# 2024 State of Zero Trust & Encryption Study

**Sponsored by Entrust**

Independently conducted by Ponemon Institute LLC

Publication Date: May 2024

ENTRUST

SECURING A WORLD IN MOTION

Ponemon INSTITUTE

# Table of Contents



This year's data collection was conducted in December 2023 and completed in January 2024.

# Part 1

## Executive Summary

As the threat landscape continues to evolve and bad actors use increasingly persistent and sophisticated attacks, organizations are investing in advanced technologies and processes. The purpose of this report, sponsored by Entrust, is to provide important information about the use of Zero Trust, encryption trends, credential management, and HSMs to prepare for and prevent cyberattacks. The research also reveals what organizations believe to be the most significant threats. The top three are hackers, system or process malfunction, and unmanaged certificates.

A second report will present the research findings of PKI and IoT, as well as how organizations are preparing to transition to post-quantum cryptography in order to mitigate the quantum threat. For both reports, Ponemon Institute surveyed 4,052 IT and IT security practitioners who are familiar with the use of these technologies in their organizations.

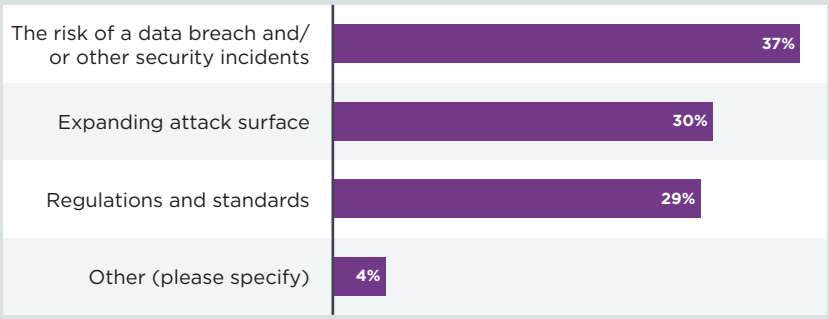
The countries and regions in this research are the United States (908 respondents), the United Kingdom (458 respondents), Canada (473 respondents), Germany (582 respondents), Australia/New Zealand (274 respondents), Japan (334 respondents), Singapore (367 respondents), the United Arab Emirates (355 respondents), and Saudi Arabia (301 respondents).

Zero Trust is defined in this research as an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. It assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership. Sixty-one percent of respondents say their organizations have adopted Zero Trust at some level. However, only 18 percent of respondents have implemented all Zero Trust principles.

As shown in Figure 1, 67 percent of respondents say the most important drivers to implementing a Zero Trust strategy are the risk of a data breach and/or other security incidents (37 percent) or the expanding attack surface (30 percent).

**Figure 1. What is the most important driver to implementing a Zero Trust strategy?**

Only one choice permitted.



# Following are the most salient findings from this year's research.

## The slow but growing adoption of Zero Trust

**As evidence of the importance of Zero Trust to secure the organization, 57 percent of respondents that have or will implement Zero Trust say their organizations will include it in their encryption plans or strategies.**

Of the respondents that say their organization has begun their Zero Trust journey, 18% say they have implemented all Zero Trust principles, 14% say they've laid the foundation for a Zero Trust strategy, and another 17% say they have started exploring various solutions to help implement a Zero Trust strategy. According to research, a lack of in-house expertise is slowing adoption.

**Senior leaders are supporting an enterprise-wide Zero Trust strategy.**

Fifty-nine percent of respondents say their leadership has significant or very significant support for Zero Trust. As evidence of senior leadership's support, only 37 percent of respondents say lack of leadership buy-in is a challenge. The biggest challenges when implementing Zero Trust are lack of in-house expertise (47 percent of respondents) or lack of budget (40 percent of respondents).

**Securing identities is the highest priority for a Zero Trust strategy.**

Respondents were asked to select the one area that has the highest priority for their Zero Trust strategy. The risk areas are identities, devices, networks, applications, and data. Forty percent of respondents say identities and 24 percent of respondents say devices are the priorities.

**Best-of-breed solutions are most important for a successful Zero Trust strategy (44 percent of respondents).**

This is followed by an integrated solution ecosystem from one to three vendors (22 percent of respondents).

# Trends in encryption and encryption in the public cloud: 2019 to 2024

**Hackers are becoming more of a threat to sensitive and confidential data.**
Organizations need to make the hacker threat an important part of their security strategies. Since the last report, a significant increase from 29 percent of respondents to 46 percent of respondents cite hackers as the biggest concern to being able to protect sensitive and confidential information.

**Management of keys and enforcement of policy continue to be the most important features in encryption solutions.**
Respondents were asked to rate the importance of certain features in encryption solutions. The most important features are management of keys, enforcement of policy, and system performance and latency.

**Since 2019, organizations have been steadily transferring sensitive and confidential data to public clouds whether or not it is encrypted or made unreadable via some other mechanism.**
In this year's study, 80 percent of respondents say their organizations currently transfer data (52 percent) or are likely to do so in the next 12 to 24 months (28 percent).

**Encryption performed on-premises prior to sending data to the cloud using organizations' own keys has declined significantly since 2019.**
The main methods for protecting data at rest in the cloud are using keys generated/managed by the cloud provider (39 percent of respondents) or encryption is performed in the cloud using keys their organizations generate and manage on-premises. Only 23 percent of respondents say encryption is performed on-premises.

**There has been a significant decrease in organizations only using keys controlled by their organization (from 42 percent to 22 percent of respondents).**
Instead, the primary strategy for encrypting data at rest in the cloud is the use of a combination of keys controlled by their organization and by the cloud provider, with a preference for keys controlled by their organization, a significant increase from 19 percent of respondents to 32 percent of respondents in 2024. This is followed by only using keys controlled by the cloud provider (24 percent of respondents).

**The importance of privileged user access controls has increased significantly.**
Respondents were asked to rate the importance of cloud encryption features on a scale of 1 = not important to 5 = most important. Privileged user access controls increased from 3.23 in 2022 to 4.38 in 2024 on the 5-point scale. The importance of granular access controls and the ability to encrypt and rekey data while in use without downtime also increased significantly.

# Trends in credential management and HSMs: 2019 to 2024

### Lack of skilled personnel and no clear ownership make the management of credentials painful.

Fifty-nine percent of respondents say managing keys has a severe impact on their organizations. There are interesting trends since 2019 in what causes the pain. The lack of skilled personnel (50 percent of respondents) and no clear ownership (47 percent of respondents) continue to make credential management difficult. Insufficient personnel increased from 34 percent to 46 percent of respondents. Not causing as much pain are the inadequacy of key management tools (from 52 percent to 32 percent) and systems are isolated and fragmented (from 46 percent to 29 percent).

### Many types of keys are getting less painful to manage.

Between 2019 to 2024 the following keys have become less painful to manage: keys for external cloud or hosted services including Bring Your Own Keys (from 54 percent to 22 percent of respondents), SSH keys (from 57 percent to 27 percent of respondents) and signing keys (e.g. code signing, digital signatures (from 52 percent to 25 percent of respondents).

### Management of credentials is challenging because it is harder to consistently apply security policies over credentials used across multi-cloud and cross-cloud environments.

Fifty-five percent of respondents say the management of credentials is becoming more challenging in a multi-cloud and cross-cloud environment. Thirty-six percent of respondents say it is due to the difficulty in consistently applying security policies over credentials used across cloud services followed by it is harder to have visibility over credentials that protect and enable access to critical data and applications (33 percent of respondents).

The applications that require the use of credential management across cloud-based deployments are mainly KMIP-compliant applications (44 percent of respondents), and databases, back-up, and storage (43 percent of respondents).

### More organizations are using hardware security modules (HSMs).

HSMs are dedicated crypto processors that are specifically designed for the protection of the crypto key lifecycle. Since 2019, the use of HSMs has increased from 47 percent of respondents to 55 percent of respondents.

### Organizations value the use of HSMs.

Since 2019, organizations are increasing the use of HSMs as part of their encryption and credential management strategies. The use of application-level encryption, database encryption, and TLS/SSL have increased significantly. For the first time, respondents were asked where HSMs are deployed. Most are deployed in online root, offline root, and issuing CAs.

# Part 2

## Key Findings

In this section, we provide a deeper dive into the global consolidated research findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

**A. The slow but growing adoption of Zero Trust**

**B. Trends in encryption and public cloud encryption: 2019 to 2024**

**C. Trends in credential management & HSMs: 2019 to 2024**

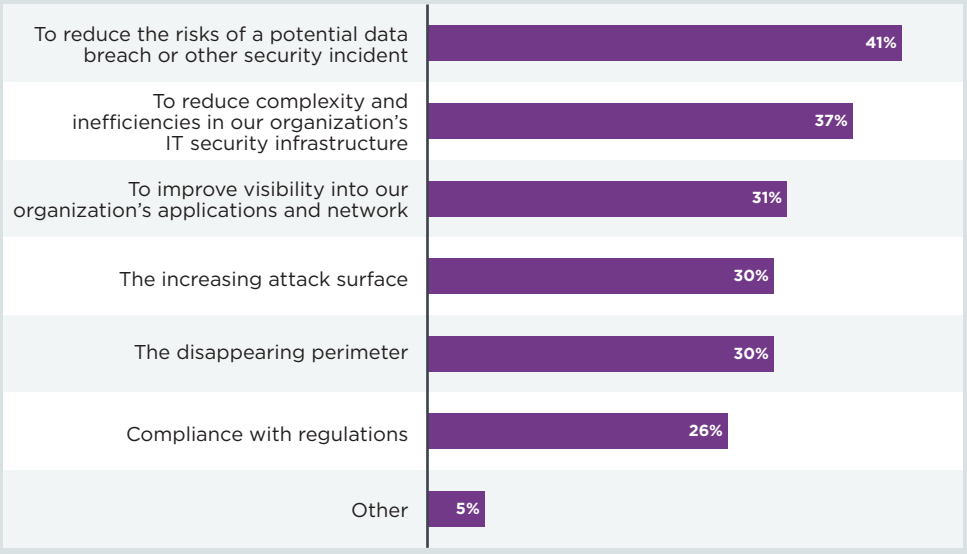
## A. The slow but growing adoption of Zero Trust

**Concerns about experiencing a data breach is the No. 1 incentive to invest in security, including Zero Trust.** Forty-one percent of respondents say security investments are made primarily to reduce the risks of a potential data breach or other security incident. This is a shift in perceptions about what drives security investments. In past Ponemon Institute studies, compliance with regulations was a No. 1 or No. 2 reason for investing in security.

Other reasons that influence security investment decisions are shown in Figure 2. They are to reduce complexity and inefficiencies in their organizations' IT security infrastructure (37 percent of respondents) or to improve visibility into their organizations' applications and network (31 percent of respondents).

**Figure 2. What most influences your organization's security investment decisions?**

Two choices permitted.

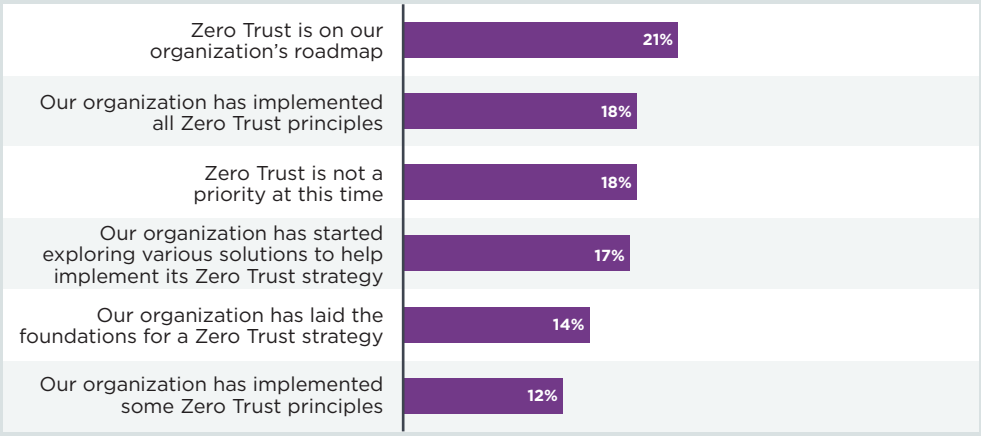


**As evidence of the importance of Zero Trust to secure the organization, 57 percent of respondents that have or will implement Zero Trust say their organizations will include Zero Trust in their encryption plans or strategies.** Currently, however, most organizations are at the early stage of Zero Trust adoption. According to the research, a lack of in-house expertise is slowing adoption.

As shown in Figure 3, 18 percent of respondents say they have implemented all Zero Trust principles, 14% say they've laid the foundation for a Zero Trust strategy, and another 17% say they have started exploring various solutions to help implement a Zero Trust strategy.

**Figure 3. Which best describes the current stage of Zero Trust in your organization?**

Only one choice permitted.

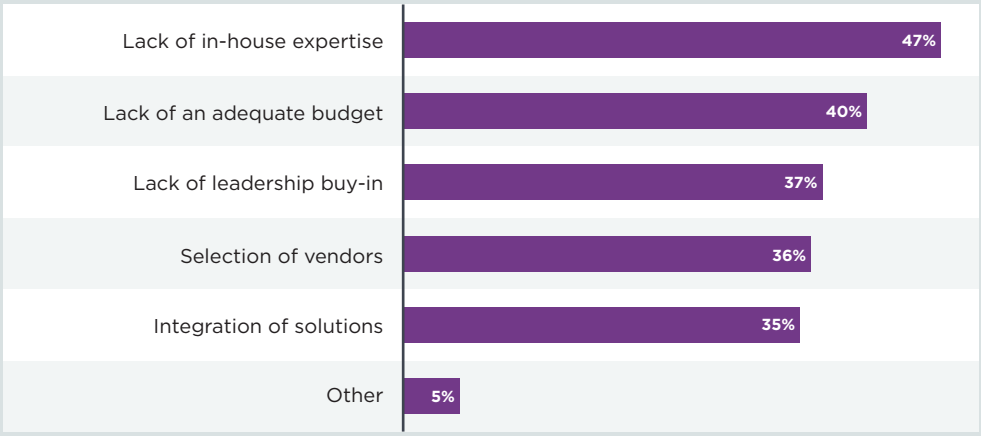



**Senior leaders are supporting an enterprise-wide Zero Trust strategy.** Respondents were asked to rate the level of senior leaders' support for an enterprise-wide Zero Trust strategy on a scale from 1 = no support to 10 = very significant support. Fifty-nine percent of respondents say their leadership has significant or very significant support for this strategy.

Figure 4 provides evidence of senior leadership's support. Only 37 percent of respondents say lack of leadership buy-in is a challenge. The biggest challenges when implementing Zero Trust are a lack of in-house expertise (47 percent of respondents) or lack of budget (40 percent of respondents).

**Figure 4. What are the top two challenges when implementing a Zero Trust strategy?**

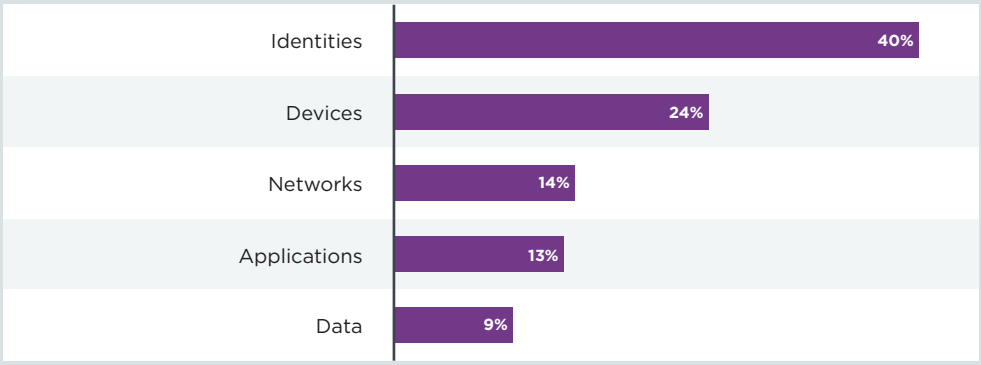
Two responses permitted.



**Securing identities is the highest priority for a Zero Trust strategy.** Figure 5 lists risk areas that would be included in a Zero Trust strategy. Forty percent of respondents say identities has the highest priority. Twenty-four percent of respondents say devices is a high priority.

**Figure 5. Which risk area has the highest priority for your Zero Trust strategy?**

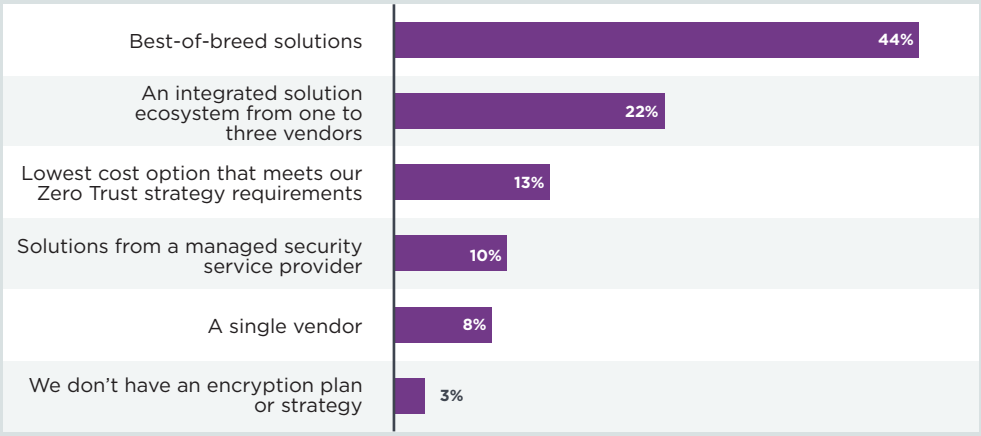
Only one choice permitted.




**Best-of-breed solutions are most important for a successful Zero Trust strategy (44 percent of respondents).** This is followed by an integrated solution ecosystem from one to three vendors (22 percent of respondents), as shown in Figure 6.

**Figure 6. What is most important for a successful Zero Trust strategy?**

Two responses permitted.

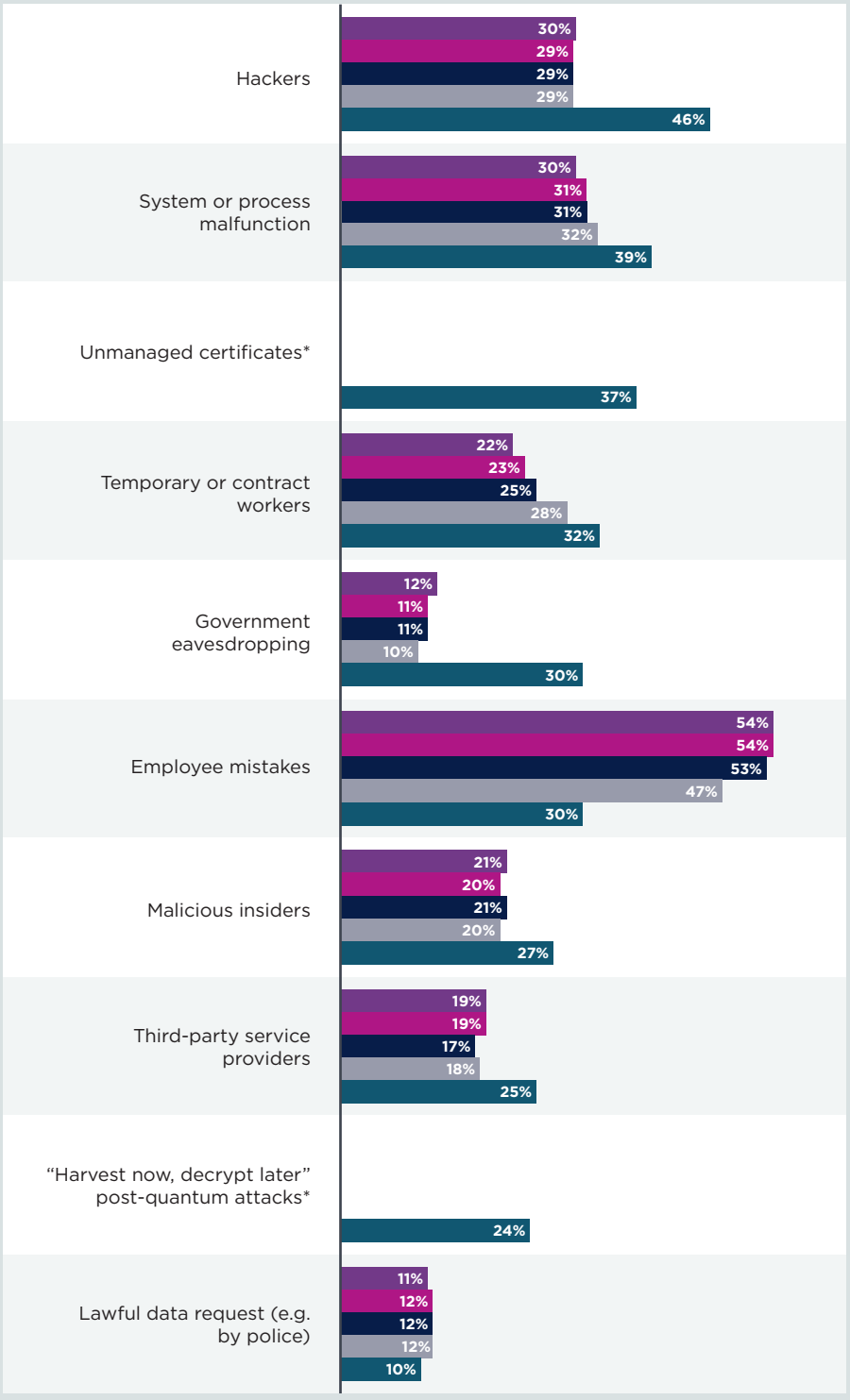


# B. Trends in encryption and in public cloud services: 2019 to 2024

**Hackers are becoming more of a threat to sensitive and confidential data.** Organizations need to make the hacker threat an important part of their security strategies. Since the last report, a significant increase from 29 percent of respondents to 46 percent of respondents cite hackers as the biggest concern to being able to protect sensitive and confidential information, as shown in Figure 12.

**Figure 12. What are the main areas of concern that might result in the exposure of sensitive or confidential data?**

Three responses permitted.

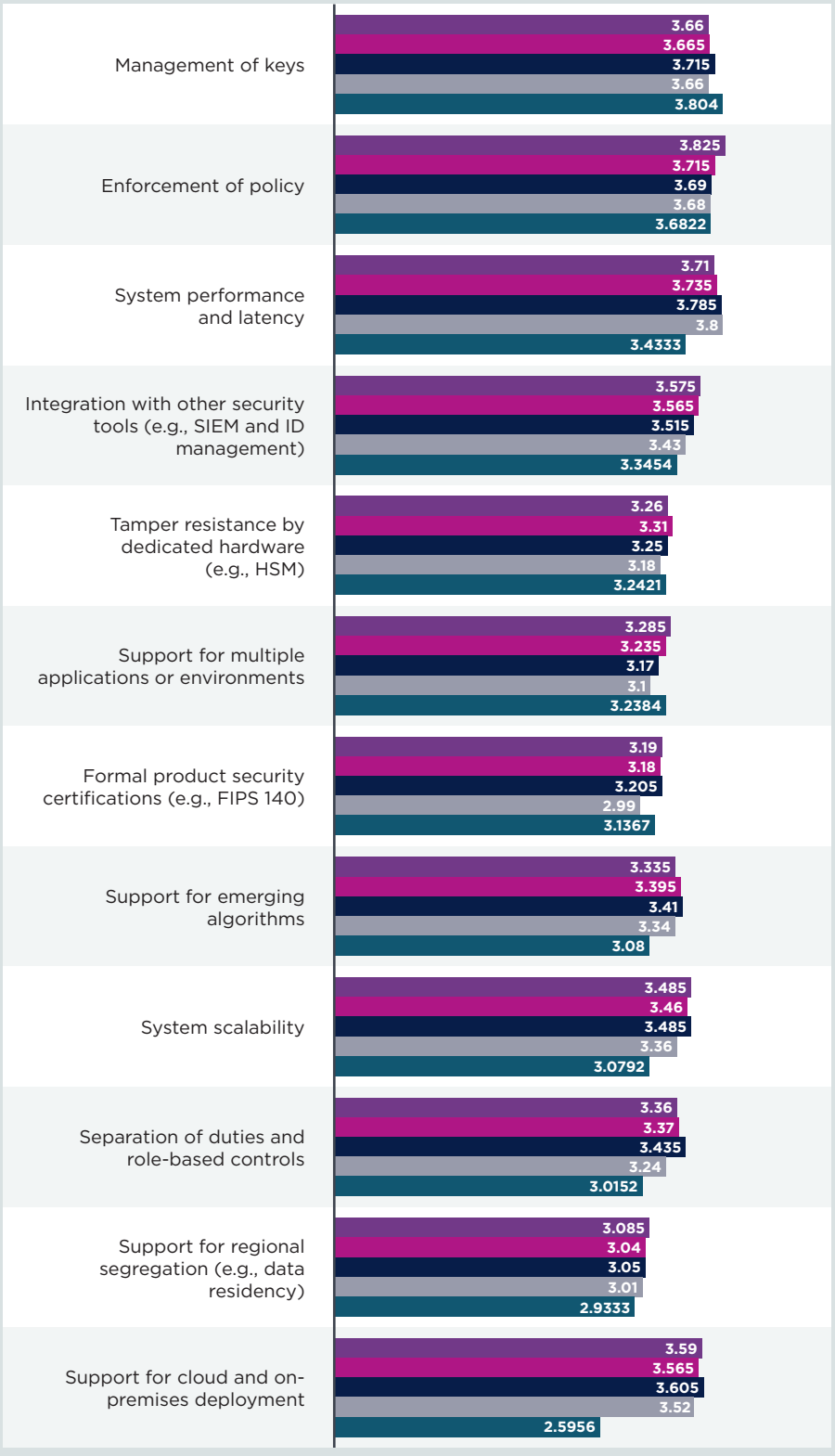



* Not a response for previous years

**Management of keys and enforcement of policy continue to be the most important features in encryption solutions.** Respondents were asked to rate the importance of certain features in encryption solutions on a scale from 1 = not important to 5 = most important. As shown in Figure 13, the most important features are management of keys (3.8), enforcement of policy (3.68), and system performance and latency (3.43).

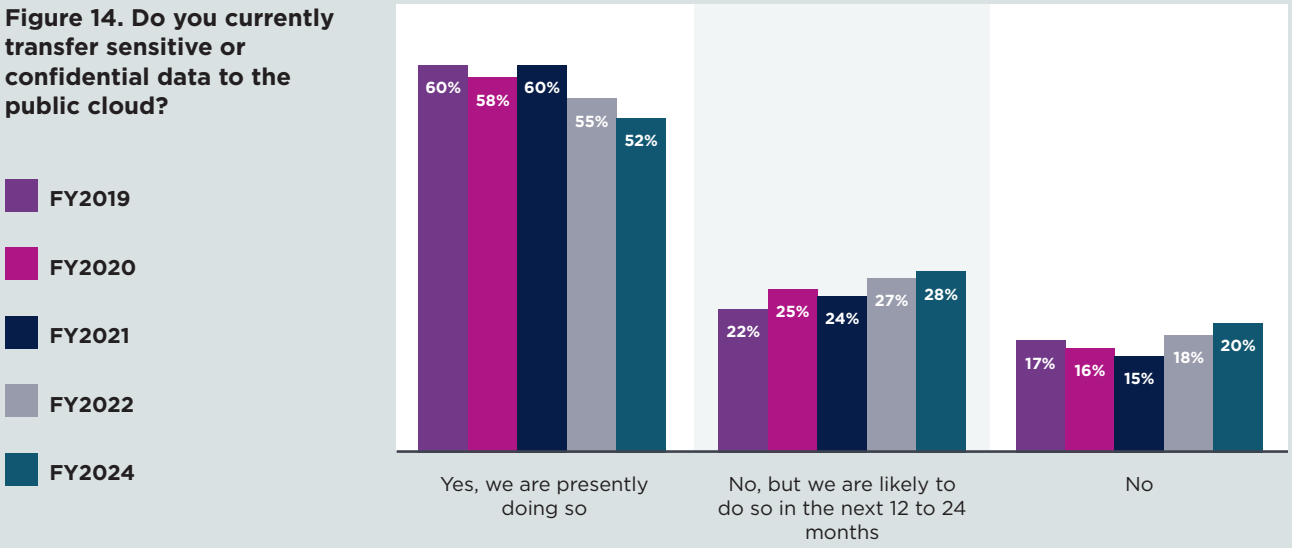
**Figure 13. How important are the following features associated with encryption solutions**

On a scale of 1 = not important to 5 = very important



**According to the research, since 2019 organizations have been steadily transferring sensitive and confidential data to public clouds whether or not it is encrypted or made unreadable via some other mechanism.** As shown in Figure 14, in this year's report 52 percent of respondents say their organizations currently transfer data, and 28 percent say they are likely to do so in the next 12 to 24 months.

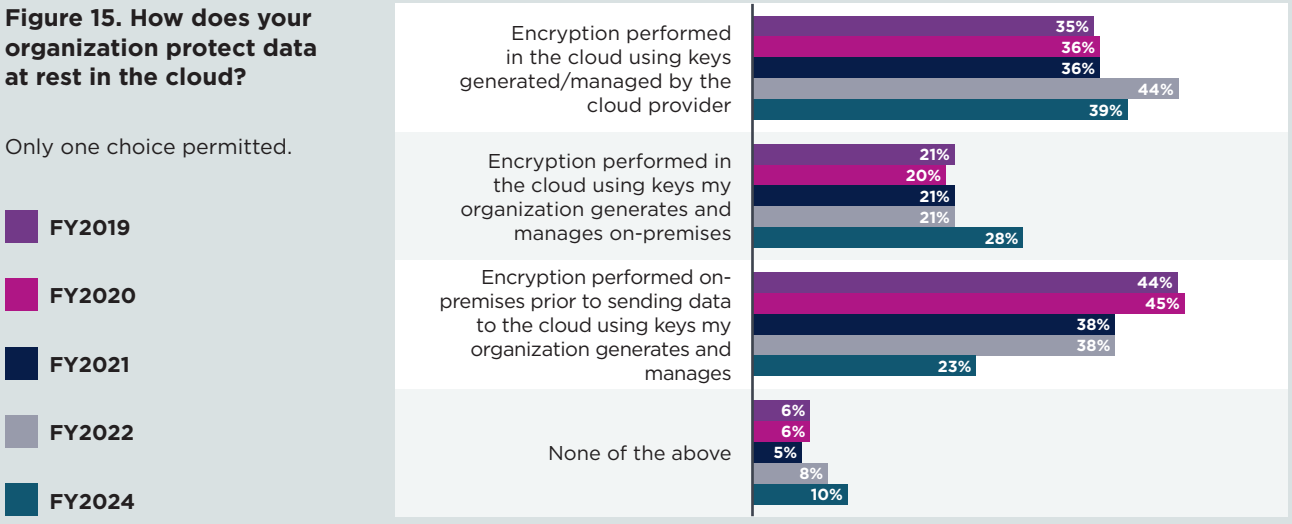
**Figure 14. Do you currently transfer sensitive or confidential data to the public cloud?**




**Encryption performed on-premises prior to sending data to the cloud using organizations' own keys has declined significantly since 2019.** As shown in Figure 15, the main methods for protecting data at rest in the cloud are using keys generated/managed by the cloud provider (39 percent of respondents) or encryption is performed in the cloud using keys their organizations generate and manage on-premises (28 percent). Only 23 percent of respondents say encryption is performed on-premises.

**Figure 15. How does your organization protect data at rest in the cloud?**

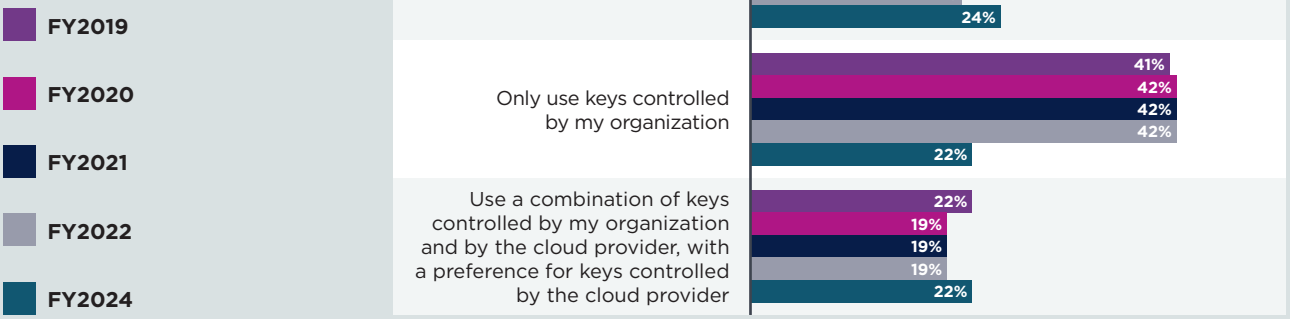
Only one choice permitted.



**There has been a significant decrease in organizations only using keys controlled by their organization (from 42 percent to 22 percent of respondents).** Instead, the primary strategy for encrypting data at rest in the cloud is the use of a combination of keys controlled by their organization and by the cloud provider, with a preference for keys controlled by their organization, a significant increase from 19 percent to 32 percent of respondents. This is followed by only using keys controlled by the cloud provider (24 percent of respondents), as shown in Figure 16.

**Figure 16. For encryption of data at rest in the cloud, what is your organization's strategy?**

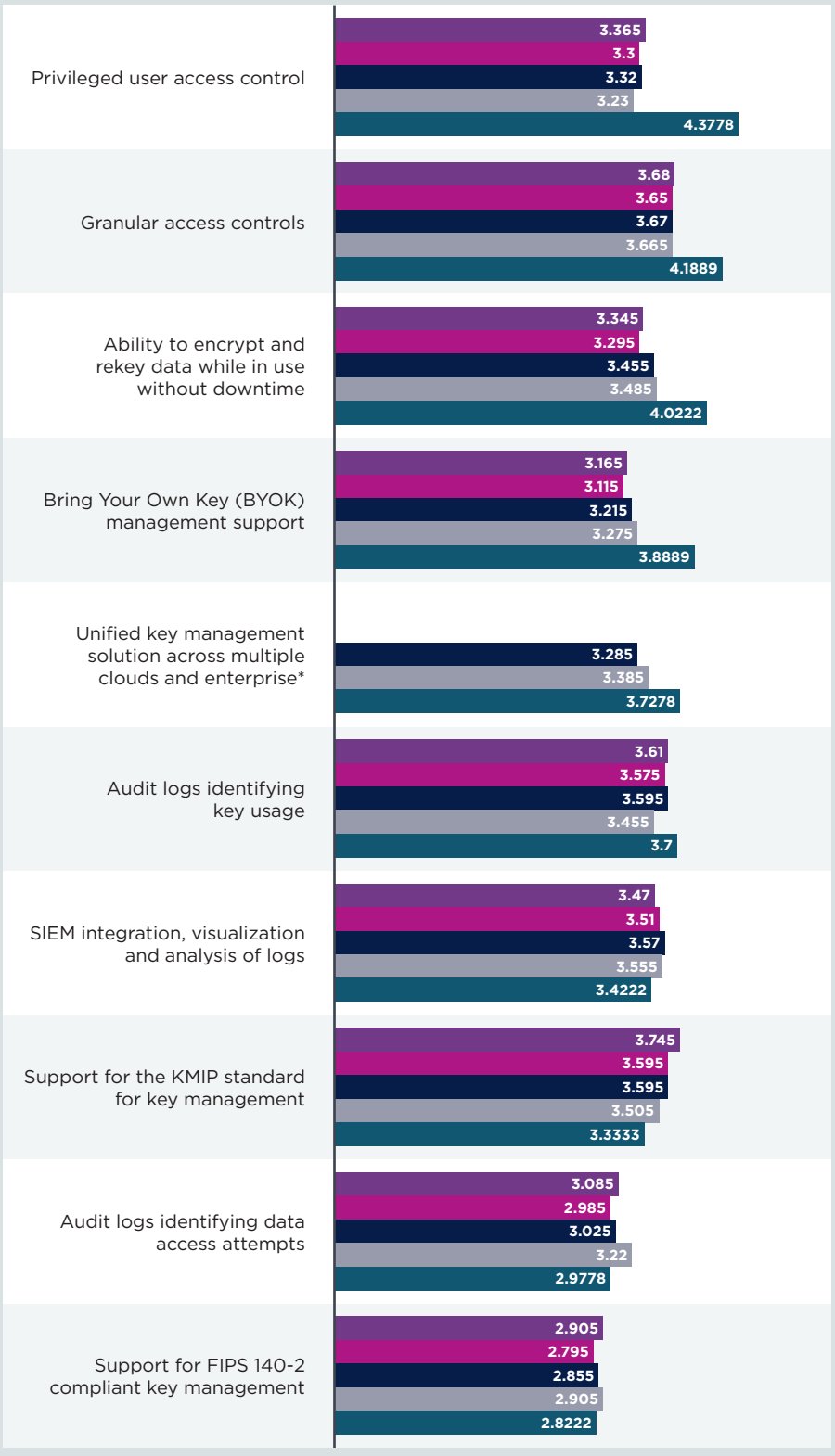
Only one choice permitted.



**The importance of privileged user access controls has increased significantly.** Respondents were asked to rate the importance of cloud encryption features on a scale of 1 = not important to 5 = most important. As shown in Figure 17, privileged user access controls increased from 3.23 in 2022 to 4.38 in 2024. Granular access controls and the ability to encrypt and rekey data while in use without downtime increased significantly as well.

**Figure 17. How important are the following features associated with cloud encryption to your organization?**

On a scale of 1 = not important to 5 = very important




* Response not available for all years

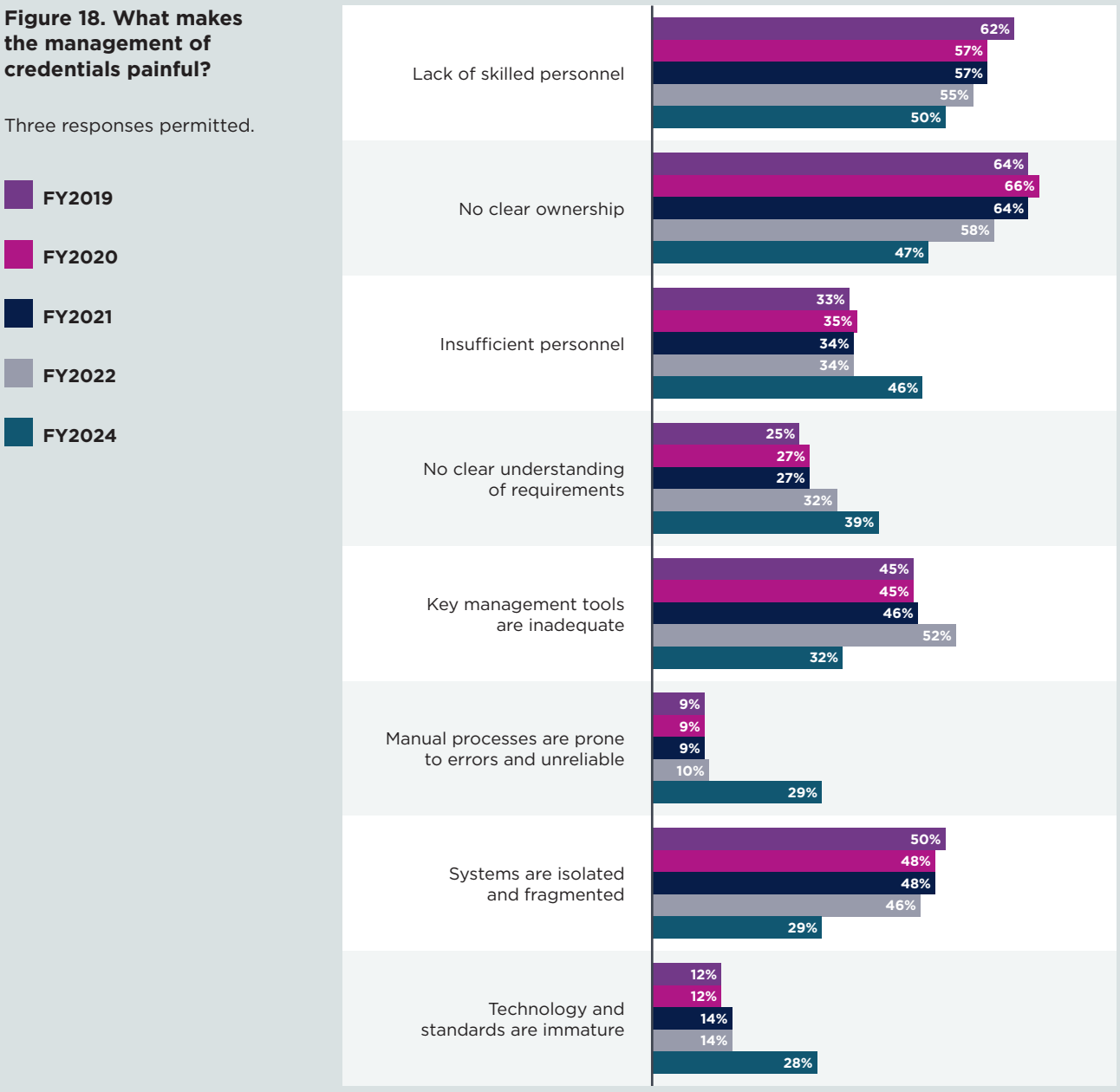
## C. Trends in credential management and HSMs: 2019 to 2024

**Lack of skilled personnel and no clear ownership make the management of credentials painful.** Respondents were asked to rate the overall "pain associated with managing credentials (keys, certificates, and secrets) on a scale from 1 = minimal impact to 10 = severe impact. Fifty-nine percent of respondents say managing keys has a high or severe impact on their organizations.

According to Figure 18, there are interesting trends in what causes the pain since 2019. The lack of skilled personnel (50 percent of respondents) and no clear ownership (47 percent of respondents) continue to make credential management difficult. Not causing as much pain are the inadequacy of key management tools (from 52 percent to 32 percent) and systems are isolated and fragmented (from 46 percent to 29 percent). Insufficient personnel increased from 34 percent to 46 percent of respondents.

**Figure 18. What makes the management of credentials painful?**

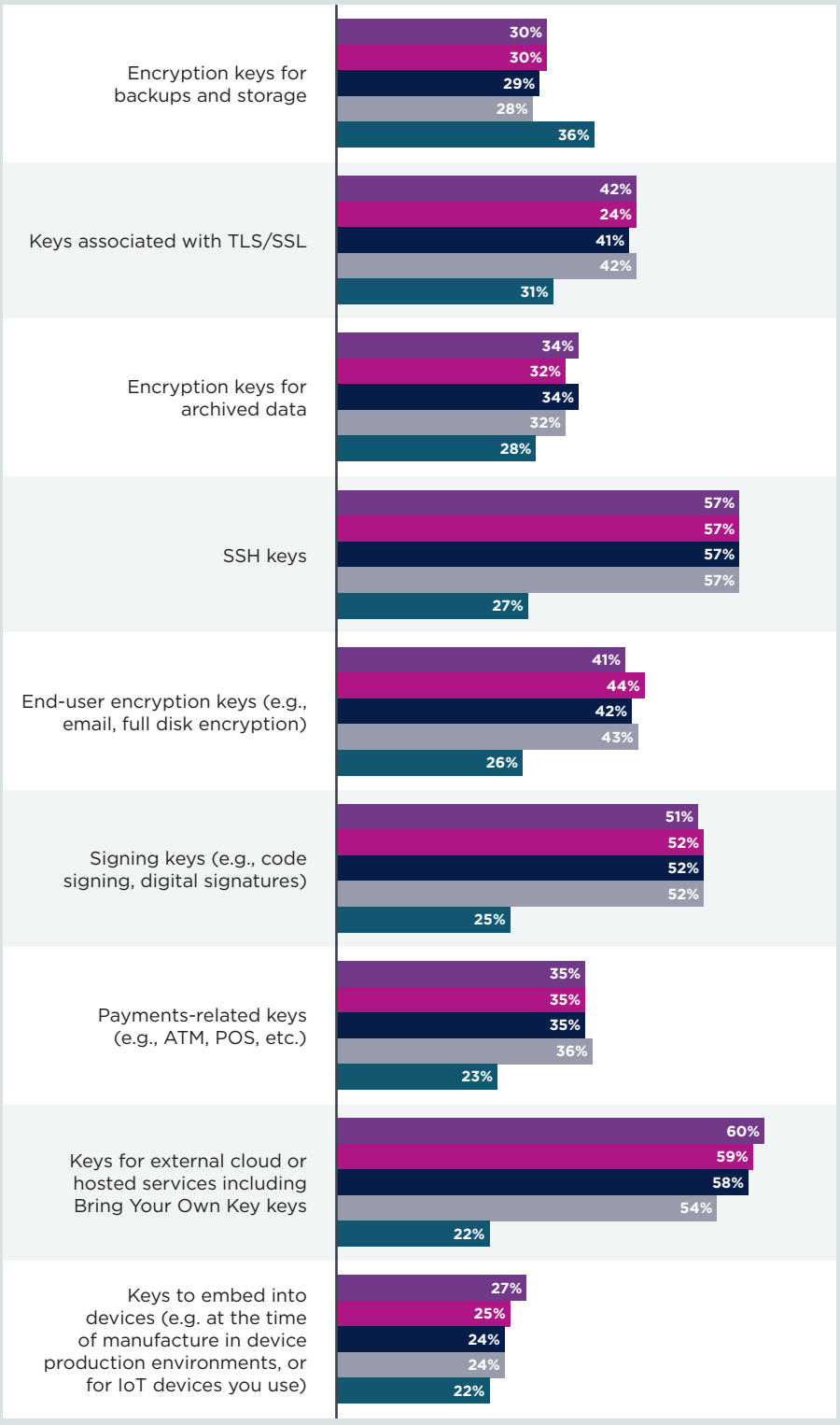
Three responses permitted.



**Many types of keys are getting less painful to manage.** Figure 19 presents the keys considered to be very painful and painful to manage from 2019 to 2024. As shown, the keys becoming less painful are keys for external cloud or hosted services including Bring Your Own Keys (from 54 percent to 22 percent of respondents), SSH keys (from 57 percent to 27 percent of respondents), and signing keys (e.g. code signing, digital signatures (from 52 percent to 25 percent of respondents).

**Figure 19. Which types of keys are most difficult to manage?**

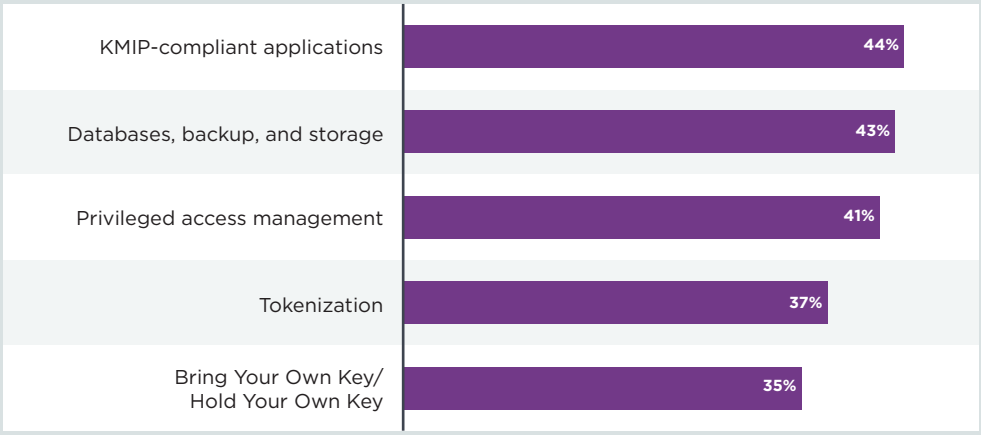
Very painful and painful responses presented.



The applications that require the use of credential management across cloud-based deployments are mainly KMIP-compliant applications (44 percent of respondents) and databases, back-up, and storage (43 percent of respondents) as shown in Figure 20.

**Figure 20. Which applications are requiring the use of credential management across cloud-based deployments?**

Two responses permitted.



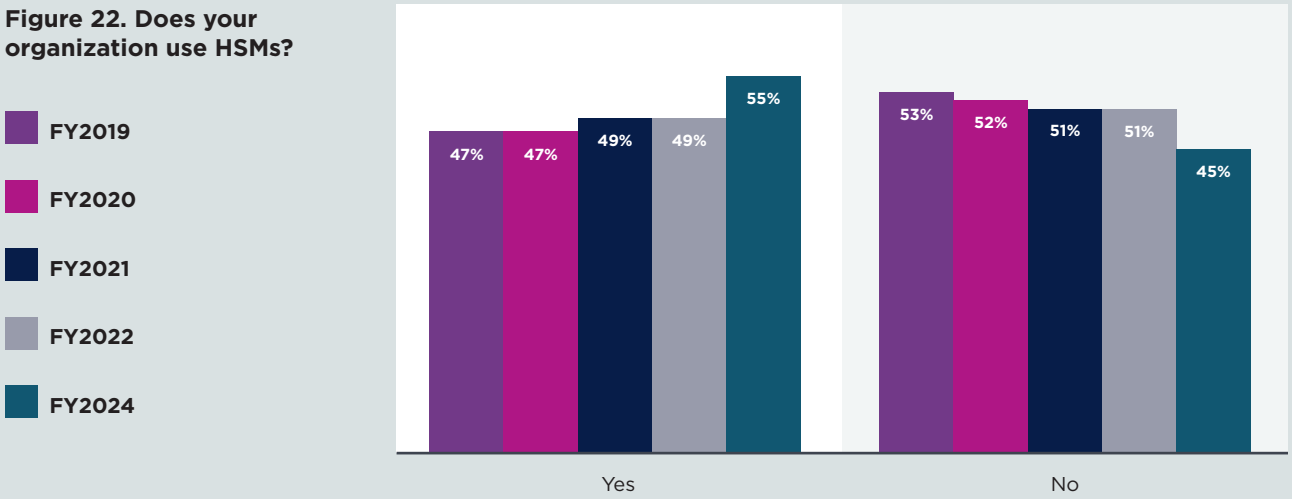

**Management of credentials is challenging because it is harder to consistently apply security policies over credentials used across cloud services.** Fifty-five percent of respondents say the management of credentials is becoming more challenging in a multi-cloud and cross-cloud environment (reference appendix page 34). As shown in Figure 21, 36 percent of respondents say it is due to difficulty in consistently applying security policies over credentials used across cloud services, followed by it is harder to have visibility over credentials that protect and enable access to critical data and applications (33 percent of respondents).

**Figure 21. Why is the management of credentials more challenging in a multi-cloud and cross-cloud environment?**

Only one choice permitted.

**More organizations are using hardware security modules (HSMs) since 2019.** HSMs are dedicated crypto processors that are specifically designed for the protection of the crypto key lifecycle. Since 2019, the use of HSMs has increased from 47 percent of respondents to 55 percent of respondents, as shown in Figure 22.

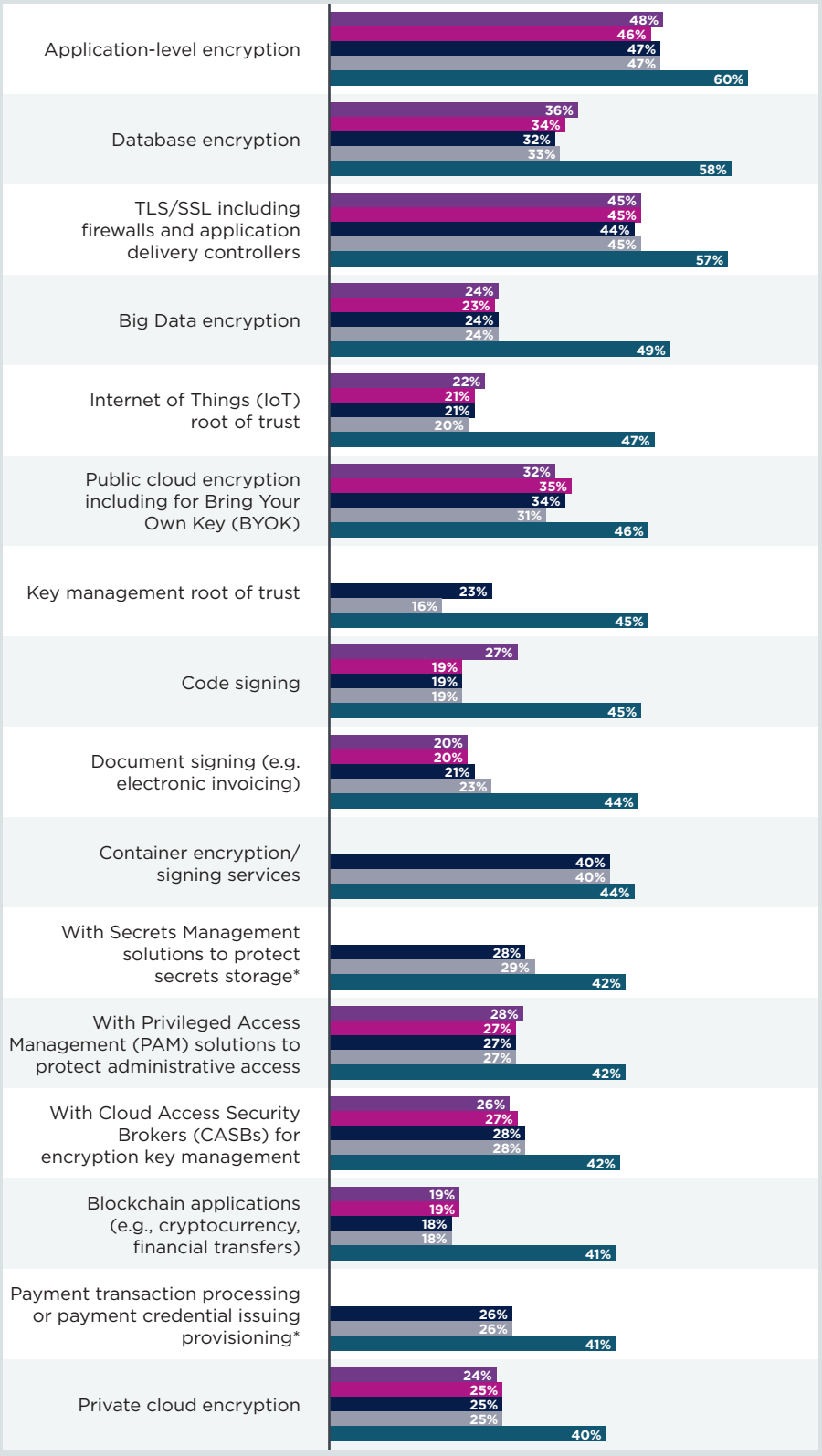
**Figure 22. Does your organization use HSMs?**



**Organizations value the use of HSMs.** Since 2019, organizations are increasing the use of HSMs as part of their encryption and credential management strategies. Figure 23 shows trends in deploying HSMs. Application-level encryption, database encryption, and TLS/SSL have increased significantly.

**Figure 23. For what purpose does your organization presently deploy or plan to use HSMs today and in the next 12 months?**

More than one response permitted.

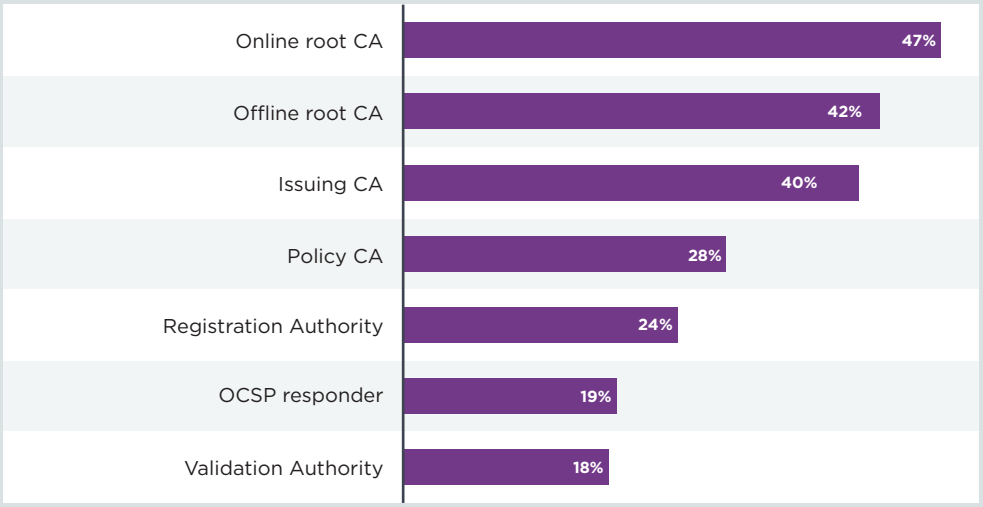



* Response not available for all years

**For the first time, respondents were asked where HSMs are deployed.** According to Figure 24, most are deployed in online root, offline root, and issuing CAs.

**Figure 24. Where are HSMs deployed?**

More than one response permitted.




ENTRUST
SECURING A WORLD IN MOTION

Ponemon INSTITUTE

# Appendix 1.

## Methods & Limitations

Table 1 reports the sample response for nine separate country/regional samples. Data collection was started in November 2023 and completed in December 2023. Since the report is published in 2024, we label the data captured in 2023 as FY2024.

Our consolidated sampling frame of practitioners in all countries consisted of 80,307 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 4,377 returns of which 325 were rejected for reliability issues. Our final consolidated 2024 sample was 4,052, thus resulting in an overall 5 percent response rate.

The first encryption trends study was conducted in the United States in 2005. Trend analysis was performed on combined country samples.

**Table 1. Survey response in nine countries/regions**

| Legend | Survey response | Sampling frame | Final sample | Response rate |
|---|---|---|---|---|
| AU/NZ | Australia/New Zealand | 5,600 | 274 | 4.9% |
| CA | Canada | 10,010 | 473 | 4.7% |
| DE | Germany | 12,849 | 582 | 4.5% |
| JP | Japan | 11,030 | 334 | 3.0% |
| SA | Saudi Arabia | 3,774 | 301 | 8.0% |
| SG | Singapore | 3,663 | 367 | 10.0% |
| UAE | United Arab Emirates | 4,996 | 355 | 7.1% |
| UK | United Kingdom | 10,585 | 458 | 4.3% |
| US | United States | 17,800 | 908 | 5.1% |
| | Consolidated | 80,307 | 4,052 | 5.0% |

Table 2 summarizes our survey samples for 10 countries/regions over a 14-year period.

**Table 2. Sample history over 14 years**

| | FY24 | FY22 | FY20 | FY19 | FY18 | FY17 | FY16 | FY15 | FY14 | FY13 | FY12 | FY11 | FY10 | FY09 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AU/NZ | 274 | 279 | 317 | 325 | 327 | 315 | 331 | 334 | 359 | 414 | 938 | 471 | 477 | 482 |
| CA | 473 | | | | | | | | | | | | | |
| DE | 582 | 478 | 467 | 473 | 531 | 543 | 531 | 563 | 564 | 602 | 499 | 526 | 465 | 490 |
| JP | 334 | 514 | 487 | 504 | 502 | 468 | 450 | 487 | 476 | 521 | 466 | 544 | | |
| ME* | | 206 | 276 | 276 | 268 | | | | | | | | | |
| SA | 301 | | | | | | | | | | | | | |
| SG | 367 | | | | | | | | | | | | | |
| UAE | 355 | | | | | | | | | | | | | |
| UK | 458 | 368 | 408 | 389 | 402 | 468 | 460 | 487 | 509 | 637 | 550 | 651 | 622 | 615 |
| US | 908 | 833 | 677 | 689 | 683 | 710 | 701 | 758 | 789 | 892 | 531 | 912 | 964 | 997 |

*In previous years of this report, the Middle East included a combination of the respondents located in Saudi Arabia and the United Arab Emirates.

Figure 25 reports the respondent's organizational level within participating organizations. By design, 69 percent of respondents are at or above the supervisory levels and 31 percent of respondents reported their position as associate/staff/technician. Respondents have on average 12 years of security experience with approximately 6.2 years of experience in their current position.

**Figure 25. Distribution of respondents according to position level**

Country samples are consolidated.

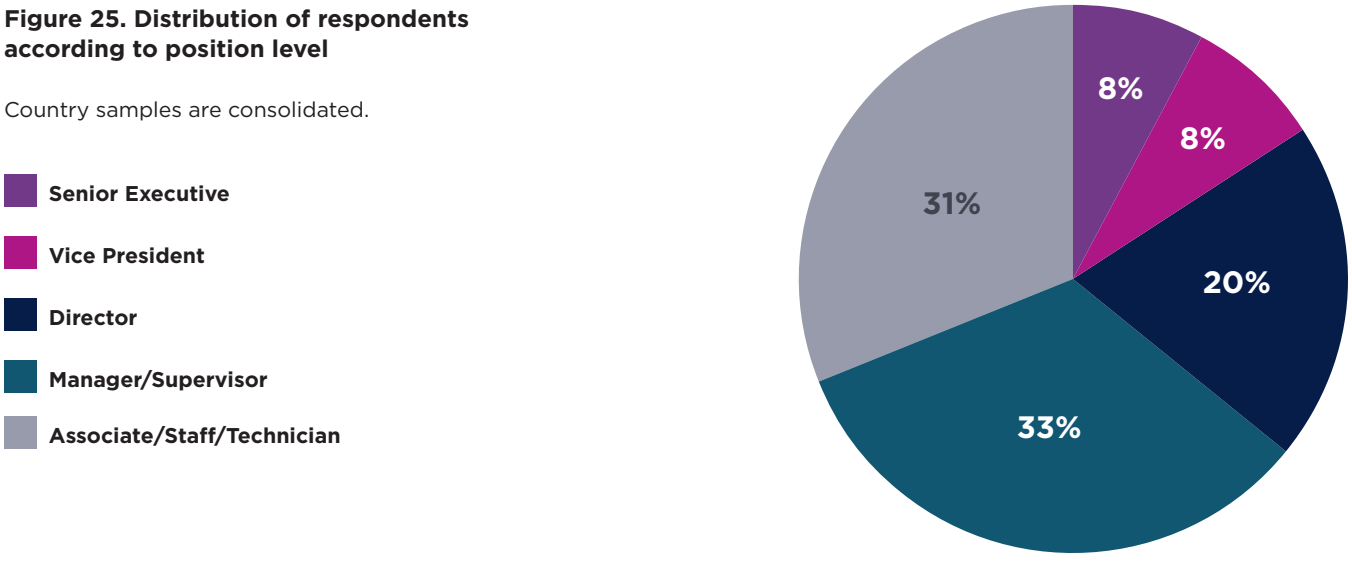


Figure 26 identifies the organizational location of respondents in our study. Forty percent of respondents are located within IT operations. This is followed by security at 16 percent of respondents, lines of business (16 percent of respondents), and compliance (15 percent of respondents).

**Figure 26. Distribution of respondents according to organizational location**

Country samples are consolidated.

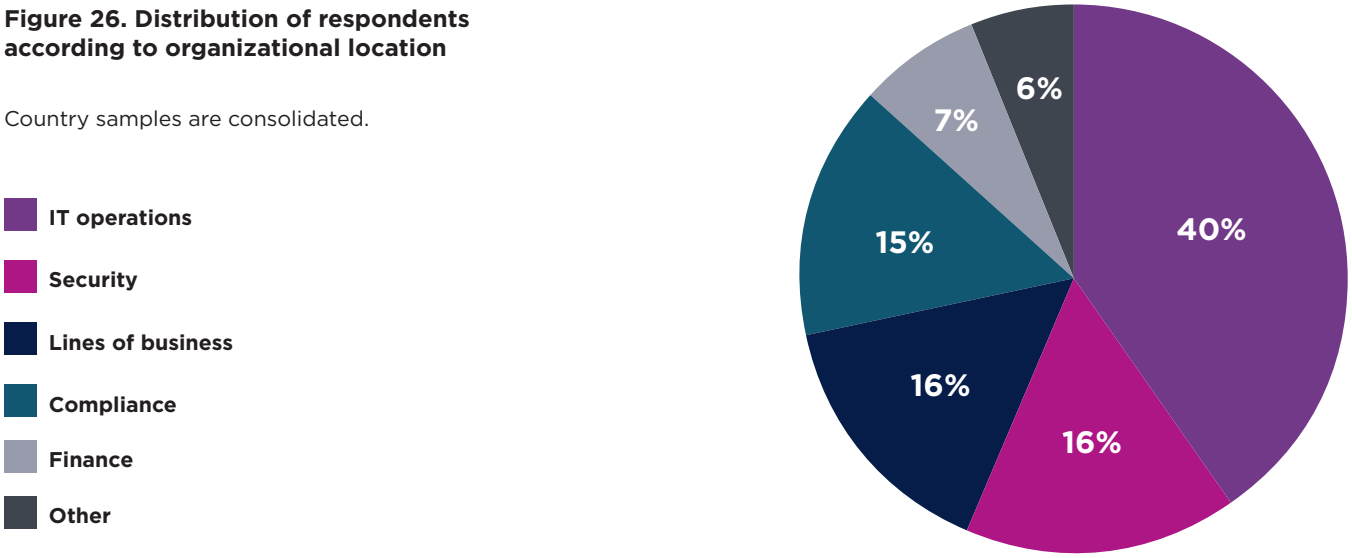
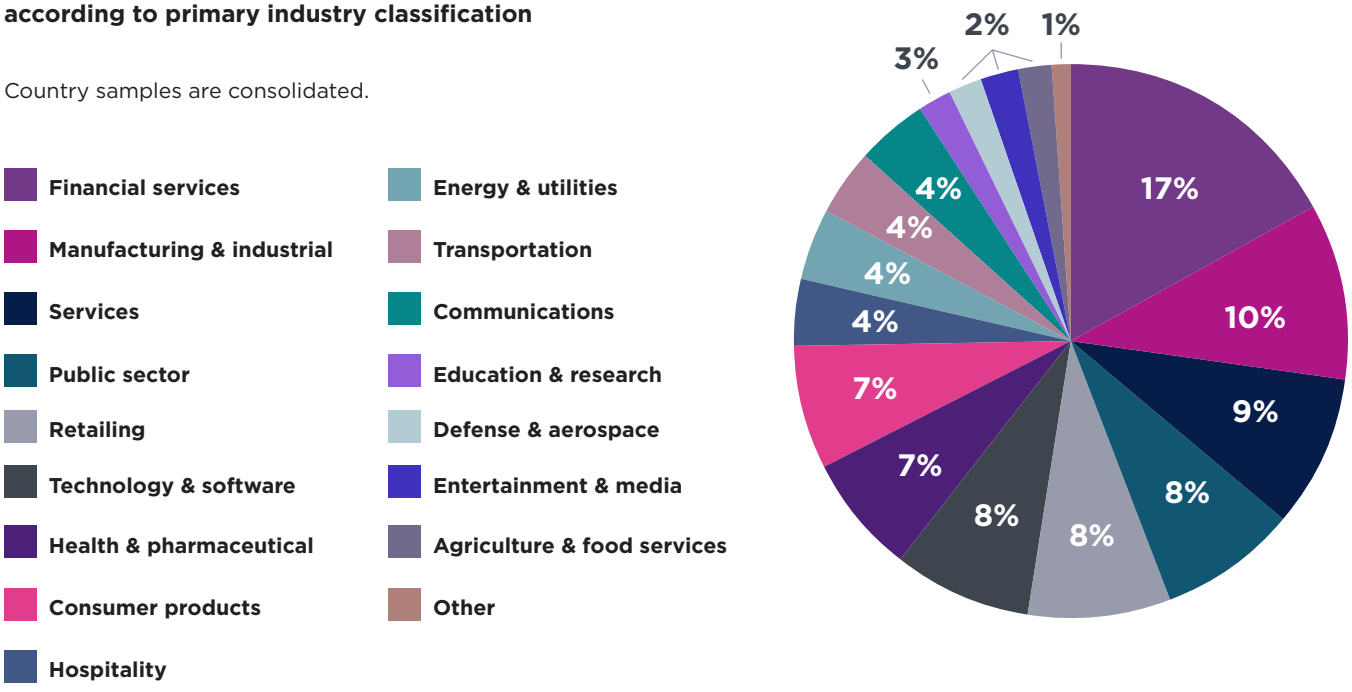



Figure 27 reports the industry classification of respondents' organizations. Seventeen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments, and credit cards. Ten percent of respondents are located in manufacturing and industrial organizations, 9 percent of respondents are in services. This is followed by public sector, retailing, and technology and software (each at 8 percent of respondents).

**Figure 27. Distribution of respondents according to primary industry classification**

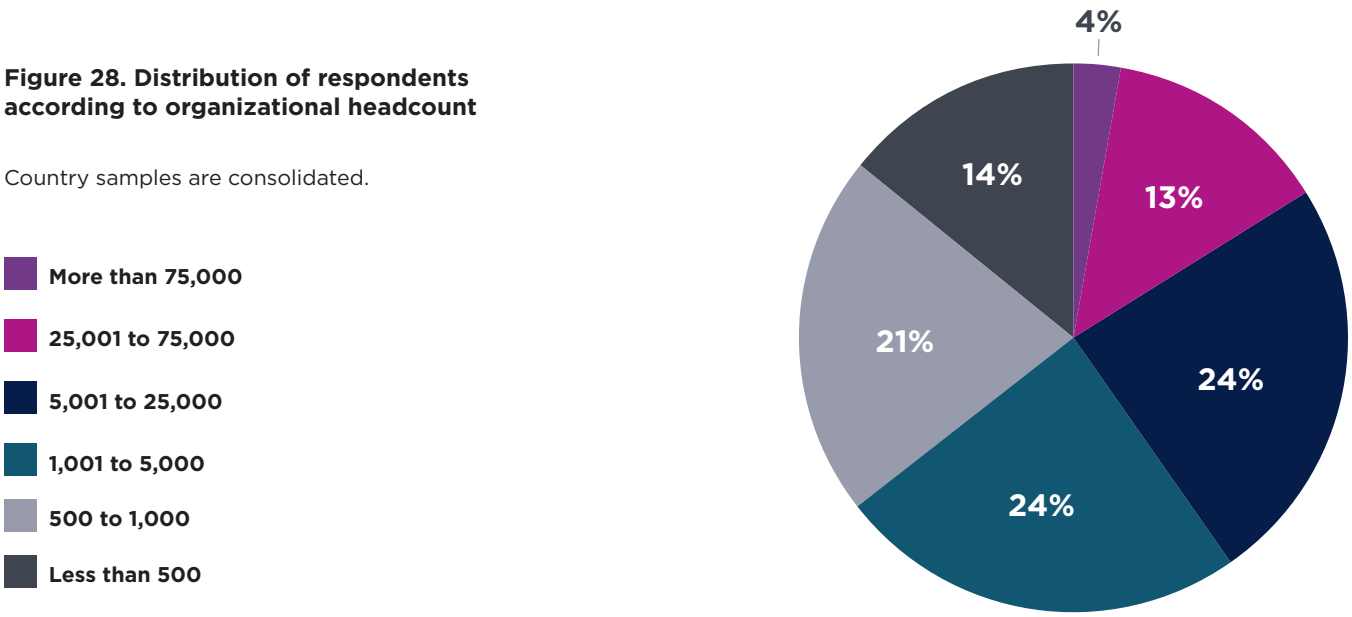
Country samples are consolidated.



According to Figure 28, 65 percent of respondents are located in organizations with a global headcount of more than 1,000 employees.

**Figure 28. Distribution of respondents according to organizational headcount**

Country samples are consolidated.




## Limitations

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

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners in nine countries, 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 survey.
- **Sampling-frame bias:** The accuracy of survey results is dependent upon the degree to which our sampling frames are representative of individuals who are IT or IT security practitioners within the sample of nine countries selected.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process including sanity checks, there is always the possibility that some respondents did not provide truthful responses.

# Appendix 2.

## Survey Data Tables

The following tables provide the consolidated results for nine country/region samples.

| 2024 Survey Response | Global |
|---|---|
| Sampling frame | 80,307 |
| Total returns | 4,377 |
| Rejected or screened surveys | 325 |
| Overall sample (encryption trends) | 4,052 |
| PKI subsample | 2,176 |
| Ratio subsample to overall sample | 54% |
| | 5.0% |

**Part 1. Zero Trust practices**

| Q1. Which best describes the current stage of Zero Trust in your organization? | Global |
|---|---|
| Zero Trust is not a priority at this time (please skip to Q8a) | 17% |
| Zero Trust is on our organization's roadmap (please skip to Q8a) | 21% |
| Our organization has started exploring various solutions to help implement its Zero Trust strategy | 18% |
| Our organization has laid the foundations for a Zero Trust strategy | 14% |
| Our organization has implemented some Zero Trust principles | 12% |
| Our organization has implemented all Zero Trust principles | 18% |
| Total | 100% |

| **Q2. What is the most important driver to implementing a Zero Trust strategy?** Please select one choice only. | **Global** |
|---|---|
| Regulations and standards | 29% |
| The risk of a data breach and/or other security incidents | 37% |
| Expanding attack surface | 30% |
| Other (please specify) | 4% |
| Total | 100% |

| **Q3. Is your organization's encryption plan or strategy included or will it be included as part of the corporate Zero Trust strategy?** Please select one choice only. | **Global** |
|---|---|
| Yes | 57% |
| No | 43% |
| Total | 100% |

| **Q4. Please rate the level of senior leaders' support for an enterprise-wide Zero Trust strategy on a scale from 1 = no support to 10 = very significant support.** | **Global** |
|---|---|
| 1 or 2 | 12% |
| 3 or 4 | 10% |
| 5 or 6 | 19% |
| 7 or 8 | 29% |
| 9 or 10 | 30% |
| Total | 100% |

| **Q5. What are the top two challenges when implementing a Zero Trust strategy?** Please select only two choices. | **Global** |
|---|---|
| Lack of in-house expertise | 47% |
| Lack of an adequate budget | 40% |
| Lack of leadership buy-in | 37% |
| Selection of vendors | 36% |
| Integration of solutions | 35% |
| Other (please specify) | 5% |
| Total | 200% |

| **Q6. Which risk area has the highest priority for your Zero Trust strategy?** Please select one choice only. | **Global** |
|---|---|
| Identities | 40% |
| Devices | 24% |
| Networks | 14% |
| Applications | 13% |
| Data | 9% |
| Total | 100% |

| **Q7. Which is the most important capability your organization needs to support its Zero Trust strategy?** Please select only one choice. | **Global** |
|---|---|
| Best-of-breed solutions | 44% |
| An integrated solution ecosystem from one to three vendors | 22% |
| Lowest-cost option that meets our Zero Trust strategy requirements | 13% |
| Solutions from a managed security service provider | 10% |
| A single vendor | 8% |
| We don't have an encryption plan or strategy | 3% |
| Total | 100% |

**Part 2. Post-quantum cryptography**

| **Q8a. Does your organization plan to migrate to post-quantum cryptography (PQC) within the next five years?** | **Global** |
|---|---|
| Yes | 61% |
| No (please skip to Q14) | 31% |
| Unsure (please skip to Q14) | 8% |
| Total | 100% |

| **Q8b. If yes, how will your organization achieve migration?** Please select one choice only. | **Global** |
|---|---|
| Implement pure PQC | 36% |
| A hybrid approach combining traditional crypto with PQC | 31% |
| Test PQC with our organization's systems and applications | 26% |
| Other (please specify) | 7% |
| Total | 100% |

| Q9. Do you have full visibility into your entire cryptographic estate (e.g., keys, certificates, secrets, libraries and algorithms) across environments? | Global |
|---|---|
| Yes | 45% |
| No | 44% |
| Unsure | 11% |
| Total | 100% |

| Q10. Does your organization have the right technology to support the larger key lengths and computing power required with PQC? | Global |
|---|---|
| Yes | 50% |
| No | 41% |
| Unsure | 9% |
| Total | 100% |

| Q11a. Is your organization preparing for the post-quantum threat? | Global |
|---|---|
| Yes | 41% |
| No, we have not yet considered the impact of the quantum threat (please skip to Q12) | 27% |
| No, we are aware of the potential impact but haven't started to create a strategy (please skip to Q12) | 23% |
| Unsure (please skip to Q12) | 9% |
| Total | 100% |

| **Q12. What are your greatest concerns when it comes to the quantum threat and migration to PQC?** Please select your top three choices only. | **Global** |
|---|---|
| The inability to improve the discovery/inventory of our organization's cryptographic assets (e.g., keys, certificates, secrets, algorithms, etc.) | 43% |
| The inability to have an enterprise-wide strategy | 37% |
| Not having an adequate budget | 31% |
| Not having in-house expertise | 28% |
| Not having senior leadership and board sponsorship | 27% |
| Not having the right scale and technologies to support the extra computing power required by new algorithms | 38% |
| The post-quantum cryptographic algorithms proposed are new and may not be secure after deployment | 40% |
| The ability to test all our organization's systems, endpoints, and networks and manage the transition | 32% |
| The "harvest now, decrypt later" threat due to long-term encrypted data that is at risk | 24% |
| Total | 300% |

| **Q13. What is the current state of your organization's crypto-agility?** Please select one choice only. | **Global** |
|---|---|
| Our organization has a fully implemented crypto-agile approach | 28% |
| Our organization has some level of crypto-agility | 28% |
| Our organization is defining crypto-agility processes | 24% |
| Our organization plans to implement a crypto-agilite approach but has not started as of yet | 15% |
| Do not know | 5% |
| Total | 100% |

**Part 3. Encryption posture**

| **Q14. What most influences your organization's security investment decisions?** Please select your top two choices. | **Global** |
|---|---|
| To reduce the risks of a potential data breach or other security incident | 41% |
| The increasing attack surface | 30% |
| The disappearing perimeter | 30% |
| To reduce complexity and inefficiencies in our organization's IT security infrastructure | 37% |
| Compliance with regulations | 26% |
| To improve visibility into our organization's applications and network | 31% |
| Other (please specify) | 5% |
| Total | 200% |

| **Q15. How important are the following features associated with encryption solutions that may be used by your organization?** 1 = not important to 5 = very important | **Global** |
|---|---|
| Enforcement of policy | 3.68 |
| Management of keys | 3.80 |
| Support for multiple applications or environments | 3.24 |
| Separation of duties and role-based controls | 3.02 |
| System scalability | 3.08 |
| Tamper resistance by dedicated hardware (e.g., HSM) | 3.24 |
| Integration with other security tools (e.g., SIEM and ID management) | 3.35 |
| Support for regional segregation (e.g., data residency) | 2.93 |
| System performance and latency | 3.43 |
| Support for emerging algorithms (e.g., ECC) | 3.08 |
| Support for cloud and on-premises deployment | 2.60 |
| Formal product security certifications (e.g., FIPS 140) | 3.14 |

| **Q16. Where is your encrypted data stored?** Please select one choice only. | **Global** |
|---|---|
| On-premises storage | 28% |
| On-premises and in single cloud service provider | 24% |
| On-premises and in multiple cloud service providers | 27% |
| Across multiple cloud service providers | 21% |
| Total | 100% |

| **Q17. What are the main areas of concern that might result in the exposure of sensitive or confidential data?** Please select three choices only. | **Global** |
|---|---|
| Hackers | 46% |
| Malicious insiders | 27% |
| System or process malfunction | 39% |
| Employee mistakes | 30% |
| Temporary or contract workers | 32% |
| Third-party service providers | 25% |
| Lawful data request (e.g. by police) | 10% |
| Government eavesdropping | 30% |
| Unmanaged certificates | 37% |
| “Harvest now, decrypt later” post-quantum attacks | 24% |
| Total | 300% |

**Part 4. Credential management**

| **Q18. Please rate the overall "pain" associated with managing credentials (keys, certificates and secrets) within your organization, where 1 = minimal impact to 10 = severe impact.** | **Global** |
|---|---|
| 1 or 2 | 10% |
| 3 or 4 | 13% |
| 5 or 6 | 18% |
| 7 or 8 | 28% |
| 9 or 10 | 31% |
| Total | 100% |

| **Q19. What makes the management of credentials painful?** Please select three choices only. | **Global** |
|---|---|
| No clear ownership | 47% |
| Insufficient personnel | 46% |
| Lack of skilled personnel | 50% |
| No clear understanding of requirements | 39% |
| Key management tools are inadequate | 32% |
| Systems are isolated and fragmented | 29% |
| Technology and standards are immature | 28% |
| Manual processes are prone to errors and unreliable | 29% |
| Total | 300% |

| **Q20. Following are a variety of keys that may be managed by your organization. Please rate the overall "pain" associated with managing each type of key using the adjacent 5-point scale.** (Percentage very painful and painful responses combined.) | **Global** |
|---|---|
| Encryption keys for backups and storage | 36% |
| Encryption keys for archived data | 28% |
| Keys associated with TLS/SSL | 31% |
| SSH keys | 27% |
| End-user encryption keys (e.g., email, full disk encryption) | 26% |
| Signing keys (e.g., code signing, digital signatures) | 25% |
| Payments-related keys (e.g., ATM, POS, etc.) | 23% |
| Keys to embed into devices (e.g. at the time of manufacture in device production environments, or for IoT devices you use) | 22% |
| Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys | 22% |

| **Q21a. Is the management of credentials becoming more challenging in a multi-cloud and cross-cloud environment?** | **Global** |
|---|---|
| Yes | 55% |
| No | 45% |
| Total | 100% |

| **Q21b. If yes, why is it more challenging?** Please select all that apply. | **Global** |
|---|---|
| Harder to have visibility over credentials that protect and enable access to critical data and applications | 33% |
| Harder to consistently apply security policies over credentials used across cloud services | 36% |
| Harder to remain in control over the credentials used to protect data in the cloud | 31% |
| Total | 100% |

| **Q22. Which applications are requiring the use of credential management across cloud-based deployments?** Please select your top two choices. | **Global** |
|---|---|
| Databases, backup, and storage | 43% |
| KMIP-compliant applications | 44% |
| Privileged access management | 41% |
| Bring Your Own Key/Hold Your Own Key | 35% |
| Tokenization | 37% |
| Total | 200% |

**Part 5. Hardware Security Modules (HSMs)**

| **Q23. What best describes your level of knowledge about HSMs?** | **Global** |
|---|---|
| Very knowledgeable | 36% |
| Knowledgeable | 30% |
| Somewhat knowledgeable | 20% |
| No knowledge (please skip to Q27) | 14% |
| Total | 100% |

| **Q24. Does your organization use HSMs?** | **Global** |
|---|---|
| Yes | 55% |
| No | 45% |
| Total | 100% |

| **Q25. For what purpose does your organization presently deploy or plan to use HSMs?** Please select all that apply. (HSMs used today.) | **Global** |
|---|---|
| Application-level encryption | 60% |
| Database encryption | 58% |
| Big Data encryption | 49% |
| Public cloud encryption including for Bring Your Own Key (BYOK) | 46% |
| Private cloud encryption | 40% |
| TLS/SSL including firewalls and application delivery controllers | 57% |
| Internet of Things (IoT) root of trust | 47% |
| Key management root of trust | 45% |
| Document signing (e.g. electronic invoicing) | 44% |
| Code signing | 45% |
| Payment transaction processing or payment credential issuing/provisioning | 41% |
| With Cloud Access Security Brokers (CASBs) for encryption key management | 42% |
| Container encryption/signing services | 44% |
| With Privileged Access Management (PAM) solutions to protect administrative access | 42% |
| With Secrets Management solutions to protect secrets storage | 42% |
| Blockchain applications (e.g., cryptocurrency, financial transfers) | 41% |
| Other (please specify) | 5% |
| Total | 748% |

| **Q25. For what purpose does your organization presently deploy or plan to use HSMs?** Please select all that apply. (HSMs planned to be used in the next 12 months) | **Global** |
|---|---|
| Application-level encryption | 65% |
| Database encryption | 63% |
| Big Data encryption | 62% |
| Public cloud encryption including for Bring Your Own Key (BYOK) | 44% |
| Private cloud encryption | 43% |
| TLS/SSL including firewalls and application delivery controllers | 58% |
| Internet of Things (IoT) root of trust | 51% |
| Key management root of trust | 50% |
| Document signing (e.g. electronic invoicing) | 52% |
| Code signing | 49% |
| Payment transaction processing or payment credential issuing/provisioning | 45% |
| With Cloud Access Security Brokers (CASBs) for encryption key management | 44% |
| Container encryption/signing services | 46% |
| With Privileged Access Management (PAM) solutions to protect administrative access | 46% |
| With Secrets Management solutions to protect secrets storage | 42% |
| Blockchain applications (e.g., cryptocurrency, financial transfers) | 41% |
| Other (please specify) | 5% |
| Total | 806% |

| Q26a Does your organization use HSMs to secure PKI? | Global |
|---|---|
| Yes | 51% |
| No | 49% |
| Total | 100% |

| **Q26b. If yes, where are they deployed?** Please select all that apply. | Global |
|---|---|
| Offline root CA | 42% |
| Online root CA | 47% |
| Issuing CA | 40% |
| Policy CA | 28% |
| Registration Authority | 24% |
| OCSP Responder | 19% |
| Validation Authority | 18% |
| Total | 218% |

**Part 5. Hardware Security Modules (HSMs)**

When responding to the following questions, please assume the questions apply only to public cloud services.

| Q27. Do you currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism)? | Global |
|---|---|
| Yes, we are presently doing so | 52% |
| No, but we are likely to do so in the next 12 to 24 months | 28% |
| No | 20% |
| Total | 100% |

| **Q28. How does your organization protect data at rest in the cloud?** Please select one choice only. | **Global** |
|---|---|
| Encryption performed in the cloud using keys generated/managed by the cloud provider | 39% |
| Encryption performed in the cloud using keys my organization generates and manages on-premises | 28% |
| Encryption performed on-premises prior to sending data to the cloud using keys my organization generates and manages | 23% |
| None of the above | 10% |
| Total | 100% |

| **Q29. For encryption of data at rest in the cloud, what is your organization's strategy?** Please select one choice only. | **Global** |
|---|---|
| Only use keys controlled by my organization | 22% |
| Only use keys controlled by the cloud provider | 24% |
| Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by my organization | 32% |
| Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by the cloud provider | 22% |
| Total | 100% |

| **Q30. How important are the following features associated with cloud encryption to your organization?** Scale: 1 = not important to 5 = very important (Percentage very important and important responses combined.) | **Global** |
|---|---|
| Bring Your Own Key (BYOK) management support | 3.89 |
| Privileged user access control | 4.38 |
| Granular access controls | 4.19 |
| Audit logs identifying key usage | 3.70 |
| Audit logs identifying data access attempts | 2.98 |
| SIEM integration, visualization, and analysis of logs | 3.42 |
| Support for FIPS 140-2 compliant key management | 2.82 |
| Support for the KMIP standard for key management | 3.33 |

| | |
|---|---|
| Unified key management solution across multiple clouds and enterprise | 3.73 |
| Ability to encrypt and rekey data while in use without downtime | 4.02 |
| Total | 3.65 |

| Q31a. How many public cloud providers does your organization use today? | Global |
|---|---|
| 1 | 11% |
| 2 | 27% |
| 3 | 39% |
| 4 or more | 23% |
| Total | 100% |

| Q31b. How many public cloud providers does your organization use in the next 12 to 24 months? | Global |
|---|---|
| 1 | 10% |
| 2 | 29% |
| 3 | 35% |
| 4 or more | 26% |
| Total | 100% |

**Part 7. Public Key Infrastructure (PKI)**

| **Q32. What best describes your role or involvement in your organization's enterprise PKI?** One response permitted. | **Global** |
|---|---|
| I am involved in the management of my organization's PKI | 49% |
| I am involved in developing and/or managing applications that depend upon credentials controlled by my organization's PKI | 51% |
| I am not involved in my organization's PKI or the applications that depend on them (Stop) | 0% |
| My organization does not have a PKI (Stop) | 0% |
| Total | 100% |

| **Q33. Who is most responsible for your organization's PKI strategy?** | **Global** |
|---|---|
| CIO | 17% |
| CISO | 19% |
| IT director | 15% |
| IT manager | 14% |
| IT security manager | 14% |
| IT security director | 9% |
| Technician | 12% |
| Total | 100% |

| **Q34a. Does your organization use orchestration of the PKI software?** | **Global** |
|---|---|
| Yes | 50% |
| No | 50% |
| Total | 100% |

| Q34b. If yes, how complex is the orchestration of the PKI software on a scale of 1 = not complex to 10 = extremely complex? | Global |
|---|---|
| 1 or 2 | 10% |
| 3 or 4 | 13% |
| 5 or 6 | 18% |
| 7 or 8 | 30% |
| 9 or 10 | 29% |
| Total | 100% |

| Q35. What describes how your organization's enterprise PKI is deployed? Please select all that apply. | Global |
|---|---|
| Internal corporate certificate authority (CA) | 60% |
| Externally hosted private CA – managed service | 47% |
| Public CA service | 22% |
| Private CA running within a public cloud | 21% |
| Business partner provided service | 18% |
| Government-provided service | 12% |
| None of the above (Stop) | 0% |
| Total | 180% |

| **Q36. Which certificate revocation technique(s) does your organization deploy?** Please select all that apply. | **Global** |
|---|---|
| Online Certificate Status Protocol (OCSP) | 45% |
| Manual certificate revocation list (CRL) | 37% |
| Automated CRL | 32% |
| Validation Authority | 23% |
| None | 13% |
| Unsure | 7% |
| Total | 157% |

| **Q37. How many root CAs does your organization have?** | **Global** |
|---|---|
| 1 or 2 | 10% |
| 2 or 4 | 11% |
| 5 or 6 | 17% |
| 7 or 8 | 23% |
| 9 or 10 | 18% |
| More than 10 | 13% |
| NA -- We use an external CA service | 8% |
| Total | 100% |
| Extrapolated Average | 6.47 |

| **Q38. What is your organization's primary root CA strategy?** Please select only one choice | **Global** |
|---|---|
| Offline, self-managed | 29% |
| Offline, externally hosted | 29% |
| Online, self-managed | 25% |
| Online, externally hosted | 17% |
| Total | 100% |

| **Q39. How many issuing CAs does your organization have?** | **Global** |
|---|---|
| 1 or 2 | 13% |
| 3 or 4 | 21% |
| 5 or 6 | 24% |
| 7 or 8 | 19% |
| 9 or 10 | 13% |
| More than 10 | 10% |
| NA – We use an external CA service | 0% |
| Total | 100% |
| Extrapolated value | 6.11 |

| Q40. How many certificates does your PKI issue (or have been acquired from an external service)? | Global |
|---|---|
| Less than 10 | 4% |
| 10 to 100 | 8% |
| 101 to 1,000 | 11% |
| 1,001 to 5,000 | 15% |
| 5,001 to 10,000 | 18% |
| 10,001 to 50,000 | 22% |
| 50,001 to 100,000 | 14% |
| More than 100,000 | 8% |
| Cannot determine | 0% |
| Total | 100% |
| Extrapolated value | 31,299 |

| Q41. How many distinct applications (e.g., email, network authentication, etc.) does your PKI manage certificates on behalf of? | Global |
|---|---|
| 1 to 2 | 4% |
| 3 to 4 | 8% |
| 5 to 6 | 11% |
| 7 to 8 | 15% |
| 9 to 10 | 20% |
| 11 to 12 | 22% |
| 13 to 14 | 12% |
| 15 or more | 8% |
| Total | 100% |
| Extrapolated value | 9.5 |

| Q42a. Do you have PKI specialists on staff? | Global |
|---|---|
| Yes | 52% |
| No | 48% |
| Total | 100% |

| Q42b. If not, does your organization rely on consultants or a service provider? One response permitted | Global |
|---|---|
| Rely on consultants | 45% |
| Rely on service provider | 55% |
| Total | 100% |

| Q43. Does your organization use any of the following to manage the private keys for your root/policy/issuing CAs? | Global |
|---|---|
| Smart cards (for CA/root key protection) | 41% |
| Removable media for CA/root keys | 31% |
| Software key store | 17% |
| None of the above | 11% |
| Total | 100% |

| **Q44. What are the main challenges in deploying and managing PKI?** Please select 4 top choices. | **Global** |
|---|---|
| No clear ownership | 51% |
| Insufficient personnel | 41% |
| Insufficient skills | 43% |
| Lack of clear understanding of the requirements | 38% |
| Requirements are too fragmented or inconsistent | 43% |
| No suitable products or technologies available | 31% |
| Necessary performance and reliability is hard to achieve | 35% |
| Commercial solutions are too complicated or too expensive | 37% |
| Lack of visibility of the applications that will depend on PKI | 33% |
| Lack of advisory services and support | 16% |
| Too hard to transition from current approach to a new system | 26% |
| Other (please specify) | 6% |
| Total | 400% |

| **Q45. As you plan the evolution of your PKI, where are the greatest areas of possible change and uncertainty?** Please select 3 top choices. | **Global** |
|---|---|
| PKI technologies | 43% |
| Vendors (products and services) | 41% |
| Enterprise applications | 32% |
| Internal security policies | 32% |
| External mandates and standards | 37% |
| Budget and resources | 30% |
| Management expectations | 32% |
| New applications (e.g., Internet of Things) | 28% |
| Post-quantum threat and migration to PQC | 25% |
| Other (please specify) | 0% |
| Total | 300% |

| **Q46. In your opinion, which security certifications are important when deploying PKI infrastructure?** Please select all that apply. | **Global** |
|---|---|
| Common Criteria EAL Level 4+ | 57% |
| FIPS 140-2 Level 3 | 55% |
| Regional certifications for use by government | 27% |
| Regional standards such as digital signature laws | 29% |
| Other (please specify) | 1% |
| None of the above (certification is not an important factor) | 14% |
| Total | 183% |

| **Q47. What applications use PKI credentials in your organization?** Please select all that apply. | **Global** |
|---|---|
| SSL certificates for public-facing websites and services | 64% |
| Private networks and VPN | 56% |
| Email security | 47% |
| Enterprise user authentication | 51% |
| Mobile device authentication | 60% |
| Document/message signing | 49% |
| Code signing | 43% |
| Public cloud-based applications and services | 55% |
| Private cloud-based applications | 56% |
| IoT devices/endpoints | 49% |
| Other (please specify) | 2% |
| Total | 532% |

| **Q48. In your opinion, what are the most important trends that are driving the deployment of applications that make use of PKI?** Please select 2 top choices. | **Global** |
|---|---|
| Consumer mobile | 38% |
| Cloud-based services | 46% |
| BYOD and internal mobile device management | 34% |
| Internet of Things (IoT) | 39% |
| Regulatory environment | 33% |
| E-commerce | 10% |
| Total | 200% |

| **Q49. What are the challenges to deploying PKI-enabled applications?** Please select four choices only. | **Global** |
|---|---|
| No pre-existing PKI | 36% |
| Existing PKI is incapable of supporting new applications | 34% |
| Insufficient resources | 35% |
| Insufficient skills | 37% |
| Lack of clear understanding of requirements | 35% |
| Too much change or uncertainty | 36% |
| Requirements are too fragmented or inconsistent | 33% |
| No ability to change legacy apps | 35% |
| Lack of visibility of the security capabilities of existing PKI | 34% |
| Conflict with other apps using the same PKI | 36% |
| Specific operational issues (such as revocation and performance) are hard to resolve | 27% |
| Lack of advisory support | 18% |
| Other (please specify) | 4% |
| Total | 400% |

| **Q50. What are the most important PKI capabilities for IoT deployments?** Please select three choices only. | **Global** |
|---|---|
| Support for Elliptic Curve Cryptography (ECC) | 52% |
| Scalability to millions of managed certificates | 53% |
| Online revocation | 46% |
| Ability to sign firmware for IoT devices | 31% |
| FIPS 140-2 Level 3 HSMs (Hardware Security Modules) for Root and Issuing CAs | 38% |
| Cloud deployment model | 32% |
| Cloud signing for software | 31% |
| Machine identity lifecycle management | 17% |
| Total | 300% |

| **Q51. What percentage of IoT devices that will likely be used by your organization in the next two years do you believe will rely primarily on digital certificates for identification/authentication?** | **Global** |
|---|---|
| None | 4% |
| Less than 20% | 20% |
| 20% to 40% | 19% |
| 40 to 60% | 21% |
| 60 to 80% | 20% |
| 80 to100% | 16% |
| Total | 100% |
| Extrapolated value | 47% |

| **Q52a. How important are the following IoT security capabilities to your organization today?** 5-point scale from 1 = not important to 5 = very important. (Percentage very important and important responses) | **Global** |
|---|---|
| Device discovery | 3.7 |
| Device authentication | 3.7 |
| Monitoring device behavior | 4.0 |
| Delivery of patches and updates to devices | 3.9 |
| Protecting confidentiality and integrity of data collected from the device | 3.6 |
| Average | 3.8 |

| **Q52b. How important are the following IoT security capabilities to your organization in the next 12 months?** 5-point scale from 1 = not important to 5 = very important. (Percentage very important and important responses) | **Global** |
|---|---|
| Device discovery | 3.9 |
| Device authentication | 4.0 |
| Monitoring device behavior | 4.0 |
| Delivery of patches and updates to devices | 4.1 |
| Protecting confidentiality and integrity of data collected from the device | 3.7 |
| Average | 4.0 |

### Role and organizational characteristics

| D1. What organizational level best describes your current position? | Global |
|---|---|
| IT operations | 8% |
| Security | 8% |
| Compliance | 20% |
| Finance | 33% |
| Lines of business (LOB) | 31% |
| Other | 0% |
| Total | 100% |

| D2. Select the functional area that best describes your organizational location. | Global |
|---|---|
| IT operations | 40% |
| Security | 16% |
| Compliance | 15% |
| Finance | 7% |
| Lines of business (LOB) | 16% |
| Other | 6% |
| Total | 100% |

| D3. Total years of business experience | Global |
|---|---|
| Total years of security experience | 12.0 |
| Total years in current position | 6.2 |

| D4. What industry best describes your organization's industry focus? | Global |
|---|---|
| Agriculture & food services | 2% |
| Communications | 4% |
| Consumer products | 7% |
| Defense & aerospace | 2% |
| Education & research | 3% |
| Energy & utilities | 4% |
| Entertainment & media | 2% |
| Financial services | 17% |
| Health & pharmaceutical | 7% |
| Hospitality | 4% |
| Manufacturing & industrial | 10% |
| Public sector | 8% |
| Retailing | 8% |
| Services | 9% |
| Technology & software | 8% |
| Transportation | 4% |
| Other | 1% |
| Total | 100% |

| D5. Where are your employees located? Please select all that apply. | Global |
|---|---|
| United States | 65% |
| Canada | 46% |
| Europe | 71% |
| Middle east & Africa | 41% |
| Asia-Pacific | 70% |
| Latin America | 33% |
| Total | 326% |

| D6. What is the worldwide headcount of your organization? | Global |
|---|---|
| Less than 500 | 14% |
| 500 to 1,000 | 21% |
| 1,001 to 5,000 | 24% |
| 5,001 to 25,000 | 24% |
| 25,001 to 75,000 | 13% |
| More than 75,000 | 4% |
| Total | 100% |