents. On average, organizations experienced approximately five failed audits or compliance incidents due to insufficient key management within the past 24 months.

Complete findings

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

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

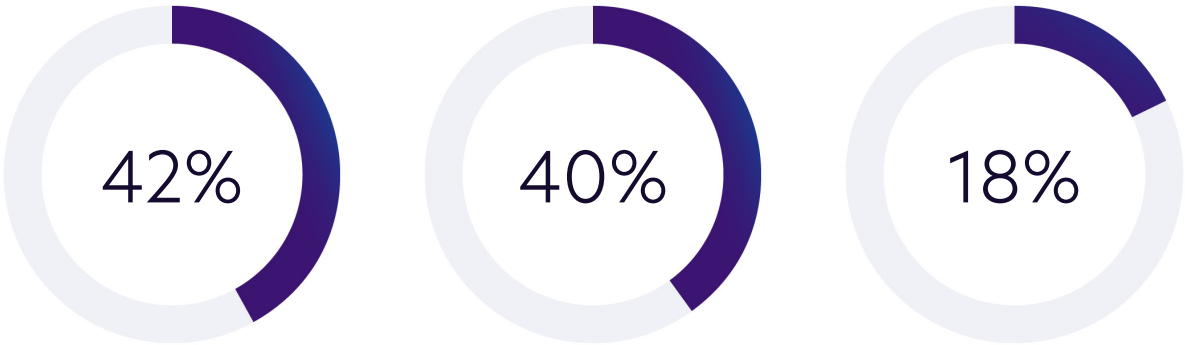
Trends in cryptography and machine identity management

Enterprise-wide cryptography strategies are a work in progress. As shown in Figure 1, 42 percent of respondents say their organizations have a limited crypto-management strategy that is applied to certain applications or use cases, while 40 percent say their organization already has an enterprise-wide strategy for cryptography/machine identity management.

Figure 1.

Does your organization have an enterprise-wide strategy for managing cryptography?

Strongly agree and agree responses combined.

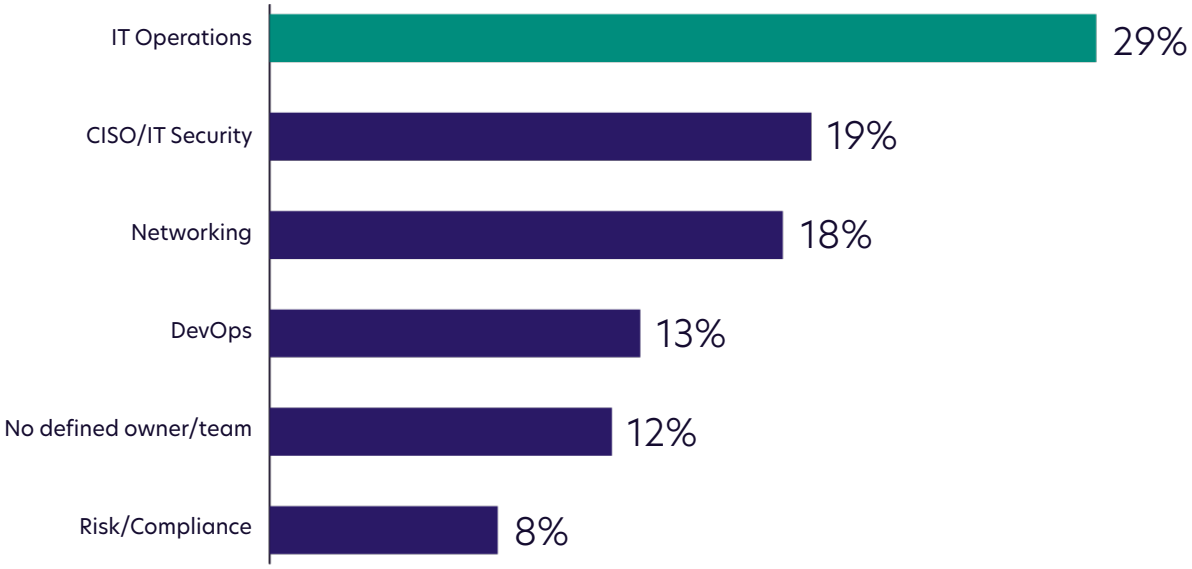


IT operations is leading cryptography strategy. Figure 2 shows that IT operations (29 percent of respondents), CISO/IT Security (19 percent of respondents), and Networking (18 percent of respondents) are the most common functions responsible for their organizations' cryptography strategy.

A possible reason why IT operations is more influential than IT security in many organizations is because of the growing adoption of PKI and cryptography, the proliferation of DevOps and cloud-native tools that use machine identities, or the general consumerization of IT.

Figure 2.

Who is responsible for enterprise cryptography strategy?

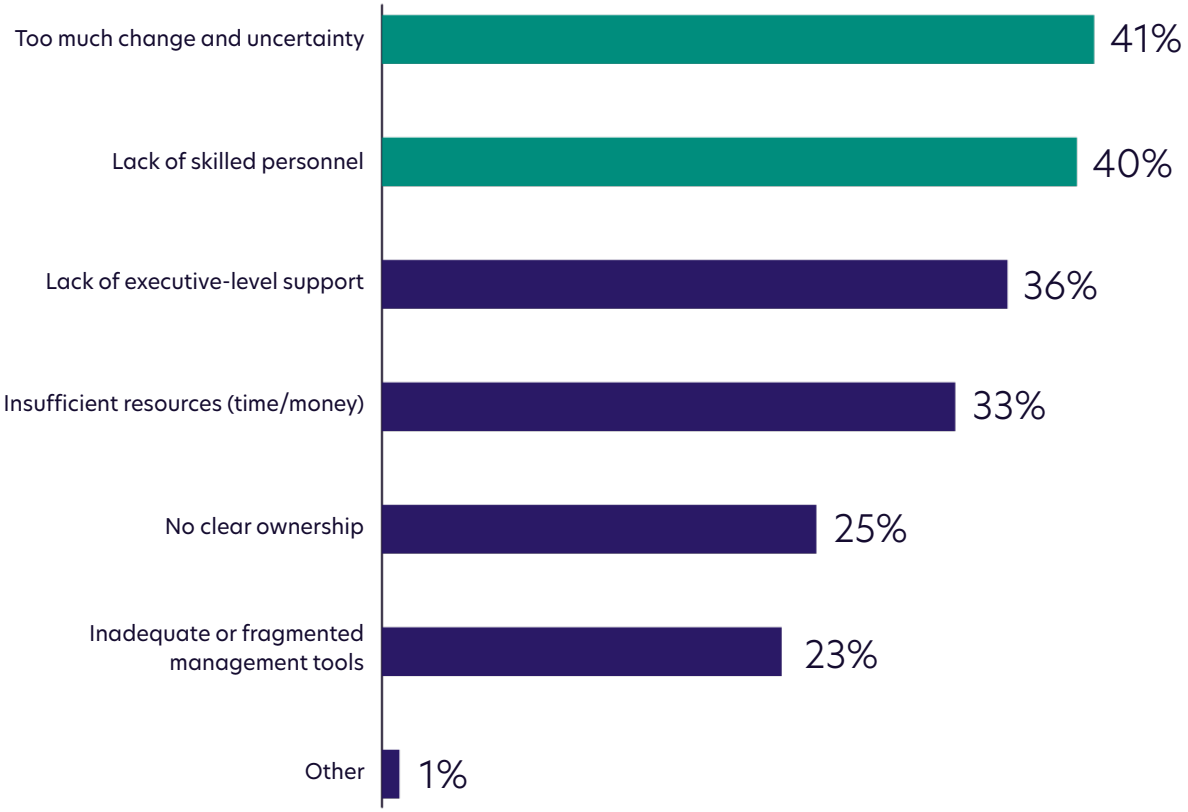


Uncertainty and lack of skilled personnel are barriers to success. The top two challenges in setting an enterprise-wide cryptography or machine identity management strategy are too much change and uncertainty (40 percent of respondents) and lack of skilled personnel (40 percent of respondents), as shown in Figure 3.

Figure 3.

Biggest challenges in setting an enterprise-wide machine identity management strategy

Two responses permitted

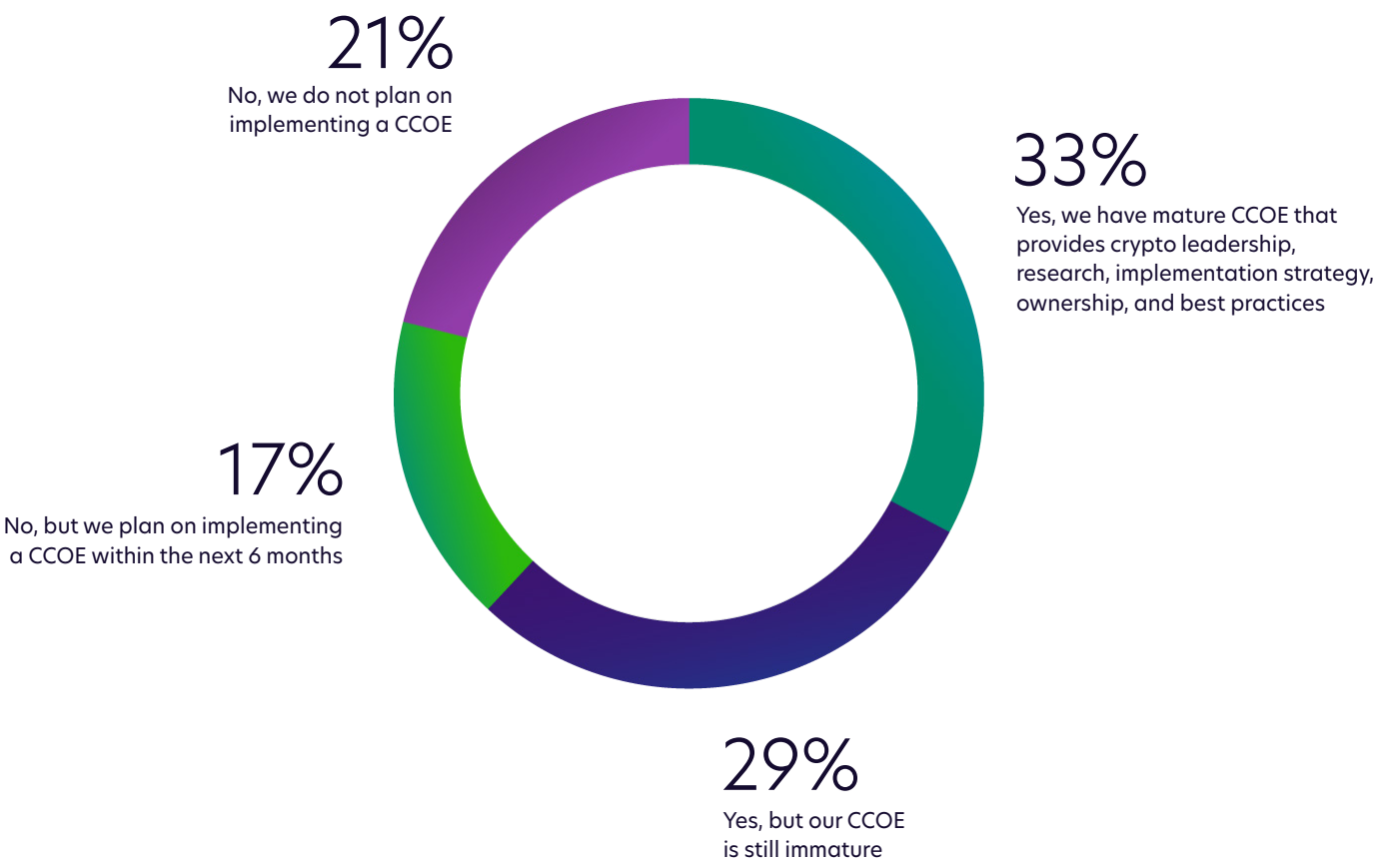


One-third of organizations have a mature CCoE. A cryptographic center of excellence (CCoE) is intended to support the direction and implementation of an enterprise-wide cryptography strategy. A CCoE does not necessarily own and operate all the necessary tools, but rather it serves as a center for policy, governance and best practices.

According to Figure 4, one-third of respondents say their organization has a mature CCoE. Another 29 percent of respondents have a CCoE, but it is still immature.

Figure 4.

Has your organization implemented a Crypto Center of Excellence (CCoE)?



Crypto-agility emerged as a top strategic priority. Figure 5 provides a list of nine strategic priorities for digital security. We asked respondents to indicate the three most important priorities for their organization this year.

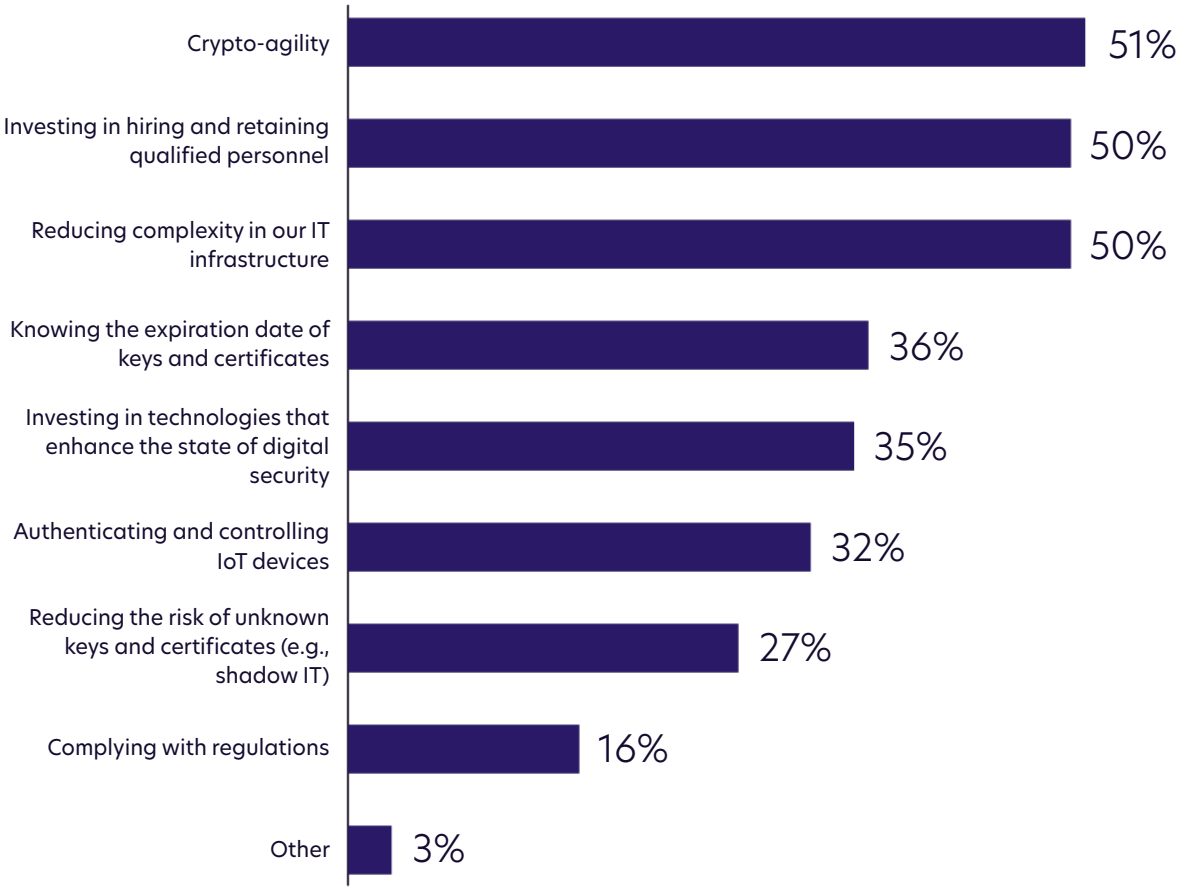
Fifty-one percent of respondents say that crypto-agility is a strategic priority for their organization, followed by investing in hiring and retaining qualified personnel and reducing complexity in our IT infrastructure (both 50 percent of respondents).

It is not surprising that organizations are focused on crypto-agility and investing in hiring and retaining qualified personnel, considering *too much change and uncertainty* and *lack of skilled personnel* were the two biggest challenges identified by respondents (see Figure 3).

Figure 5.

Strategic priorities for digital security within their organization

Three responses permitted.



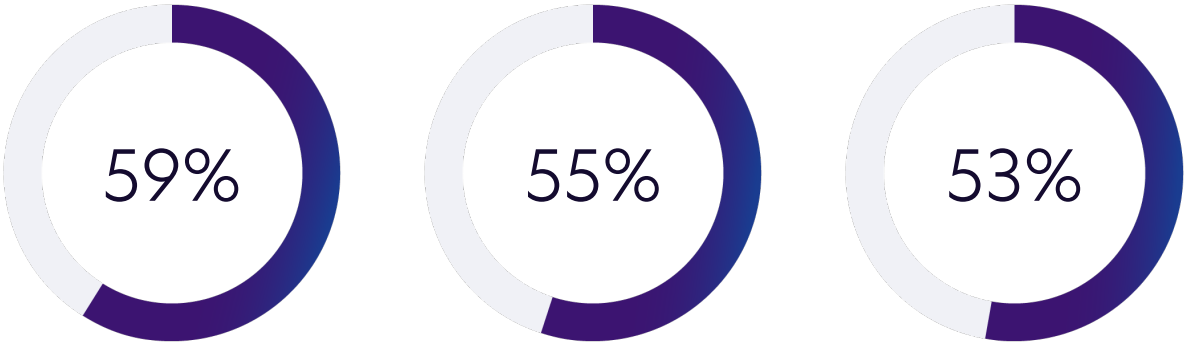
Most respondents say they are concerned about their ability to manage machine identities. As shown in Figure 6, more than half of respondents (59 percent) say they are concerned about shorter SSL/TLS certificate lifespans increasing the workload and risk of outages.

Nearly as many respondents report concerns about misconfiguration of keys and certificates (55 percent) and not knowing how many keys and certificates (including self-signed) their organization has (53 percent).

Figure 6.

Perceptions and concerns about managing machine identities

Strongly agree and agree responses combined.



My organization is concerned about the increased workload and risk of outages caused by shorter SSL/TLS certificate lifespans.

My organization is concerned about the increasing risk of misconfiguration of keys and certificates.

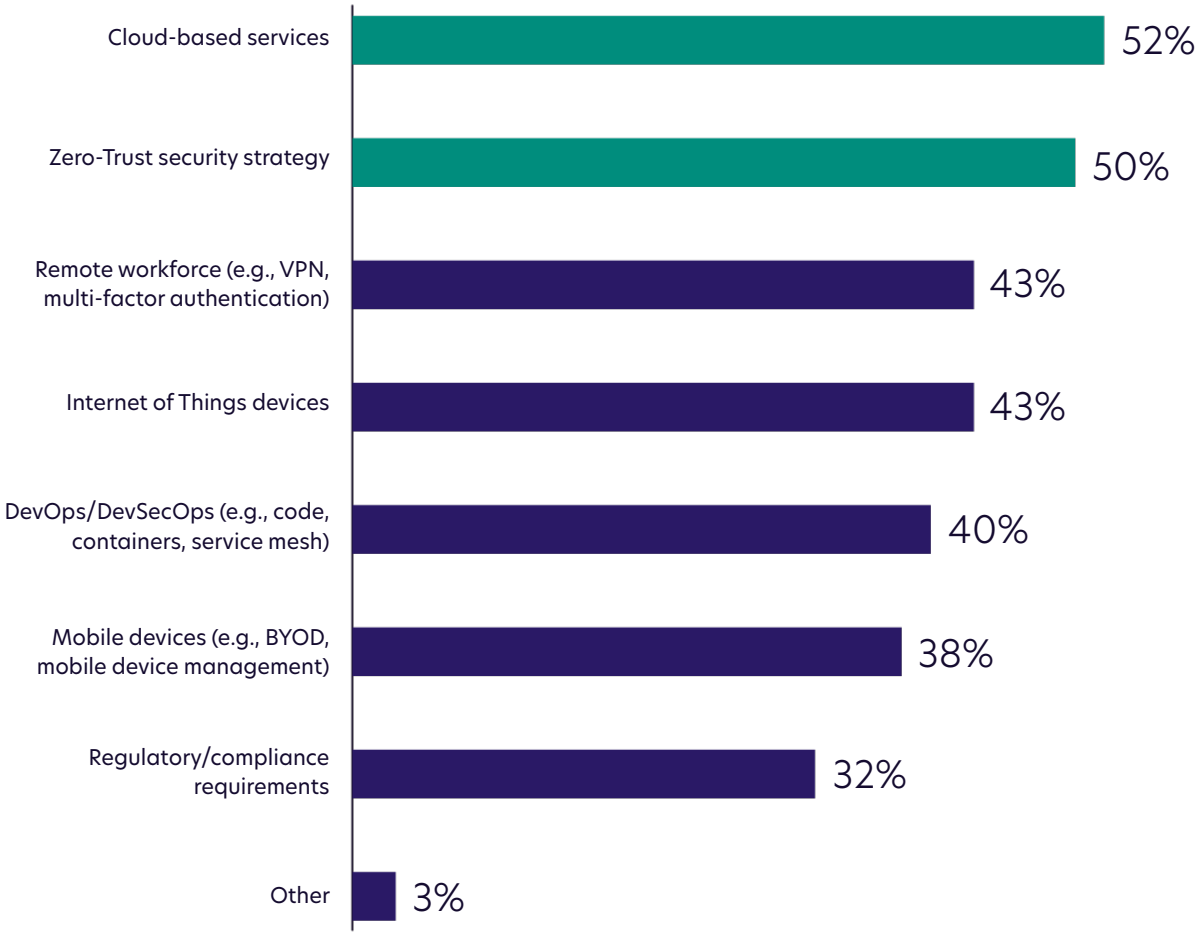
My organization does not know how many keys and certificates (including self-signed) it has.

Cloud and Zero-Trust are driving the use of PKI and machine identity. Fifty-two percent of respondents say that cloud-based services are driving deployment of PKI, keys, certificates and other secrets. Another 50 percent say of respondents say Zero-Trust strategies are an important trend. Other trends include the remote workforce (e.g., VPN, MFA), IoT devices and DevOps (e.g., code, containers, service mesh).

Figure 7.

The most important trends driving the deployment of PKI, keys, certificates and secrets

Three responses permitted.



Most respondents agree that every machine identity is important. Respondents were asked to rate the importance of managing and protecting different types of machine identities on a ten-point scale from 1 (not important) to 10 (very important).

As seen in Figure 8, 82 percent of respondents say that managing and protecting SSL/TLS certificates is important or very important, followed by user and device encryption keys (70 percent of respondents), and keys used for cloud workload or database encryption (65 percent). Machine identities considered least important include code signing keys, client certificates, and SSH keys.

There are many possible reasons why certain machine identities are considered more important than others — no clear ownership, lack of security oversight, etc. However, the majority of respondents consider every machine identity important to manage and protect.

Figure 8.

The importance of managing and protecting machine identities

On a scale from 1 = not important to 10 = very important. 7+ responses combined.

PKI and certificate management practices

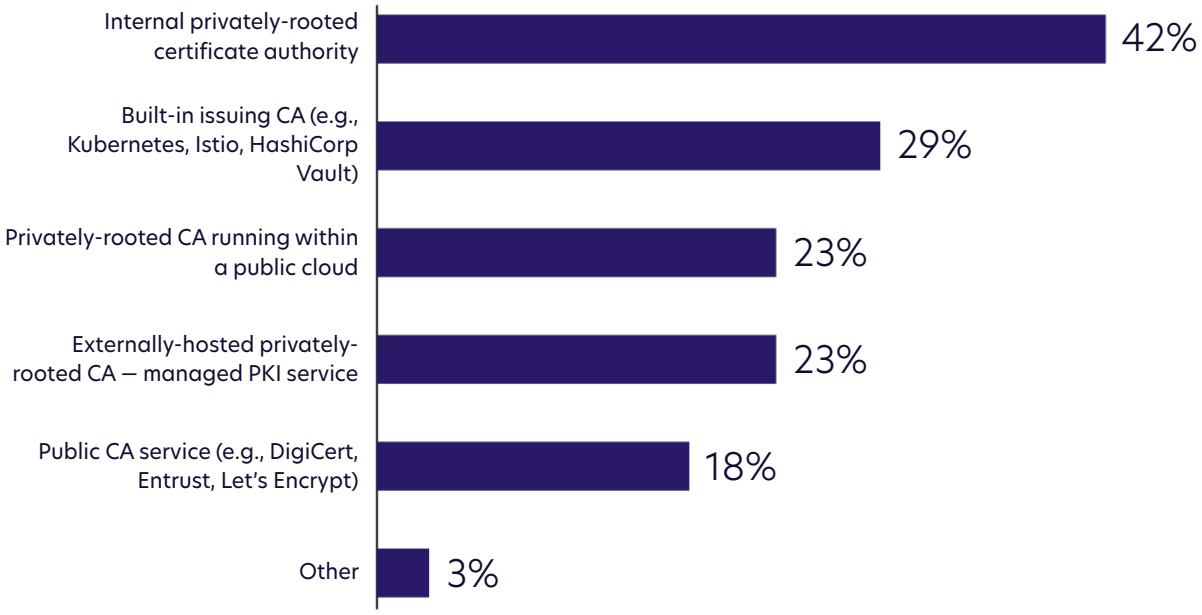
PKI deployments are everywhere. Respondents were asked to describe their organization's PKI deployment. The most common method for deploying enterprise PKI, according to Figure 9, is using an internal privately-rooted certificate authority (CA). Other popular deployments for PKI include using a built-in issuing CA (e.g., Kuberentes, Istio, HashiCorp Vault, etc.) or a private CA running within a public cloud.

One in four respondents (23 percent) say their organization utilizes an externally-hosted managed PKI service. Many respondents may not consider public CA services as a component of their organizations' PKI, even if they procure certificates from a third-party CA vendor.

Figure 9.

How would you describe your organization's PKI deployment?

More than one response permitted.



Most respondents say their PKI is understaffed. Public key infrastructure (PKI) often requires significant effort and expense to deploy and operate adequately. Figure 10 shows that organizations represented in this study have an average of six employees involved in their PKI deployment. However, as seen in Figure 11, most respondents (55 percent) say they do not have sufficient IT security staff dedicated to their PKI deployment.

Figure 10.

How many full-time employees are involved in your PKI deployment?

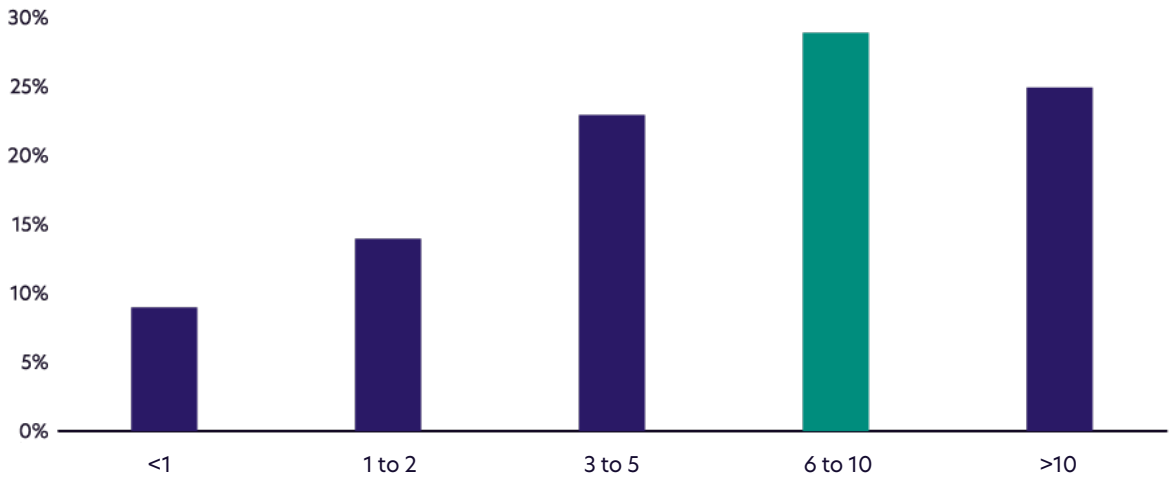


Figure 11.

In your opinion, does your organization have enough IT security staff dedicated to PKI?

How are digital certificates managed? It's not uncommon for organizations to rely on an inefficient patchwork of spreadsheets, certificate authority (CA)-specific tools, and homegrown solutions to track and manage their certificates.

As shown in Figure 12, many respondents say their organizations use multiple tools, including CA vendor-provided tools (44 percent), spreadsheets (40 percent), and in-house built solutions (33 percent). Only about one-third (36 percent) say they use a dedicated certificate lifecycle management solution.

Figure 12.

How does your organization manage its certificates?

More than one response permitted.

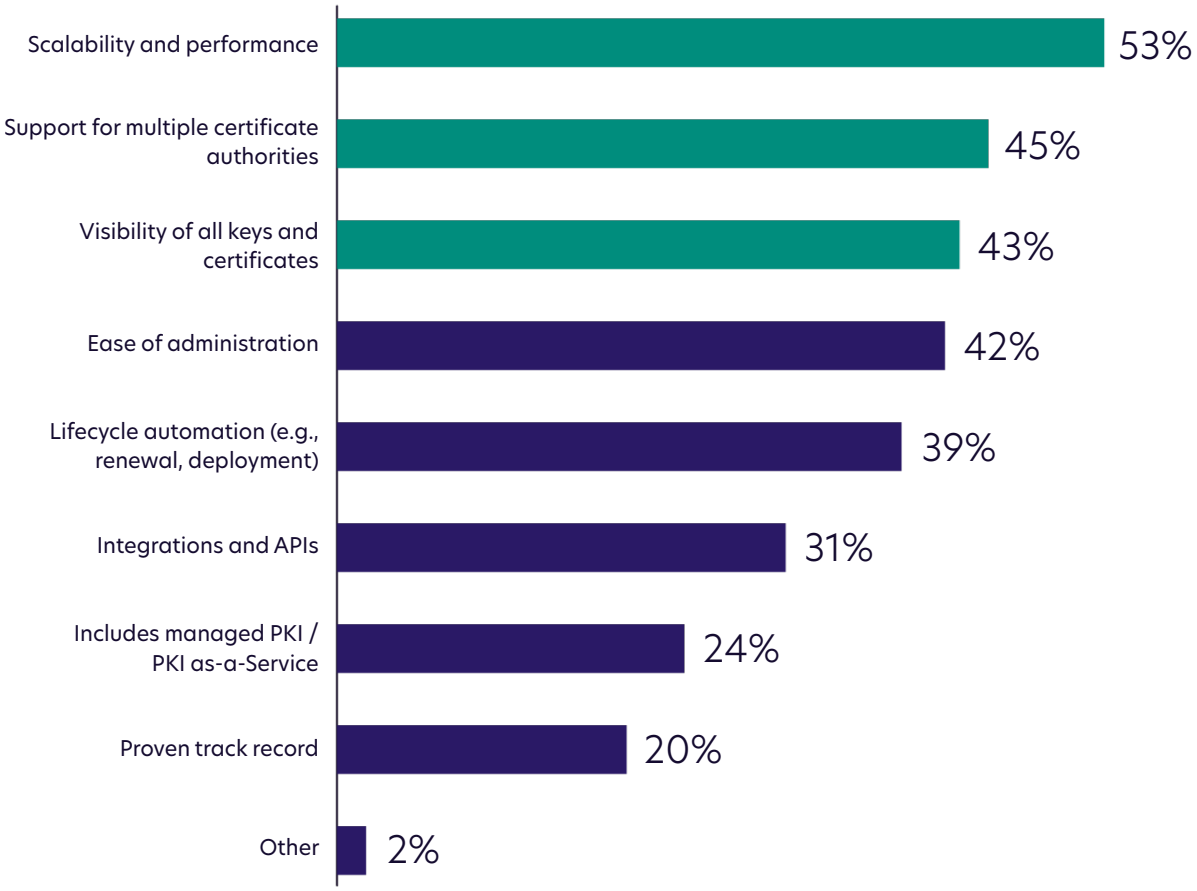
Scalability and performance is essential to PKI and certificate management. Figure 13 lists 9 features or capabilities of PKI and certificate management solutions. We asked respondents to indicate the three most important features when considering a dedicated PKI and certificate management solution for their organization.

The top three features considered important include: (1) Scalability and performance, (2) Support for multiple certificate authorities, and (3) Visibility of all keys and certificates. The importance of scalability and performance is not surprising, considering the increasing volume and velocity of certificate issuance in dynamic IT environments.

Figure 13.

The most important features in choosing a PKI and certificate management solution

Three responses permitted.



SSH key management practices

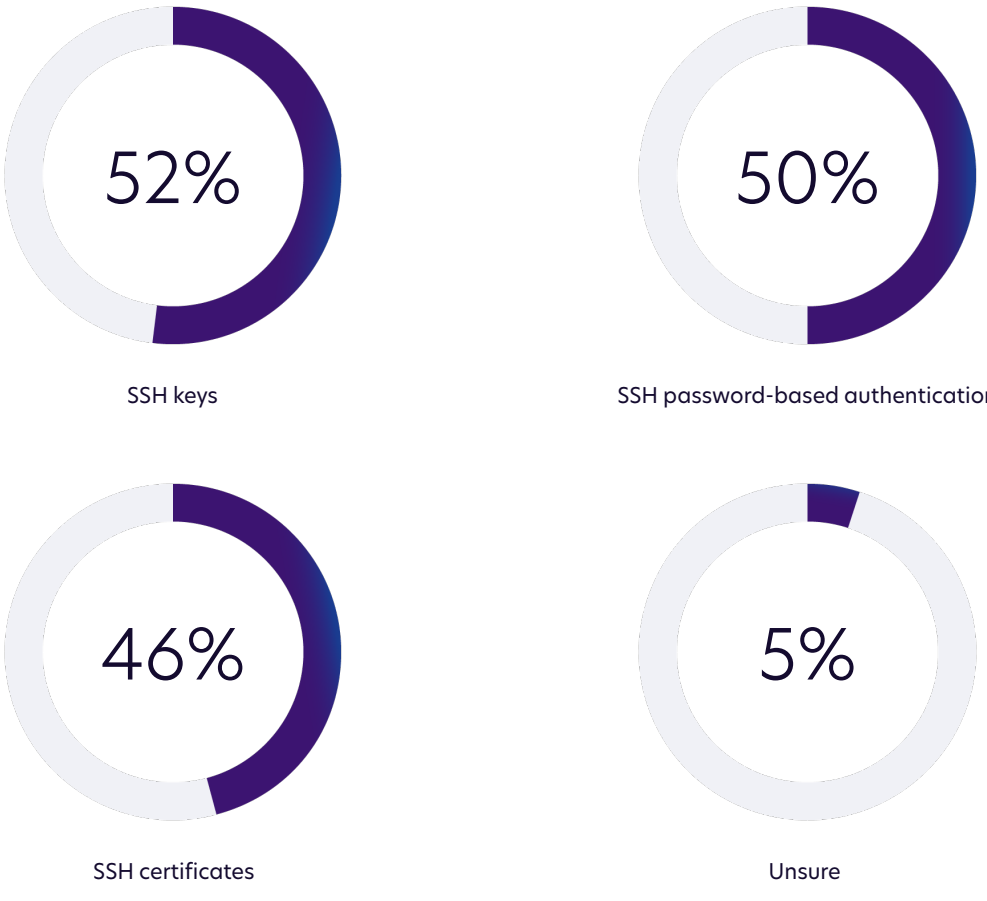
In this section, we asked respondents how familiar they are with their organizations' use of SSH credentials. Responses from individuals who said they are not familiar were excluded from the following analysis.

There is no "one way" to SSH. Eighty-four percent of the overall survey respondents (976) say they are at least somewhat familiar with their organization's use of SSH credentials. Of those respondents, 52 percent say that their organization uses SSH keys for authentication. Nearly as many respondents say they use SSH password-based authentication (50 percent) or SSH certificates (46 percent) for authentication.

Figure 14.

Which SSH credentials are used in your organization?

More than one response permitted.

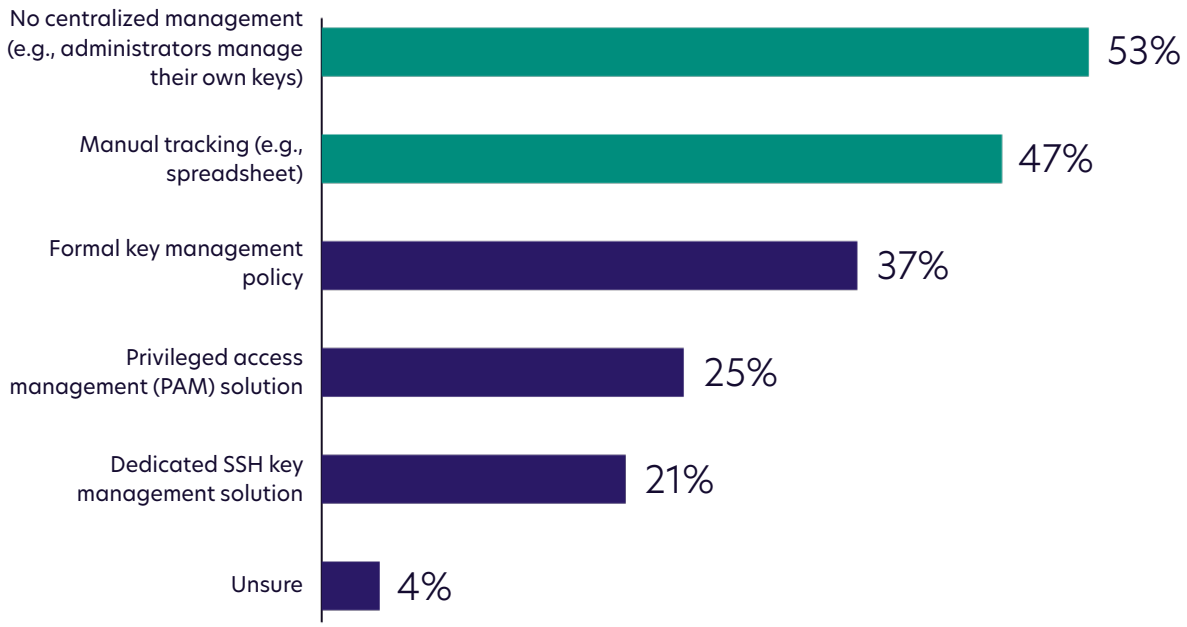


How are SSH credentials managed? Fifty-three percent of respondents say their organization has no centralized management, leaving administrators to manage their own credentials. Another 47 percent of respondents say they use some form of manual tracking, such as spreadsheets (see Figure 15). Some organizations use a dedicated technology solution to manage SSH credentials, such as a privileged access management (PAM) solution (25 percent of respondents) or a dedicated SSH key management solution (21 percent of respondents).

Figure 15.

How does your organization manage SSH credentials?

More than one response permitted.



SSH credentials are largely 'invisible'. SSH passwords, keys and certificates are widely used by administrators, but without centralized management, most respondents (59 percent) say they do not have an accurate inventory or they are unsure (see Figure 16).

According to Figure 17, 50 percent of respondents say their organizations' rotate SSH credentials regularly (at least annually), according to best practice. Roughly one in four respondents (26 percent) say their organization never rotates SSH credentials.

Figure 16.

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

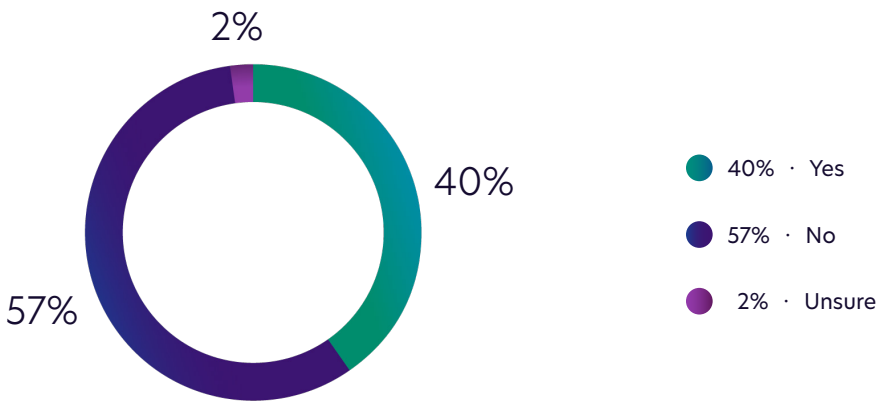
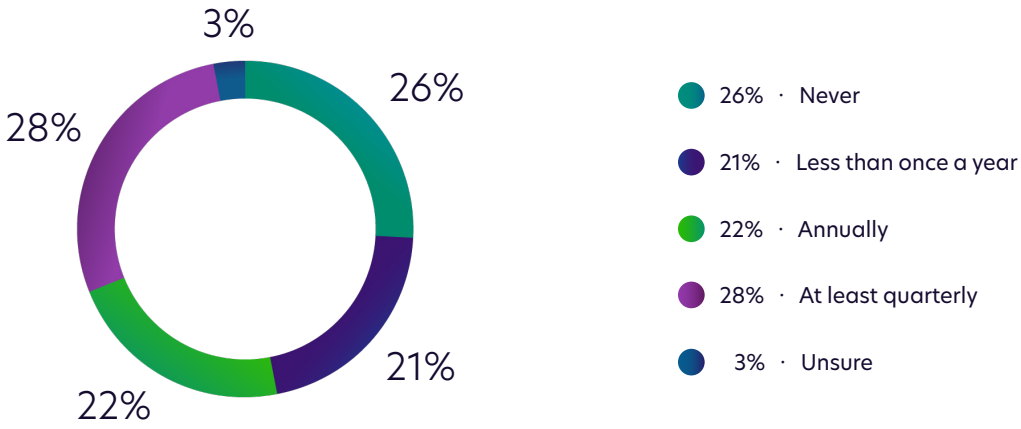


Figure 17.

How often does your organization rotate SSH credentials?



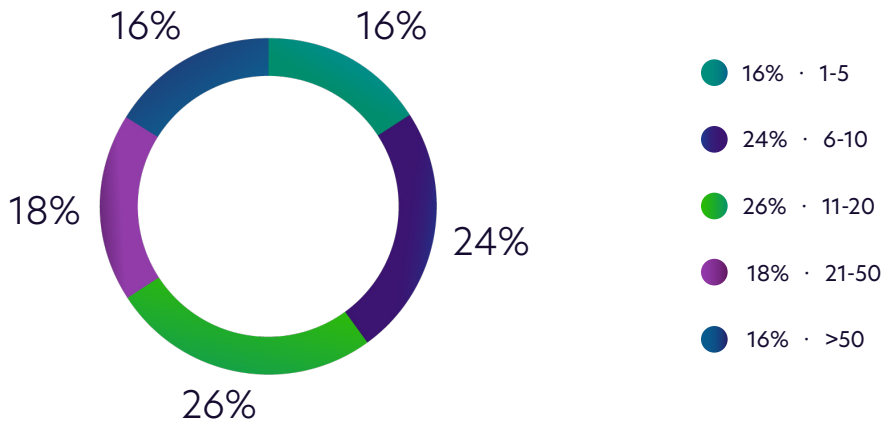
Code signing security practices

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.

Forty-five percent of the overall survey respondents (523) are involved in code signing operations. Of those respondents, 60 percent say their organization has more than 10 code signing certificates in use (see Figure 18). On average, organizations have 25 code signing certificates.

Figure 18.

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



Code-signing keys are still found on build servers and developer workstations. Hardware security modules (HSMs) and smartcards or secure USBs are most often used to store private keys used for code signing, as seen in Figure 19. However, many respondents report that code-signing keys are still stored on build servers (22 percent) and developer workstations (19 percent).

Figure 19.

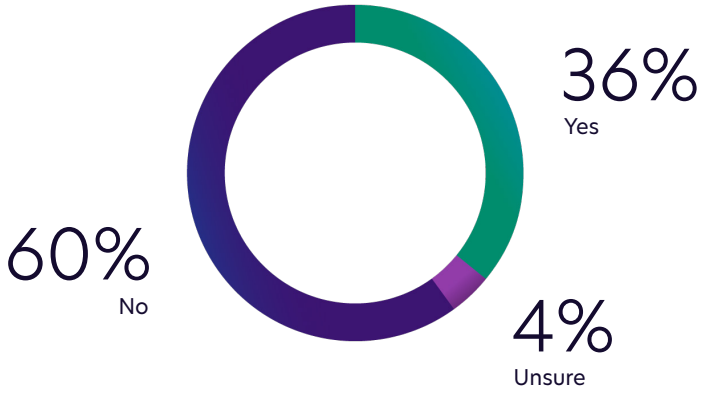
Where are code-signing keys stored in your organization?

More than one response permitted.

Most organizations have inadequate code-signing access controls. In addition to protecting and securely storing code-signing keys, access controls and workflows are essential to prevent unauthorized signing. According to Figure 20, only 36 percent of organizations have a formal access control and approval process in place for code-signing keys.

Figure 20.

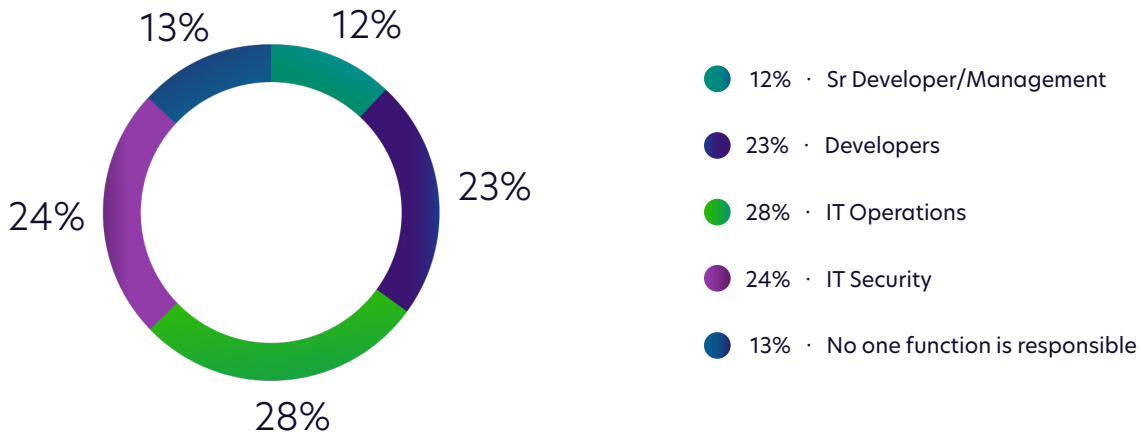
Does your organization have a formal access control and approval process for code-signing keys?



Responsibility for managing and protecting code-signing keys varies. Respondents were asked who in their organization is responsible for the management and protection of code-signing keys. As seen in Figure 21, the three most common functions responsible for this role include IT operations (28 percent), IT security (24 percent), and developers (23 percent).

Figure 21.

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

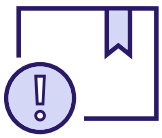


Complete findings

The impact of outages, key misuse, and failed audits

With the rapid growth of cryptographic keys and digital certificates across enterprises, the risk of machine identity-related incidents is on the rise. Without the right tools and processes, security and risk leaders often feel they are not in control.

In this section, we analyze the frequency, seriousness, and impact of three common incidents that result from mismanaged machine identities, including:



Certificate Outages

Applications, services, or websites fail due to expired or misconfigured digital certificates.

Key misuse or theft

Malicious actors misuse keys and certificates to impersonate trust or gain unauthorized access.

Audit failure

An audit failure results from insufficient key and certificate management practices.

Failed audits are the leading cause for concern. Respondents were asked to rate the seriousness and financial impact of each incident on a scale from 1 (not serious/no impact) to 10 (very serious/high impact). Figure 22 shows very serious/high impact responses (7+ responses on the 10-point scale).

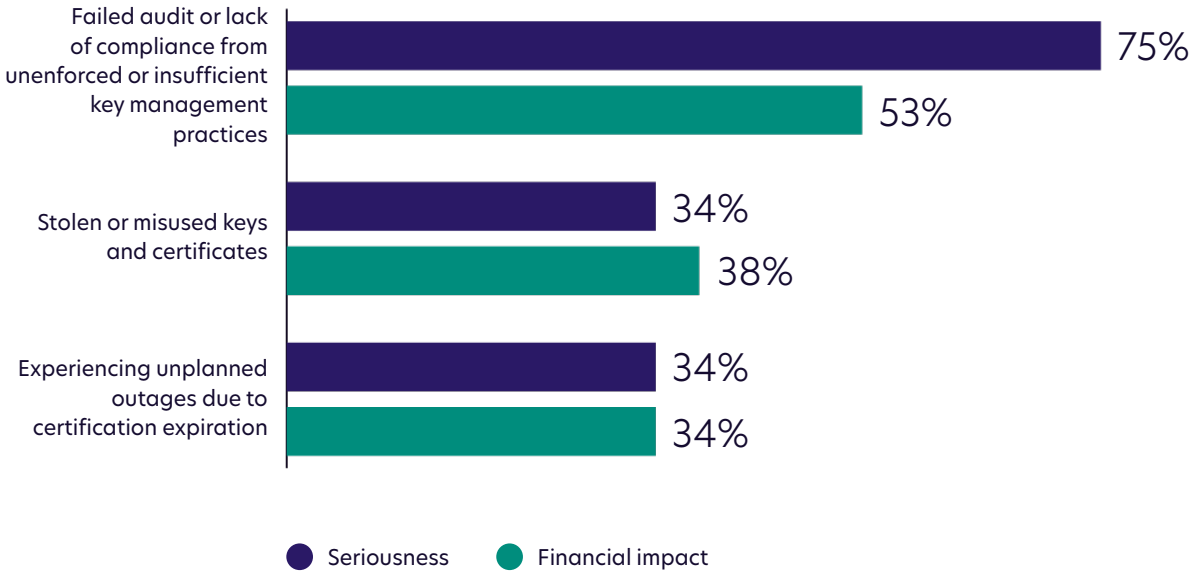
Seventy-five percent of respondents say the most serious incident would be caused by a failed audit or lack of compliance from unenforced or insufficient key management policies, and 53 percent rate the financial impact as very serious.

The perceived seriousness and financial impact of incidents caused by unexpected certificate expiration or stolen or misused keys and certificates are comparatively much lower. About one-third of respondents consider these incidents to be very serious (both 34 percent of respondents).

Figure 22.

The seriousness and financial impact of machine identity-related incidents

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

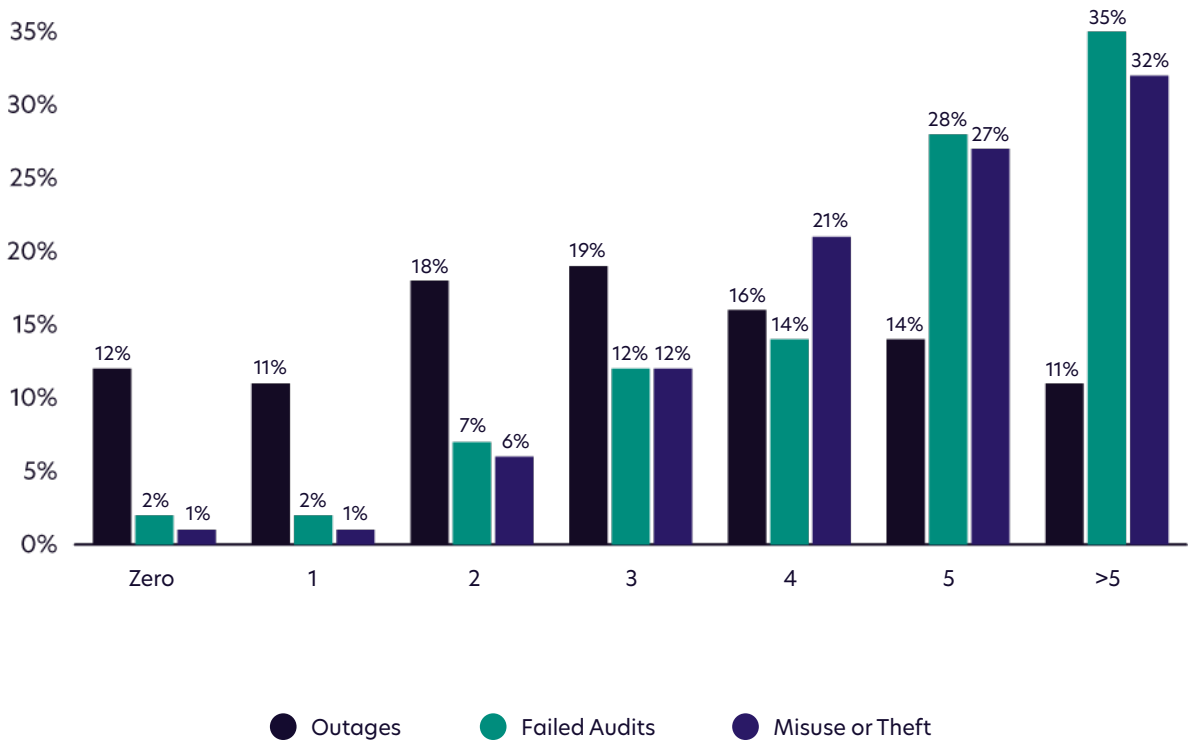


Failed audits and theft or misuse of keys and certificates are the most frequent threats. Respondents were asked to estimate the number of times each incident has occurred within the past 24 months. As shown in Figure 23, the two most frequently experienced incidents within the past 24 months were failed audits and key misuse or theft.

Organizations experienced an average of 4.94 failed audits due to insufficient key management, 4.92 incidents involving the theft or misuse of keys and certificates, and 3.10 unplanned outages due to unexpected certificate expiration.

Figure 23.

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



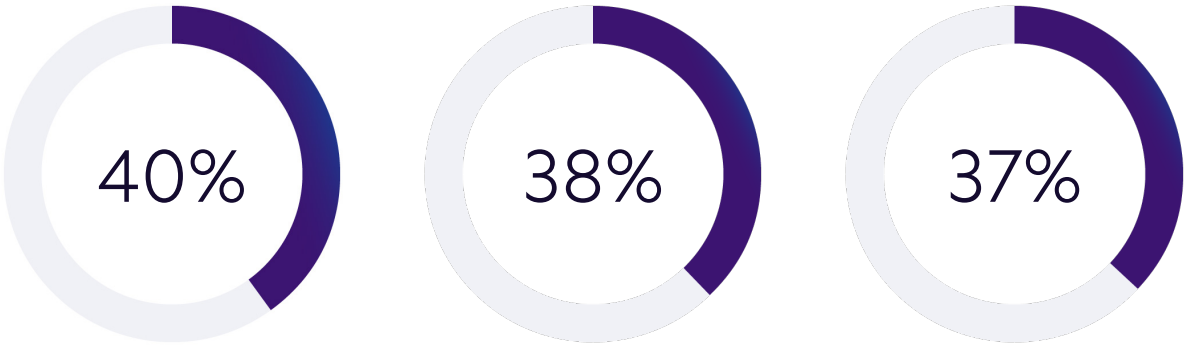
Certificate-related outages most likely to occur in the next 24 months. The expected likelihood that these incidents will occur again is shown in Figure 24. Unplanned outages due to certificate expiration were rated the most likely incident to occur within the next 24 months.

On average, respondents indicated a 37 percent likelihood of a failed audit, 38 percent likelihood that keys or certificates will be stolen or misused, and 40 percent likelihood of unplanned outages due to certificate expiration.

Figure 24.

The likelihood the incident will occur again

Extrapolated values presented.



Unplanned outage due to certificate expiration

Stolen or misused keys and certificates

Failed audit or lack of compliance from unenforced or insufficient key management policies

4 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 a Crypto Center of Excellence (CCoE) for your organization.

In the study, only one-third of organizations identified a mature crypto center of excellence (CCoE) in their business. Technology is an obvious ingredient in machine identity management. However, the proper implementation of 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 toolset to help improve security and automate processes.

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

Use best practices established by your CCoE 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

Build crypto-agility into your incident response plans.

In the report, respondents identified crypto-agility as a leading strategic priority for digital security. Algorithms evolve, certificates expire, and with the advent of quantum computing, the threat of sudden and unpredictable crypto-compromises is a serious risk.

The worst time to evaluate your risk is after a compromise has already occurred. IT and security leaders must understand which applications use cryptography, how to identify and replace vulnerable keys or algorithms, and prepare formal crypto-agile incident response plans.

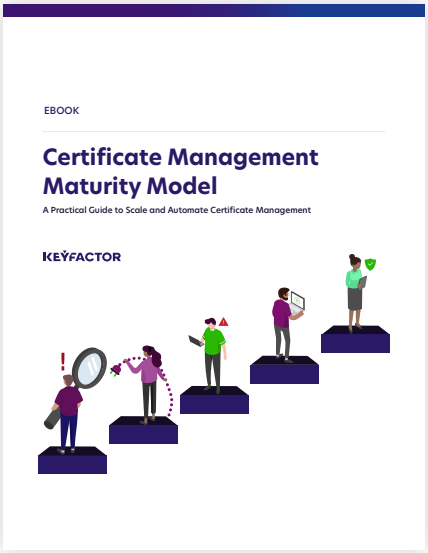
Use managed crypto services to help close the skills gap.

Forty percent of respondents in the study identified skills shortages as a barrier to setting an enterprise-wide crypto and machine identity strategy. Another 55% say they do not have sufficient staff dedicated to their PKI deployment.

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.

Next steps

Recommended resources



How to scale and automate certificate and key management in your business

Learn More →

5 reasons to move your PKI deployment to the cloud

Learn More →

Step by step guidance on how to achieve fast and secure code signing operations

Learn More →

Best practices to protect and manage SSH keys in multi-cloud operations

Learn More →

Research methodology

This year's study included 1,162 survey respondents across a wide range of industries and geographies. For the first time, the study examined organizations in the global region of Europe, the Middle East and Africa (EMEA), in addition to North America.

A sampling frame of 30,211 IT security professionals in North America and EMEA were selected as participants to this survey. The table below shows 1,286 total returns. Screening and reliability checks required the removal of 124 surveys. Our final sample consisted of 1,162 surveys or a 3.8 percent response. All respondents are familiar with their organization's PKI.

Sample Response	Freq	Pct%
Sampling frame	30,211	100%
Total returns	1,286	4.3%
Rejected or screened surveys	124	0.4%
Final sample	1,162	3.8%

Survey respondents

Here's a closer look at the 1,162 individuals who completed the survey in January 2021.

Distribution of sample by role in company

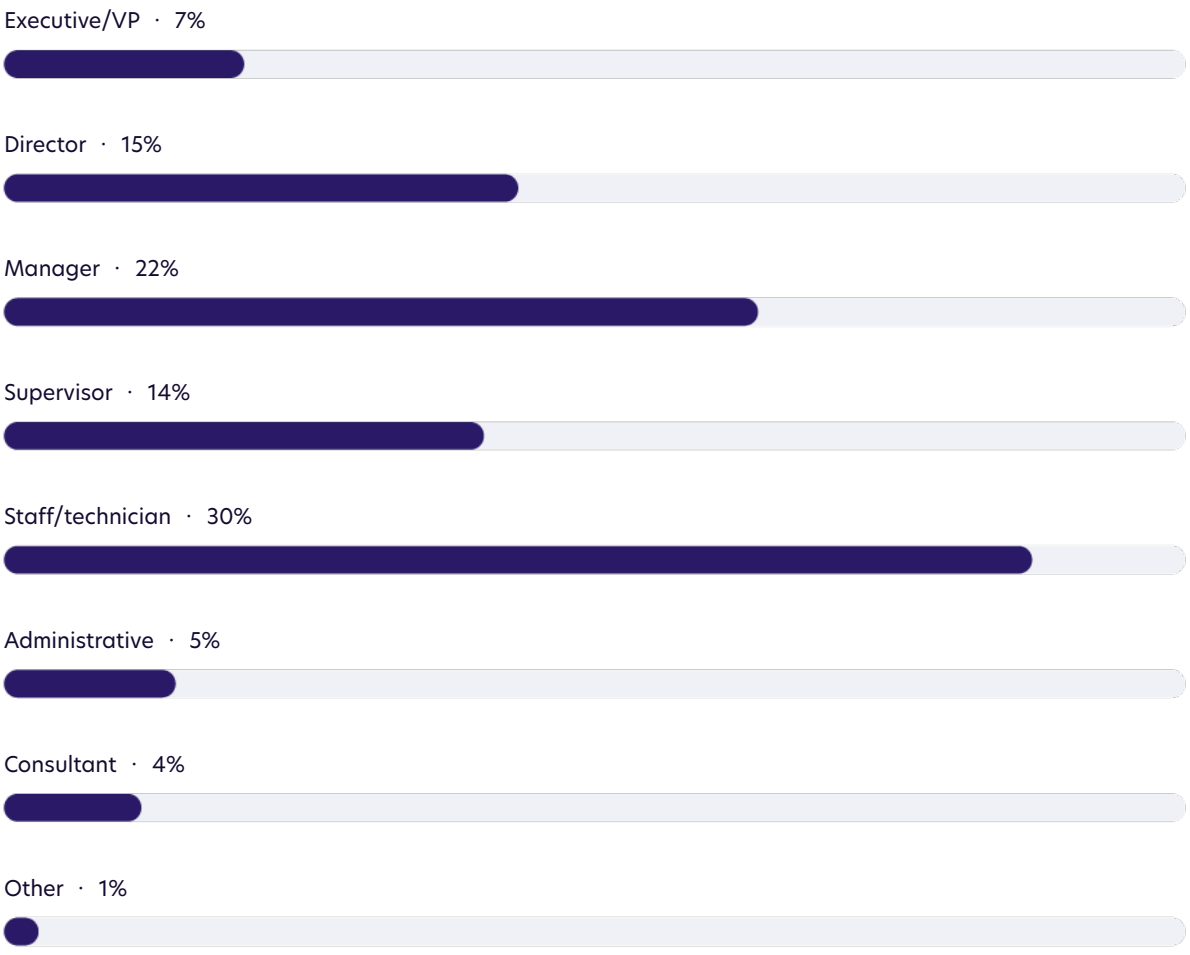


Figure 25 shows the distribution of respondents by their role within the organization. By design, more than half (58 percent) of respondents are at or above the supervisory levels. The largest category at 30 percent of respondents is staff/technician.

Distribution of sample by department or team

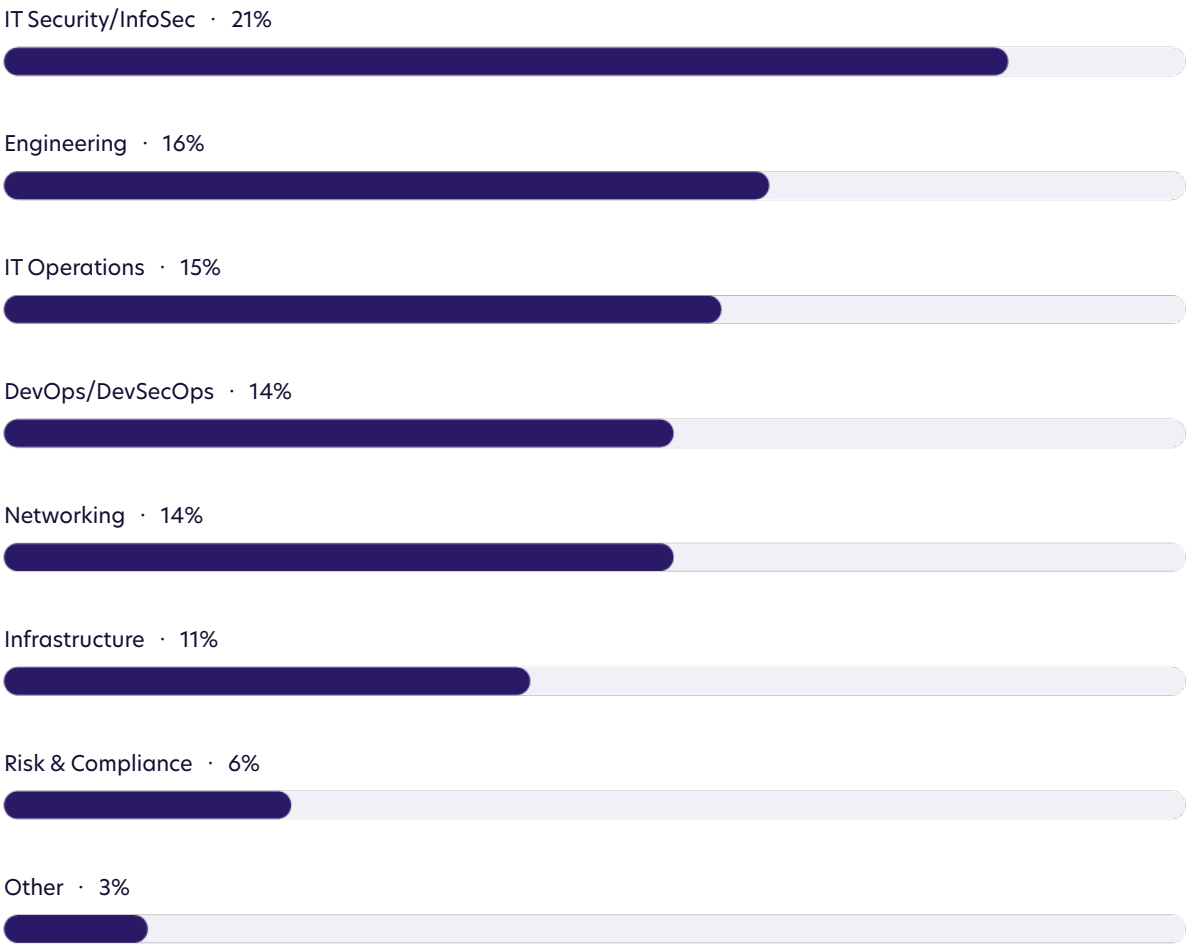


Figure 26 shows distribution of the 1,162 respondents by their department or team. The most prevalent departments were IT security/InfoSec, Engineering, IT Operations and DevOps/DevSecOps.

Distribution of sample by company size

Figure 27 shows the distribution of respondents by the size of their company (headcount). The sample was weighted relatively evenly across large, mid-size and small companies.

Distribution of sample by industry

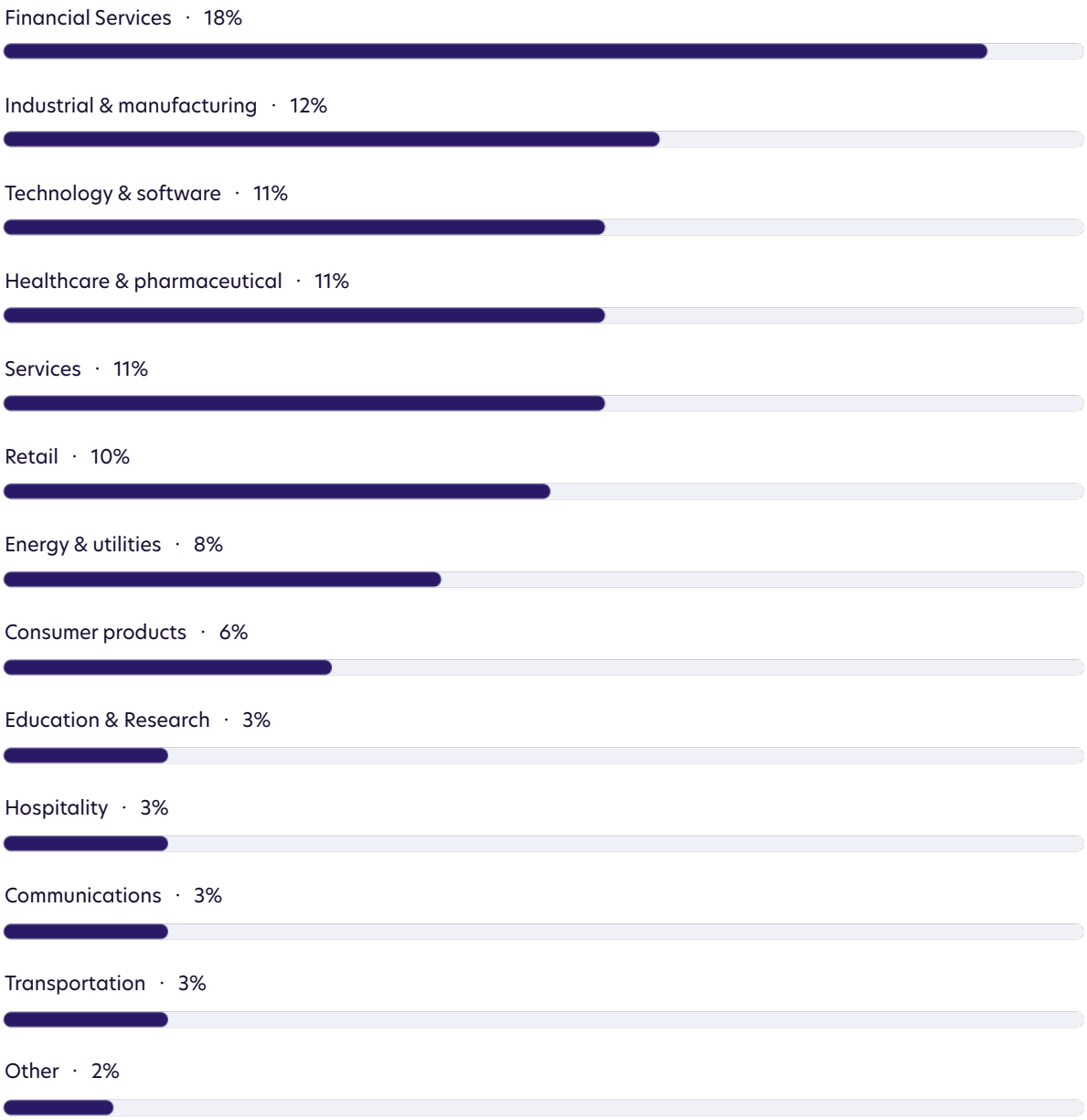


Figure 28 shows the distribution of organizations by industry. Twelve industries were represented in this year's study. The largest sectors were financial services, industrial and manufacturing, technology and software, and healthcare and pharmaceuticals.

Limitations

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 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 2021 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 is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across the entire enterprise.

We help our customers apply cryptography in the right way from modern, multi-cloud enterprises to complex IoT supply chains. With decades of cybersecurity experience, Keyfactor is trusted by more than 500 enterprises across the globe.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook. 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.