ENTRUST | Ponemon INSTITUTE

The data is in the cloud, but who's in control?

2022 GLOBAL ENCRYPTION TRENDS STUDY

Find out how organizations are using encryption to protect data and workloads across multiple cloud platforms.

01 Executive Summary

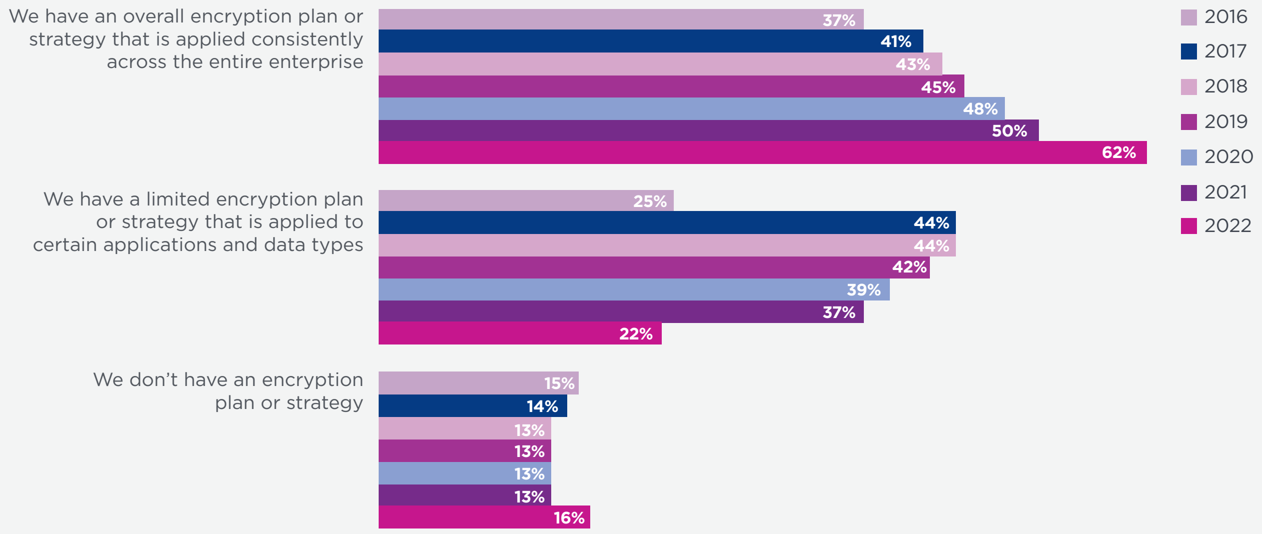
PONEMON INSTITUTE PRESENTS THE FINDINGS OF THE 2022 GLOBAL ENCRYPTION TRENDS STUDY[1]

Ponemon Institute is pleased to present the findings of the 2022 Global Encryption Trends Study, sponsored by Entrust. We surveyed 6,264 individuals across multiple industry sectors in 17 countries/regions – Australia, Brazil, France, Germany, Hong Kong, Japan, Mexico, the Middle East (which is a combination of the respondents located in Saudi Arabia and the United Arab Emirates),[2] Netherlands, the Russian Federation, Spain, Southeast Asia, South Korea, Sweden, Taiwan, the United Kingdom, and the United States.

The purpose of this research is to examine how the use of encryption has evolved over the past 17 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a U.S. sample of respondents.[3] Since then we have expanded the scope of the research to include respondents in all regions of the world.

Organizations with an overall encryption strategy increased significantly since last year. As shown in Figure 1, since 2016 the deployment of an overall encryption strategy has steadily increased. This year, 62% of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise, a significant increase from last year. Only 22% of respondents say they have a limited encryption plan or strategy that is applied to certain applications and data types, a significant decrease from last year. The average annual global budget for IT security is $24 million per organization. The countries with the highest average annual budgets are the U.S. ($41 million) and Germany ($28 million).

Figure 1. **Does your company have an encryption strategy?**
Country samples are consolidated.



[1] This year's data collection was conducted in December 2021 and completed in January 2022.
[2] Country-level results are abbreviated as follows: Australia (AU), Brazil (BZ), France (FR), Germany (DE), Hong Kong (HK), Japan (JP), Korea (KO), Mexico (MX), Middle East (AB), Netherlands (NL), Russia (RF), Spain (SP), Southeast Asia (SA), Sweden (SW), Taiwan (TW), United Kingdom (UK), and United States (US).
[3] The trend analysis shown in this study was performed on combined country samples spanning 17 years (since 2005).

FOLLOWING ARE THE FINDINGS FROM THIS YEAR'S RESEARCH

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies have continued to increase. Since conducting this study 17 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having an encryption plan or strategy. In this year's study, 61% of respondents rate the level of their senior leaders' support for an enterprise-wide encryption strategy as significant or very significant.

Certain countries/regions have more mature encryption strategies. The prevalence of an enterprise encryption strategy varies among the countries/regions represented in this research. The highest prevalence of an enterprise encryption strategy is reported in the United States, the Netherlands, and Germany. Although respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy, since last year it has increased significantly. The global average of adoption is 62% of organizations represented in this research.

Globally, the IT operations function is the most influential in framing the organization's encryption strategy. However, in the United States the lines of business are more influential. IT operations are most influential in the Netherlands, Spain, France, Southeast Asia and the United Kingdom.

The use of encryption has increased in most industries. Results suggest a steady increase in most of the 13 industry sectors represented in this research. The most significant increases in extensive encryption usage occur in manufacturing, energy & utilities and the public sector.

62% of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise.

THREATS, MAIN DRIVERS, AND PRIORITIES

Employee mistakes continue to be the most significant threats to sensitive data. In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests.

Most organizations have suffered at least one data breach. Seventy-two percent of organizations report having experienced at least one data breach. Twenty-four percent say they have never experienced a breach and 5% are unsure.

The main driver for encryption is the protection of customers' personal information. Organizations are using encryption to protect customers' personal information (53% of respondents), to protect information against specific, identified threats (50% of respondents), and the protection of enterprise intellectual property (48% of respondents).

A barrier to a successful encryption strategy is the inability to discover where sensitive data resides in the organization. Fifty-five percent of respondents say discovering where sensitive data resides in the organization is the number one challenge and 32% of respondents say budget constraints is a barrier. Thirty percent of all respondents cite initially deploying encryption technology as a significant challenge.

DEPLOYMENT CHOICES

No single encryption technology dominates in organizations. Organizations have very diverse needs for encryption. In this year's research, backup and archives, internet communications, databases, and internal networks are most likely to be deployed. For the fifth year, the study tracked the deployment of the encryption of Internet of Things (IoT) devices and platforms. Sixty-three percent of respondents say IoT platforms have been at least partially encrypted and 64% of respondents say encryption of IoT devices has been at least partially deployed.

ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others. According to the consolidated findings, system performance and latency, management of keys, and enforcement of policy are the three most important encryption features.

Intellectual property, employee/HR data, and financial records are most likely to be encrypted. The least likely data type to be encrypted is health-related information and non-financial information, which is a surprising result given the sensitivity of health information.

55% of respondents say discovering where sensitive data resides in the organization is the number one challenge.

ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management? Fifty-nine percent of respondents rate key management as very painful, which suggests respondents view managing keys as a very challenging activity. The highest rates of pain occur in Spain and Germany, while France experiences the lowest level of pain. No clear ownership and lack of skilled personnel are the primary reasons why key management is painful. The most difficult to manage are SSH keys, keys for external cloud or hosted services including BYOK keys, and signing keys.

IMPORTANCE OF HSMs

Germany, Middle East, and United States organizations are more likely to deploy HSMs. The Russian Federation is least likely to deploy HSMs. The overall global average deployment rate for HSMs is 49%.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. Forty-four percent of respondents say their organizations own and operate HSMs on-premises, accessed real-time by cloud-hosted applications, and 40% of respondents rent/use HSMs from a public cloud provider. In the next 12 months, the use of HSMs with cloud access security brokers and the ownership and operation of HSMs for the purpose of generating and managing Bring Your Own Key (BYOK) keys to send to the cloud for use by the cloud provider are expected to increase significantly.

Sixty-three percent of respondents globally rate the importance for HSMs as part of an encryption and key management strategy as very important. The pattern of responses suggests Germany, the United States, Hong Kong, and Southeast Asia are most likely to assign importance to HSMs as part of their organizations' encryption or key management activities.

What best describes an organization's use of HSMs? Fifty-five percent of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model). Forty-five percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional siloed application-specific data center deployment approach.

The top three uses are (1) application-level encryption, (2) TLS/SSL, followed by (3) container encryption/signing services. There will be a significant increase in the use of HSMs for database encryption 12 months from now.

55% of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted.

CLOUD ENCRYPTION

Fifty-five percent of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking. Another 27% of respondents expect to do so in the next one to two years. These findings indicate the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

How do organizations protect data at rest in the cloud? Forty-four percent of respondents say encryption is performed in the cloud using keys generated and managed by the cloud provider. However, 38% of respondents say encryption is performed on-premises prior to sending data to the cloud using keys their organization generates and manages. Twenty-one percent of respondents are using some form of BYOK approach.

The top three encryption features specifically for the cloud are support for the KMIP standard for key management (61% of respondents), SIEM integration, visualization, and analysis of logs (59% of respondents), and granular access controls (59% of respondents).

02 Key Findings

IN THIS SECTION, WE PROVIDE A DEEPER ANALYSIS OF THE KEY FINDINGS.

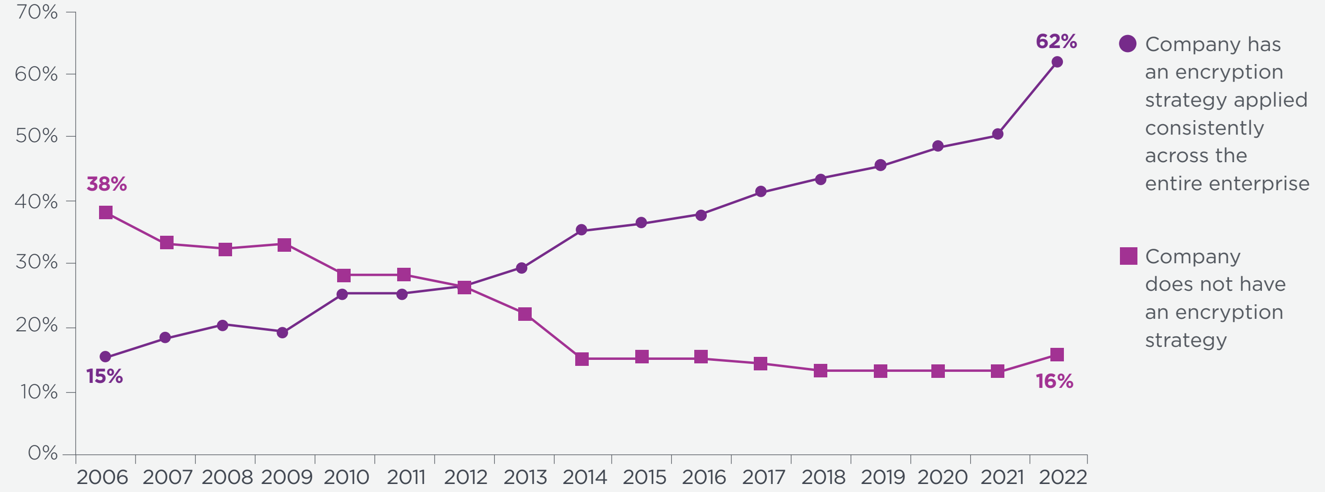
The complete audited findings are presented in the Appendix of the report. We organized the report according to the following themes.

- Strategy and adoption of encryption
- Industry trends in adoption of encryption
- Threats, main drivers, and priorities
- Deployment choices
- Encryption features considered most important
- Attitudes about key management
- Importance of HSMs[4]
- Cloud encryption

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies have continued to increase. Since conducting this study 17 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having an encryption plan or strategy. The results have essentially reversed over the years of the study. Figure 2 shows these changes over time.

Figure 2. **Trends in encryption strategy**
Country samples are consolidated.



[4] HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g., encryption or digital signing) and to manage the keys associated with those processes. These devices are used to protect critical data processing activities and can be used to strongly enforce security policies and access controls. HSMs are typically validated to formal security standards such as FIPS 140-2.

Certain countries/regions have more mature encryption strategies. According to Figure 3, the prevalence of an enterprise encryption strategy varies among the countries/regions represented in this research. The highest prevalence of an enterprise encryption strategy is reported in the United States, the Netherlands, and Germany.

Although respondents in the Russian Federation and Brazil report a low adoption of an enterprise encryption strategy since last year it has increased significantly from 26% and 28% to 50% and 52% of respondents, respectively. The global average of adoption is 62%.

Figure 3. **Differences in enterprise encryption strategies by country/region**

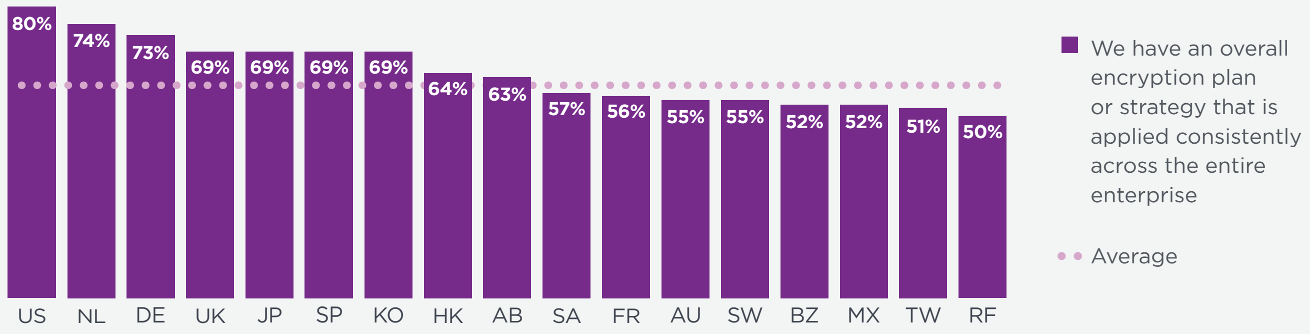
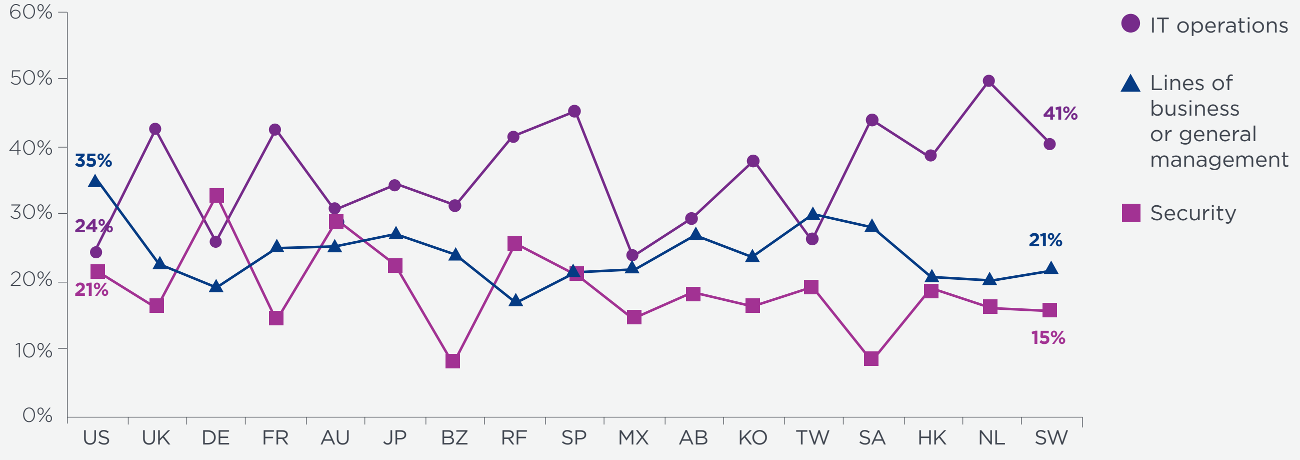


Figure 4 shows that the IT operations function remains the most influential in framing the organization's encryption strategy since the research commenced. However, in the United States the lines of business are more influential than IT operations.

A possible reason why the lines of business are more influential than IT operations in the United States is because of the growing adoption of IoT devices in the workplace, proliferation of employee-owned devices or BYOD, and the general consumerization of IT. A consequence is that lines of business are required to be more accountable for the security of these technologies.

Figure 4. **Influence of IT operations, lines of business, and security**
Country samples are consolidated.

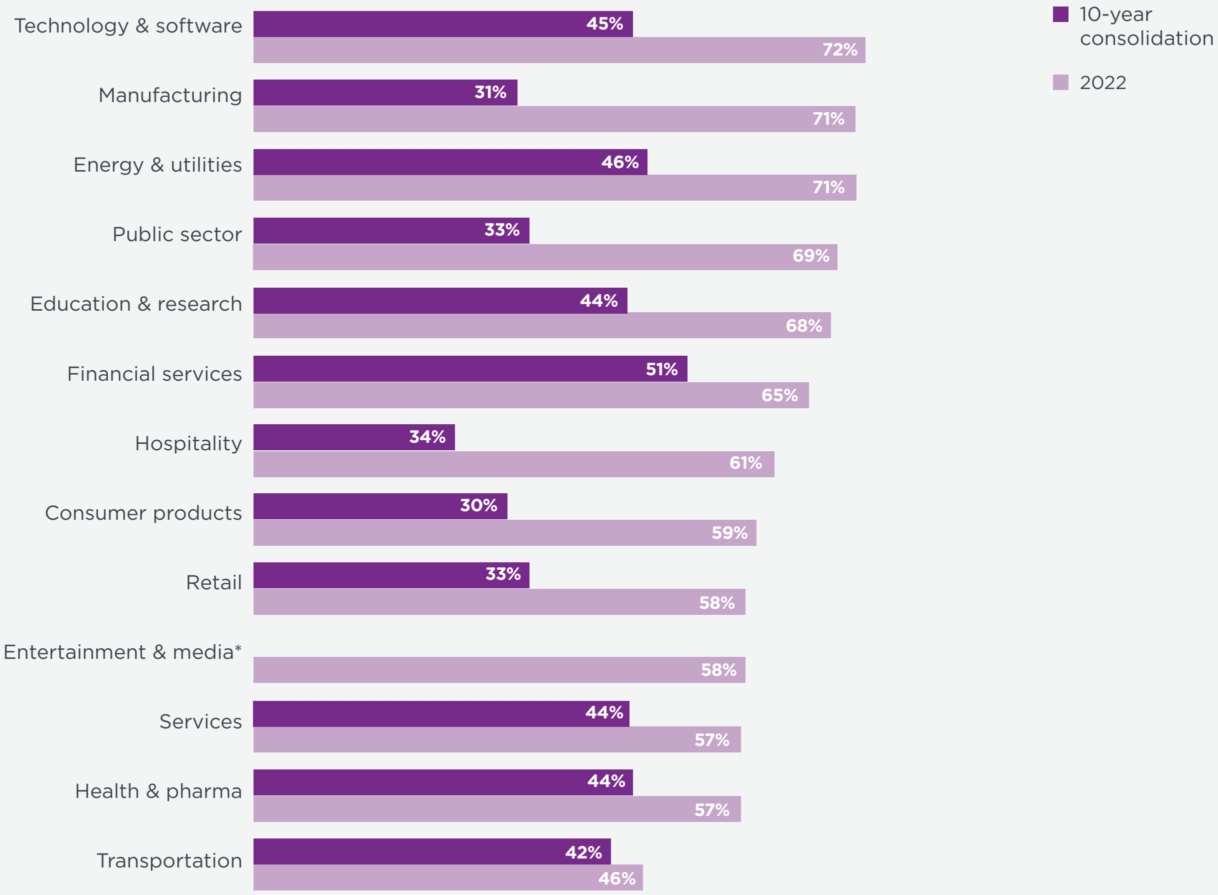


INDUSTRY TRENDS IN ENCRYPTION ADOPTION

The use of encryption increases in most industries. Figure 5 shows the current year and the nine-year average in the use of encryption solutions for 13 industry sectors. Results suggest steady and significant increases in all industry sectors. The most significant increases in extensive encryption usage have occurred in the manufacturing, energy & utilities, and public sectors.

> The most significant increases in extensive encryption usage have occurred in manufacturing, energy & utilities, and the public sector.

Figure 5. **The extensive use of encryption by industry: Current year versus 10-year average**
Country samples are consolidated. Average of 15 encryption categories.



*Historical data not available

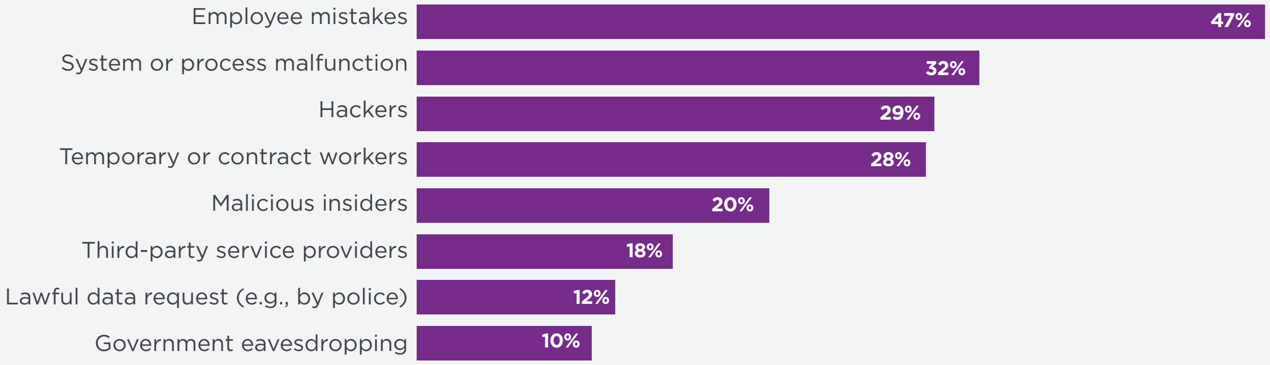
THREATS, MAIN DRIVERS, AND PRIORITIES

The threats from employee mistakes and temporary workers continue to persist, indicating an impact of ongoing labor shortages in security roles.

Employee mistakes continue to be the most significant threats to sensitive data. Figure 6 shows that the most significant threats to the exposure of sensitive or confidential data are employee mistakes, while the threat from temporary or contract workers reached 28%, its highest level ever. This may indicate an impact of the ongoing labor shortage in security roles and the risks introduced by overworked and temporary employees.

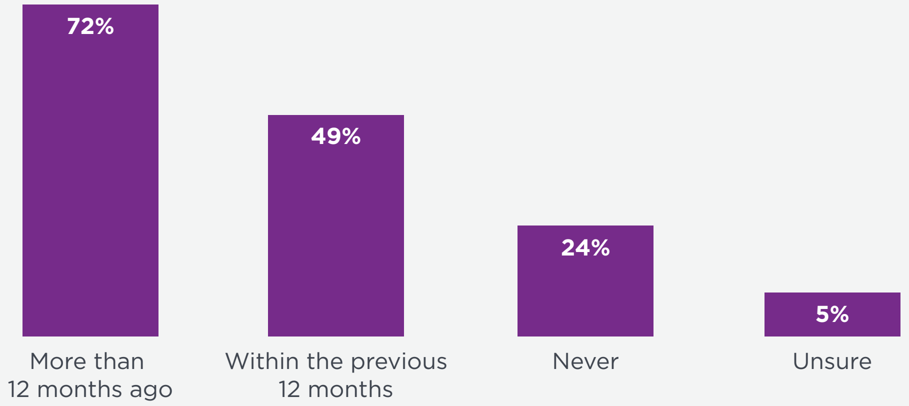
In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests.

Figure 6. **The most salient threats to sensitive or confidential data**
Consolidated country samples. Two choices permitted.



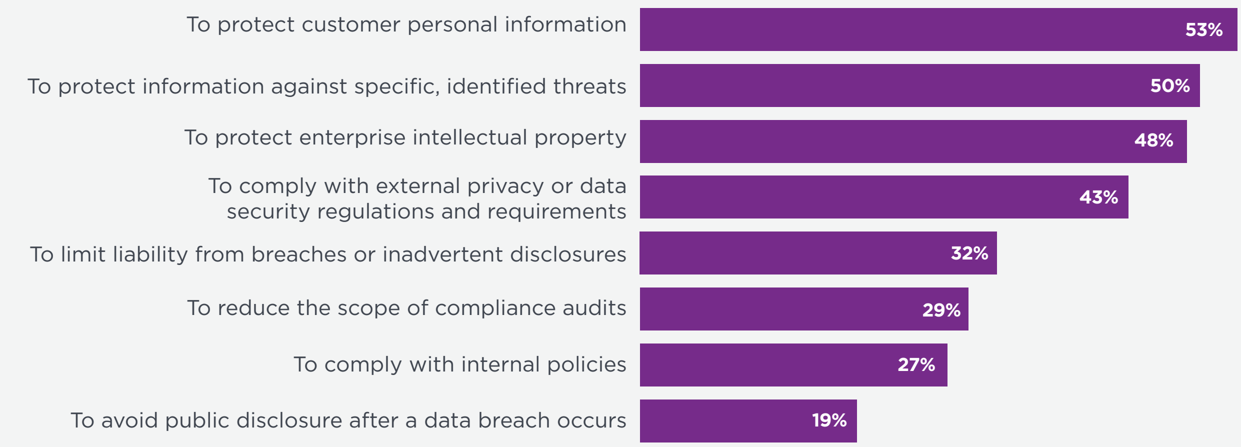
Most surveyed organizations have suffered at least one data breach. Figure 7 shows that most respondents have experienced at least one data breach, with 49% experiencing one within the previous 12 months. Only 24% report never experiencing a data breach.

Figure 7. **Has your organization experienced a data breach?**
More than one response permitted.



The main driver for encryption is protection of customers' personal information. Eight drivers for deploying encryption are presented in Figure 8. Organizations are using encryption to protect customer personal information followed by the protection of information against specific, identified threats and to protect enterprise intellectual property (53%, 50%, and 48% of respondents, respectively).

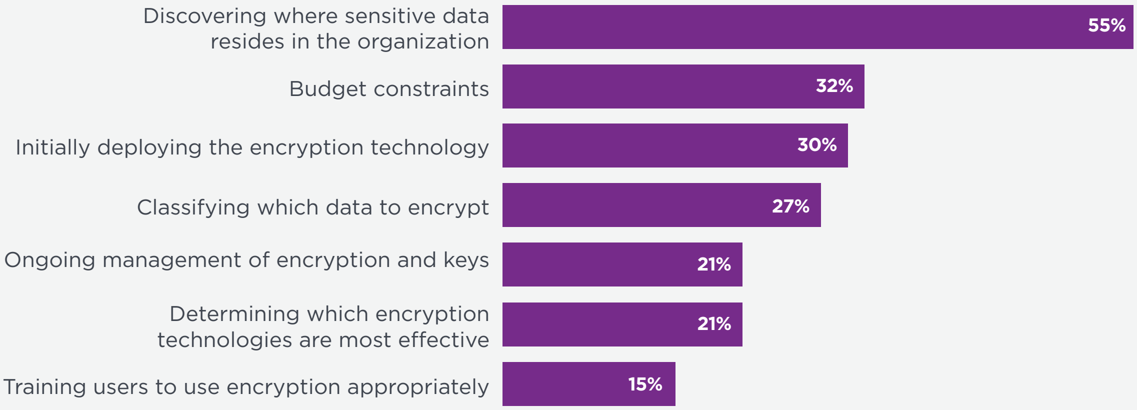
Figure 8. **The main drivers for using encryption technology solutions**
Country samples are consolidated. Three responses permitted.



A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization. Figure 9 provides a list of seven aspects that present challenges to the organization's effective execution of its data encryption strategy in descending order of importance. Fifty-five percent of respondents say discovering where sensitive data resides in the organization is the number one challenge, followed by budget constraints (32% of respondents). Thirty percent of respondents cite initially deploying encryption technology as a significant challenge.

72% of surveyed organizations have suffered at least one data breach; half experienced a breach within the past 12 months.

Figure 9. **Biggest challenges in planning and executing a data encryption strategy**
Country samples are consolidated. More than one choice permitted.



DEPLOYMENT CHOICES

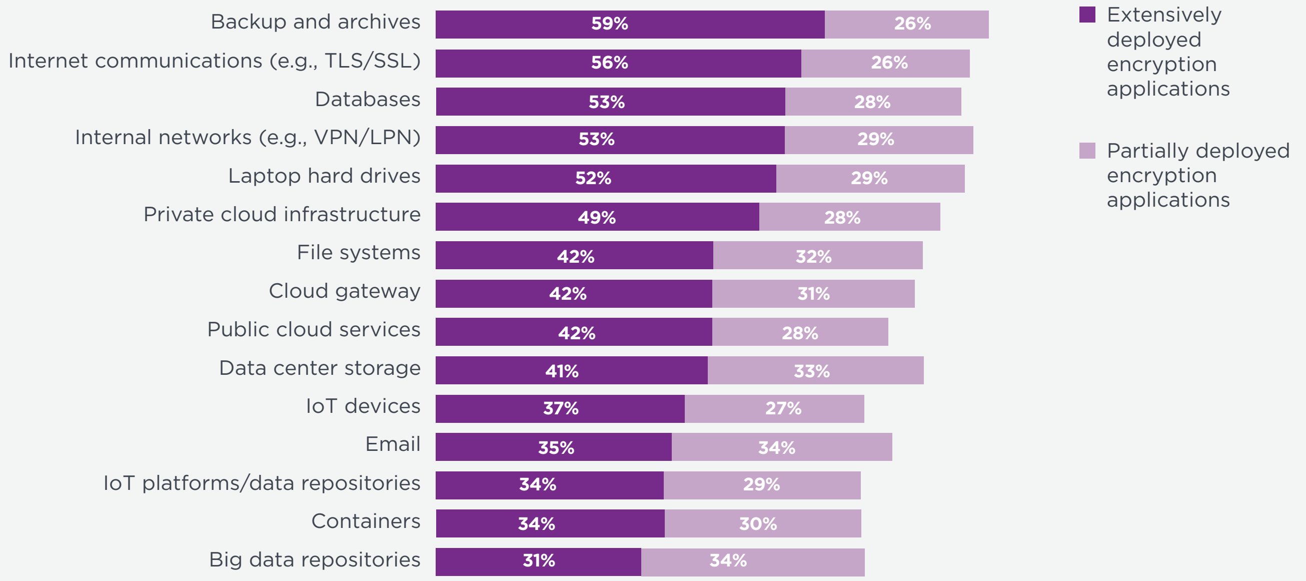
No single encryption technology dominates in organizations. We asked respondents to indicate if specific encryption technologies are widely or only partially deployed within their organizations. "Extensive deployment" means that the encryption technology is deployed enterprise-wide. "Partial deployment" means the encryption technology is confined or limited to a specific purpose (a.k.a., point solution).

Over the past five years, the deployment of encryption has grown the fastest with containers and IoT devices.

As shown in Figure 10, no single technology dominates because organizations have very diverse encryption needs. According to respondents, backup and archives, internet communications, databases, and internal networks are most likely to be extensively or partially encrypted.

Over the past five years, the deployment of encryption has grown the fastest with containers and IoT devices. Both have increased from 49% extensively or partially deployed in 2018 to 64% this year.

Figure 10. **Consolidated view on the use of 15 encryption technologies**
Country samples are consolidated.

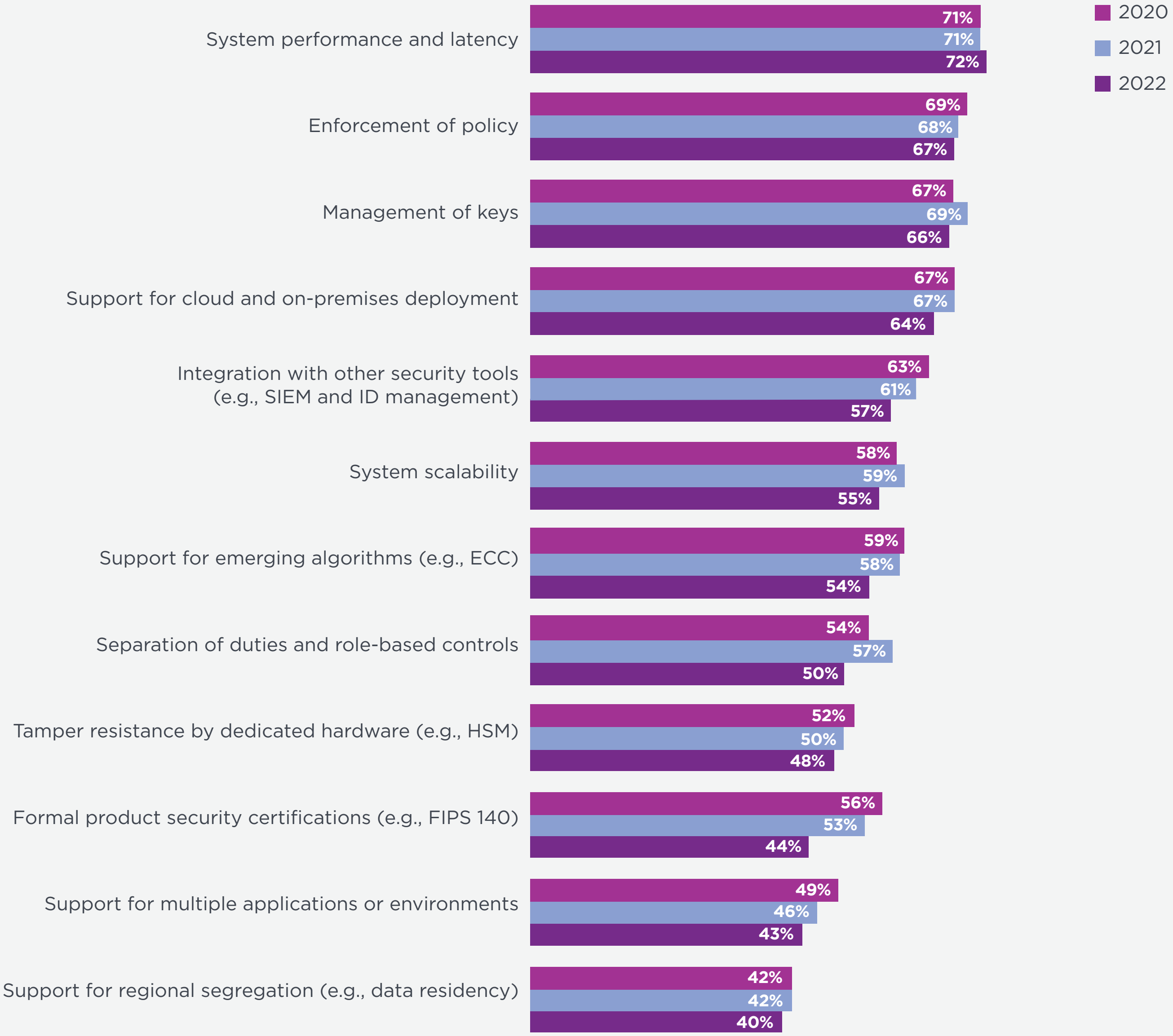


ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others. Figure 11 lists 12 encryption technology features. Each percentage defines the very important and important responses. Respondents were asked to rate encryption technology features considered most important to their organization's security posture.

According to the consolidated findings, system performance and latency, enforcement of policy, and management of keys continue to be the three most important features. The performance finding is not surprising given that encryption in networking is a prominent use case, as well as the often-emphasized requirement for transparency of encryption solutions.

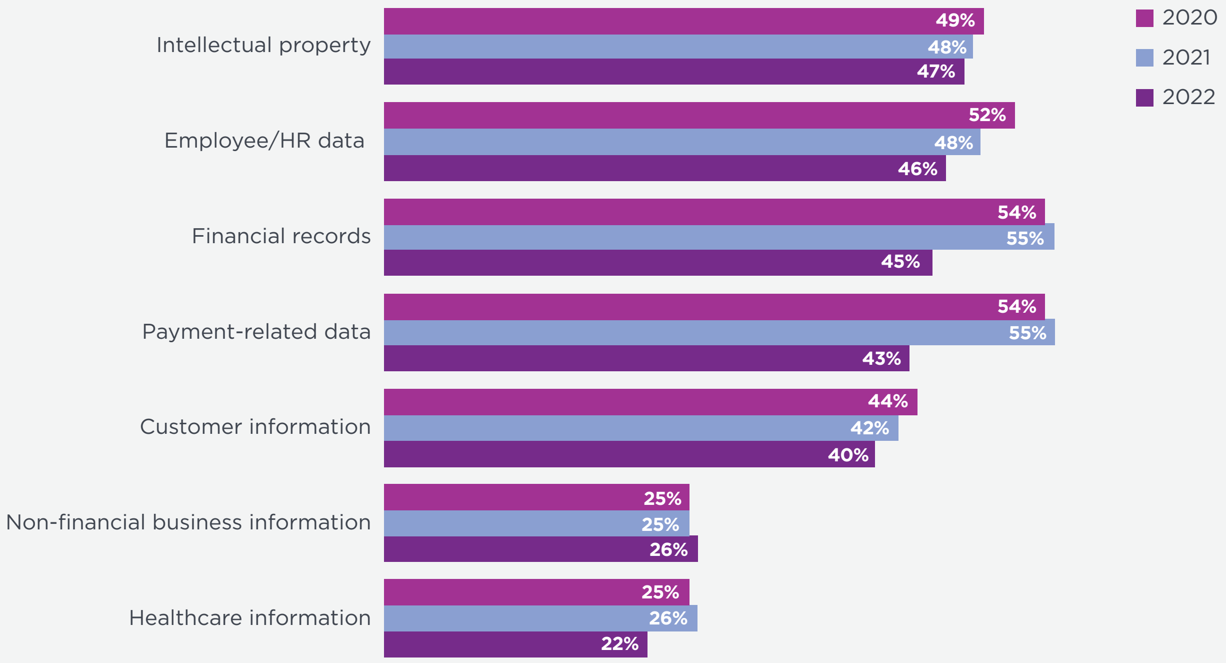
Figure 11. **Most important features of encryption technology solutions**
Country samples are consolidated. Very important and Important responses combined.



Intellectual property and employee/HR data are most often routinely encrypted. Figure 12 provides a list of seven data types that are routinely encrypted by respondents' organizations. Intellectual property is the number one data type to be routinely encrypted (47% of respondents), followed by employee/HR data (46% of respondents).

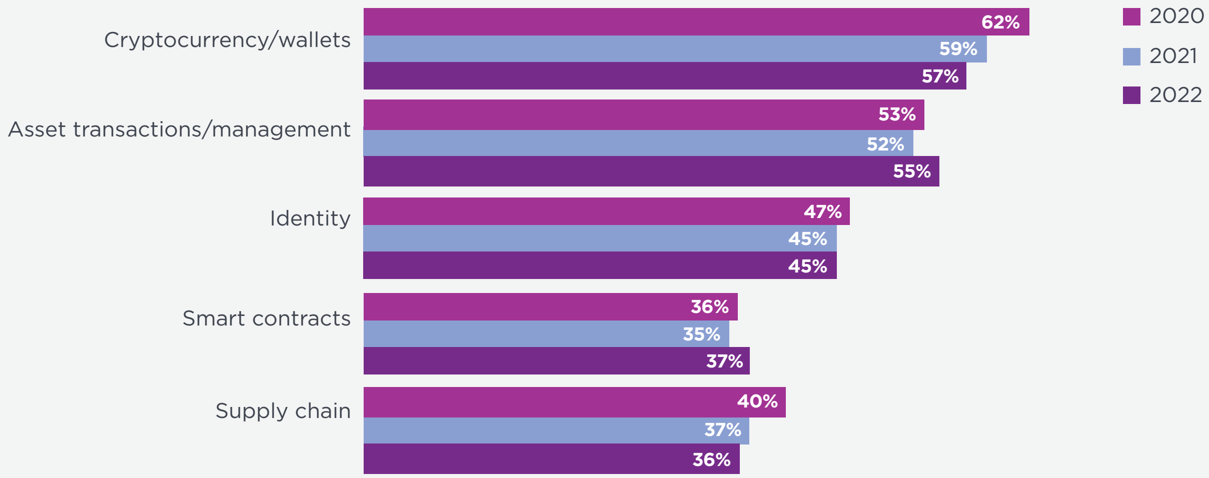
The least likely data types to be encrypted are healthcare information and non-financial business information, which is a surprising result given the number of attacks against health information and high-profile healthcare data breaches.

Figure 12. **Data types routinely encrypted**
Country samples are consolidated. More than one choice permitted.



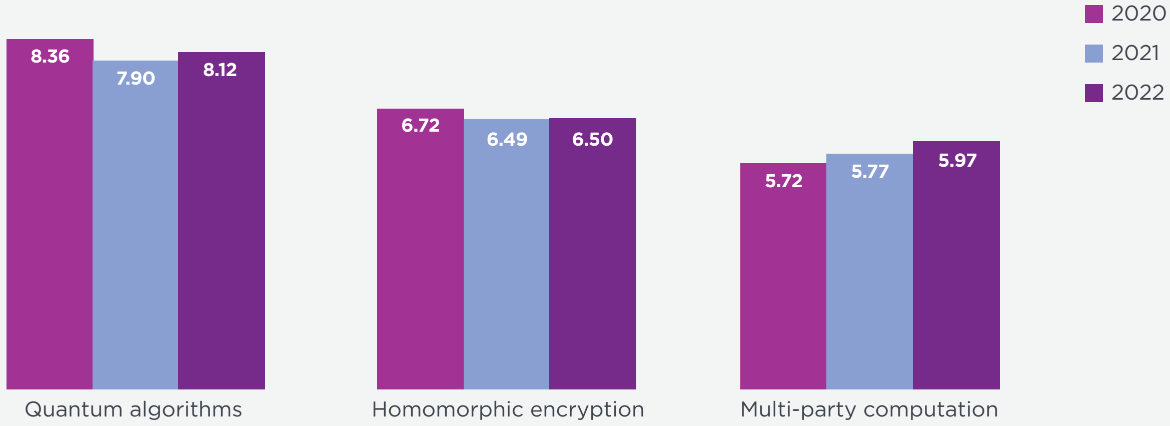
Many companies plan to use blockchain. Fifty-three percent of respondents say their organizations will use blockchain. As shown in Figure 13, the two primary use cases are for cryptocurrency/wallets and asset transactions/management.

Figure 13. **What applications does your organization plan to use blockchain for?**
More than one response permitted.



Respondents were asked when they think the solutions in Figure 14 will achieve mainstream enterprise adoption. The solution expected to achieve adoption the soonest is multi-party computation. Quantum algorithms will not achieve adoption for more than eight years.

Figure 14. **When do you think the following solutions will achieve mainstream enterprise adoption?**
Extrapolated values in years.



ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management? Using a 10-point scale, respondents were asked to rate the overall "pain" associated with managing keys within their organization, where 1 = minimal impact to 10 = severe impact. Figure 15 clearly shows that 59% of respondents chose ratings at or above 7; thus, suggesting a fairly high pain threshold.

The top **3 reasons** that make key management painful.

1. No clear ownership
2. Lack of skilled personnel
3. Key management tools are inadequate

Figure 15. **Rating on the overall impact, risk, and cost associated with managing keys**
Country samples are consolidated. On a scale from 1 = minimal impact to 10 = severe impact, 7+ responses presented.

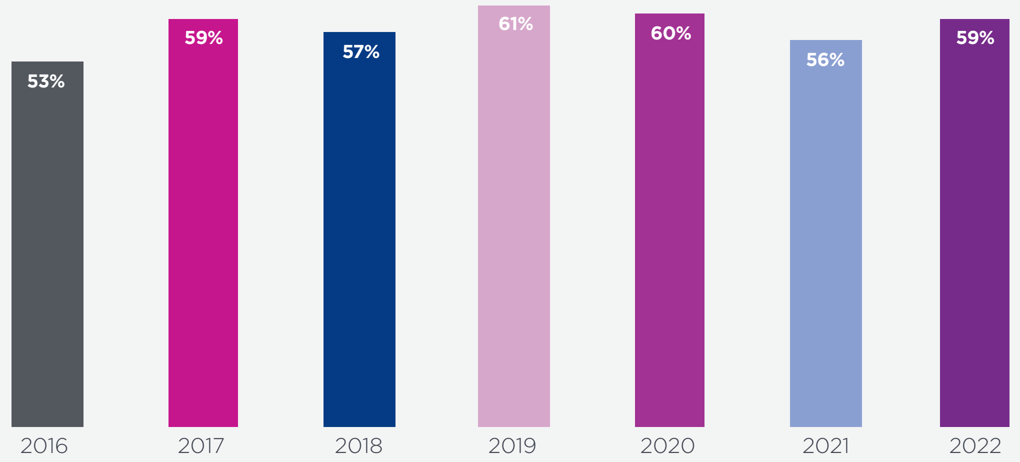
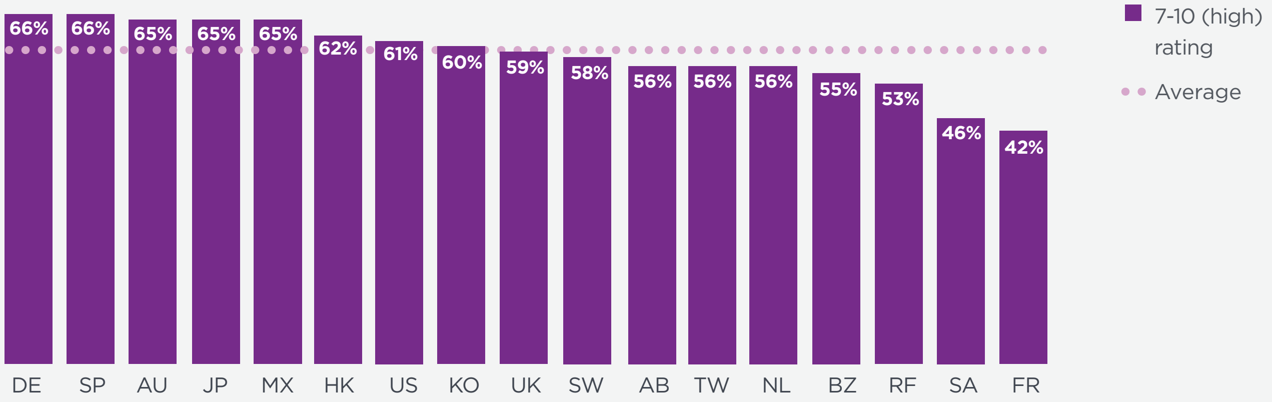


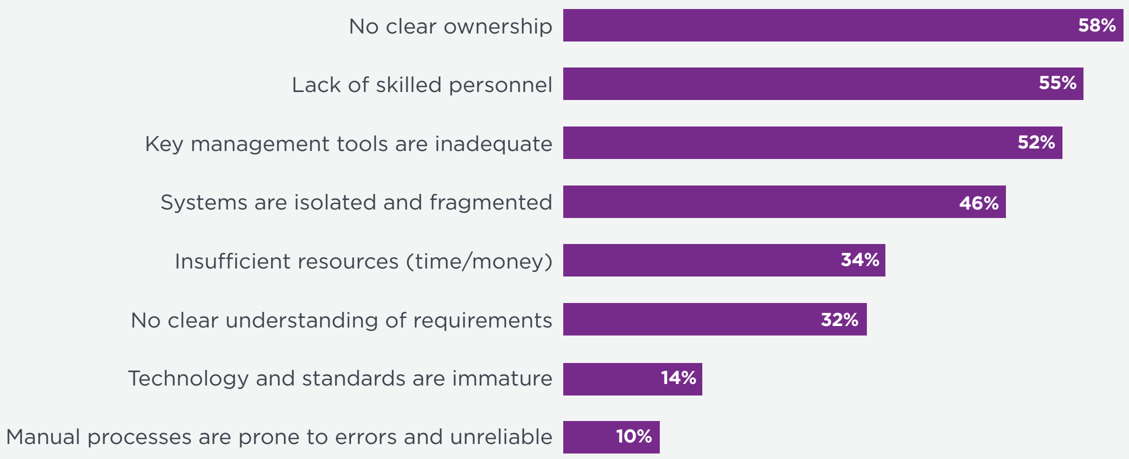
Figure 16 shows the 7+ ratings on a 10-point scale for each country/region. As can be seen, the average percentage in all country/region samples is 59%, which suggests respondents view managing keys as a very challenging activity.

Figure 16. **Percentage "pain threshold" by country/region of key management**
Percentage 7 to 10 rating on a 10-point scale.



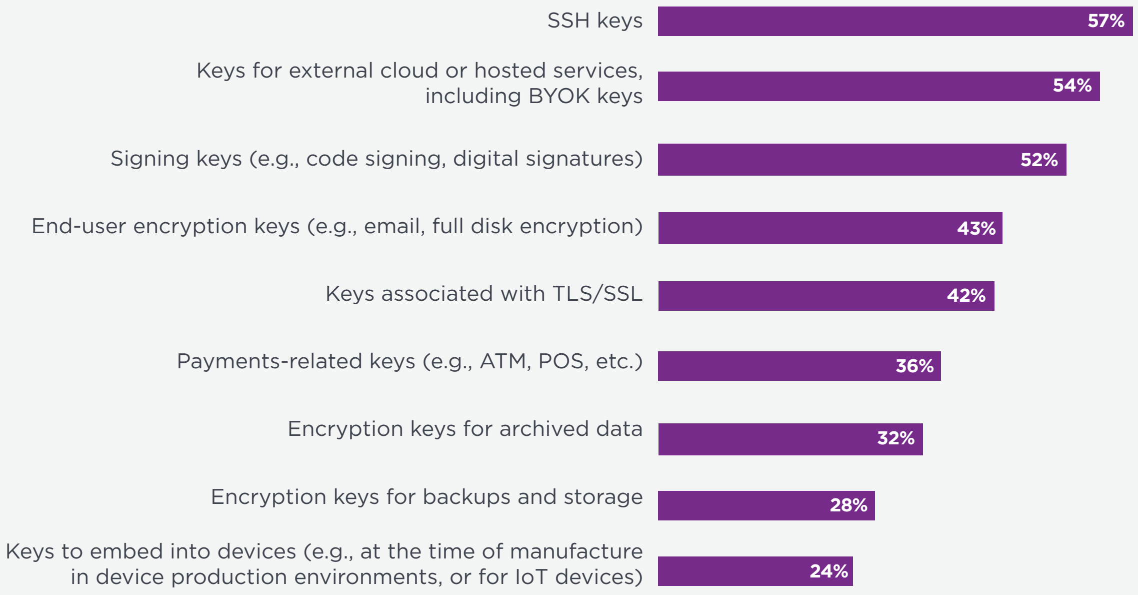
Why is key management painful? Figure 17 shows the reasons why the management of keys is so difficult. The top three reasons are: (1) no clear ownership of the key management function; (2) lack of skilled personnel; and (3) key management tools are inadequate.

Figure 17. **What makes the management of keys so painful?**
Country samples are consolidated. Three responses permitted.



Which keys are most difficult to manage? For the first time in five years, the most difficult keys to manage are SSH keys, followed by keys for external cloud or hosted services, including BYOK. As shown in Figure 18, this is followed by signing keys and end-user encryption keys.

Figure 18. **Types of keys most difficult to manage**
Country samples are consolidated. Very painful and painful responses combined.

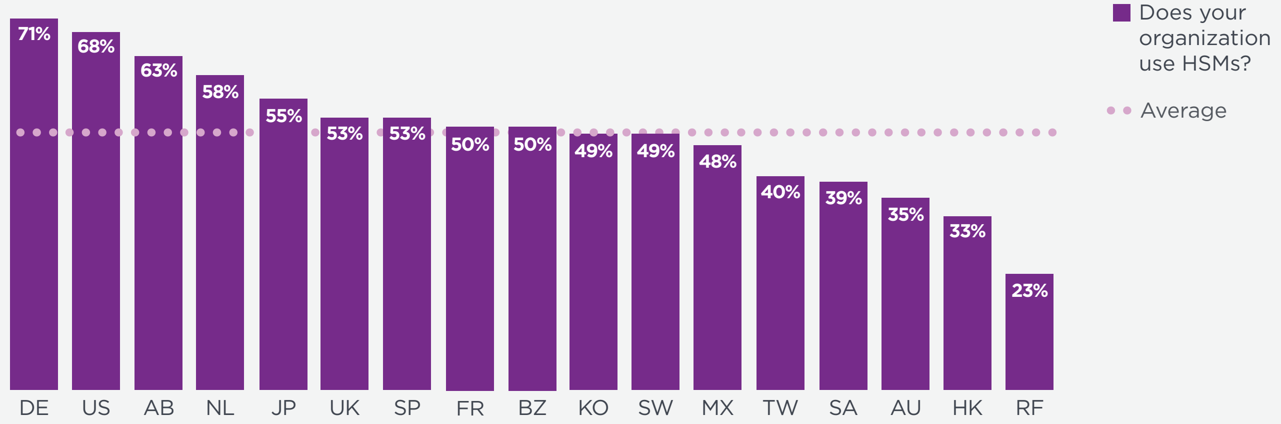


IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

Germany, Middle East, and United States organizations are more likely to deploy HSMs. Figure 19 summarizes the percentage of respondents that deploy HSMs. Germany, Middle East, and the United States are more likely to deploy HSMs than other countries/regions. The overall average deployment rate for HSMs is 49%.

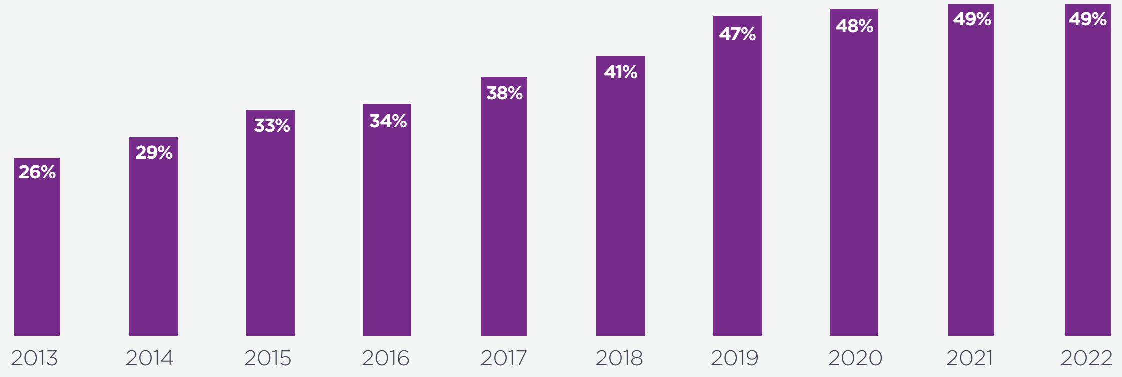
Nearly half of all organizations use HSMs, up from **38%** five years ago.

Figure 19. **Deployment of HSMs**
Yes responses presented.



Deployment of HSMs increases steadily. Figure 20 shows a 10-year trend for HSMs. As can be seen, the rate of global HSM deployment has steadily increased.

Figure 20. **HSM deployment rate over 10 years**
Country samples are consolidated.



How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. As shown in Figure 21, 44% of respondents own and operate HSMs on-premises for cloud-based applications, and 38% of respondents rent/use HSMs from a public cloud provider hosted in the cloud. In the next 12 months, respondents predict a significant increase in the ownership and operation of HSMs for the purpose of generating and managing BYOK keys to send to the cloud for use by the cloud provider. Also predicted to increase is the ownership and operation of HSMs that integrate with a cloud access security broker to manage keys and cryptographic operations.

Figure 21. **Use of HSMs in conjunction with public cloud-based applications today and in the next 12 months**
More than one choice permitted.

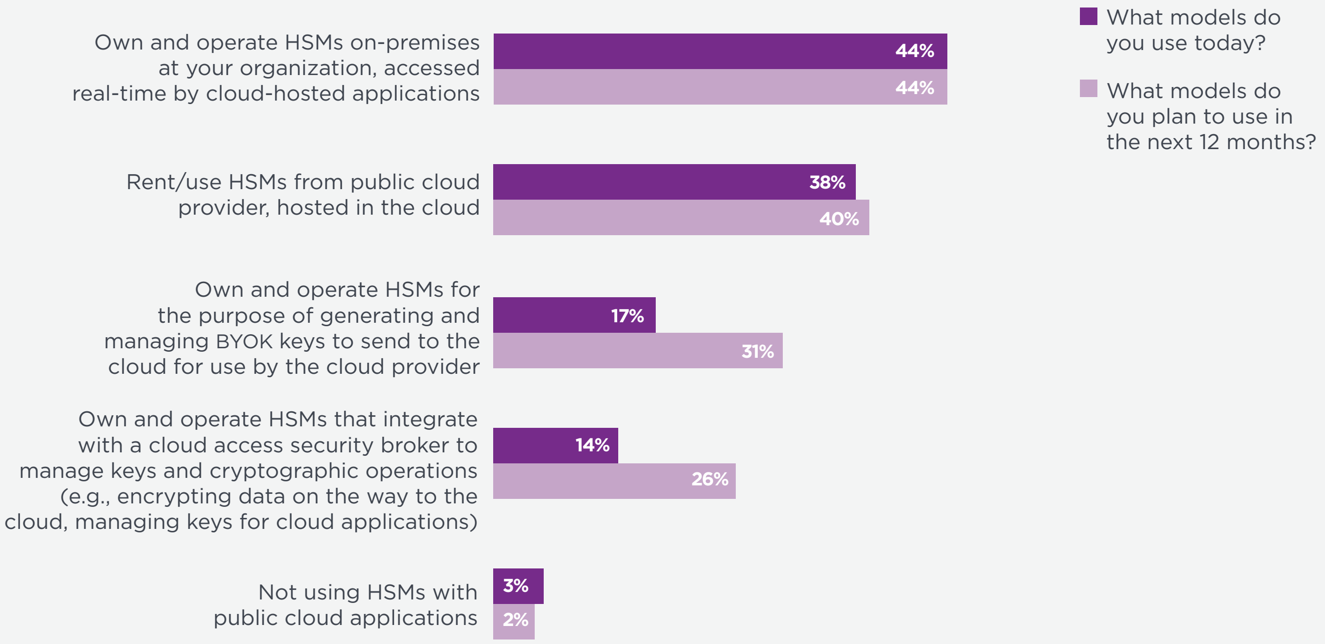


Figure 22 summarizes the percentage of respondents in 17 countries/regions that rate HSMs as either very important or important to their organization's encryption or key management program or activities. An average of 63% of respondents globally rate HSMs as very important. The pattern shown indicates that respondents in Germany, the United States, and Hong Kong are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

Figure 22. **Perceived importance of HSMs as part of encryption or key management**
Very important and Important responses combined.

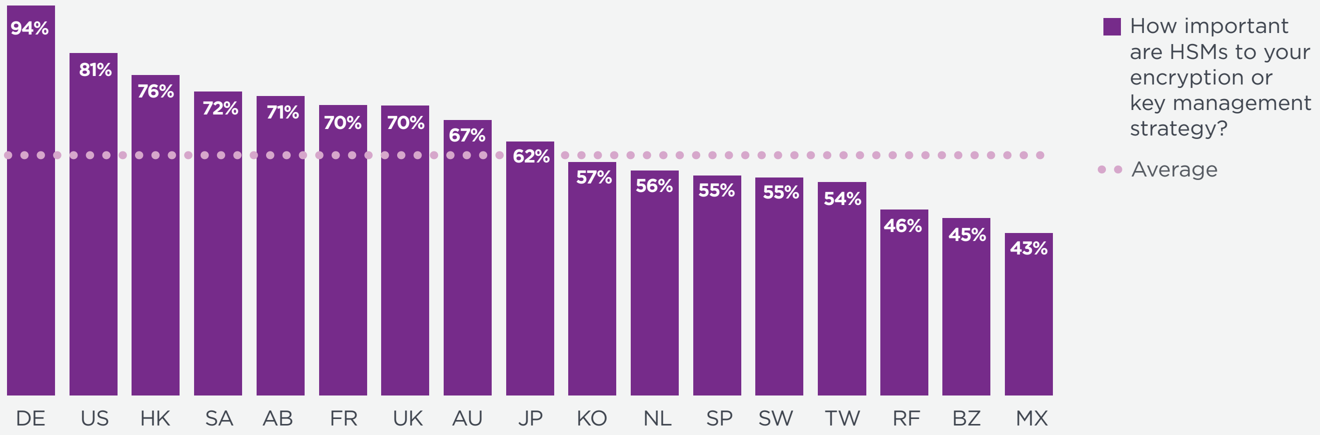
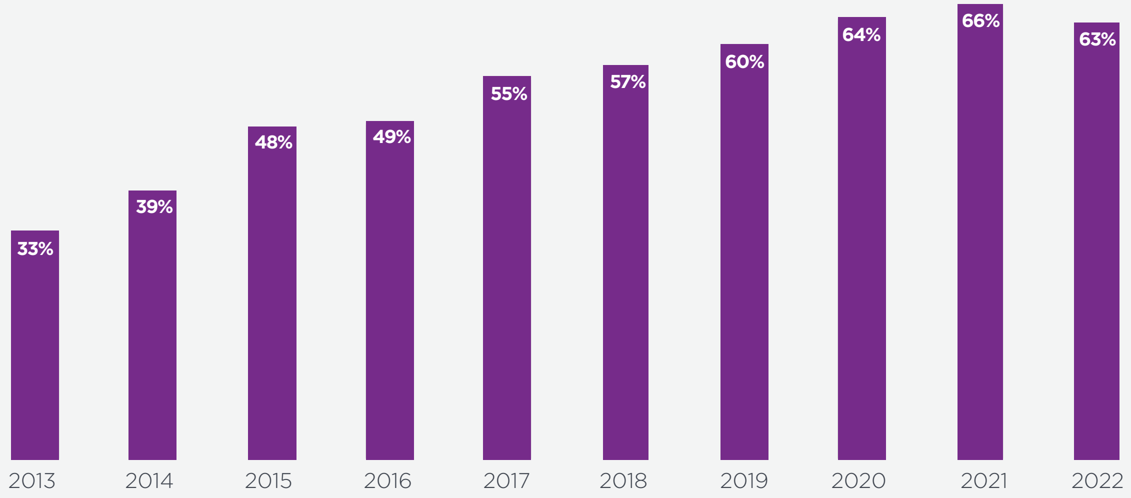


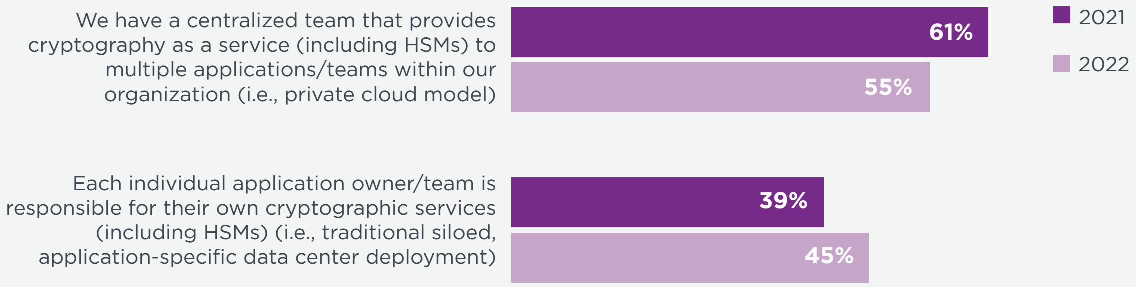
Figure 23 shows a 10-year trend in the importance of HSMs for encryption or key management, which has increased over time from 33% of respondents to 63% of respondents in this year's study.

Figure 23. **Perceived importance of HSMs as part of encryption or key management over 10 years**
Country samples are consolidated.



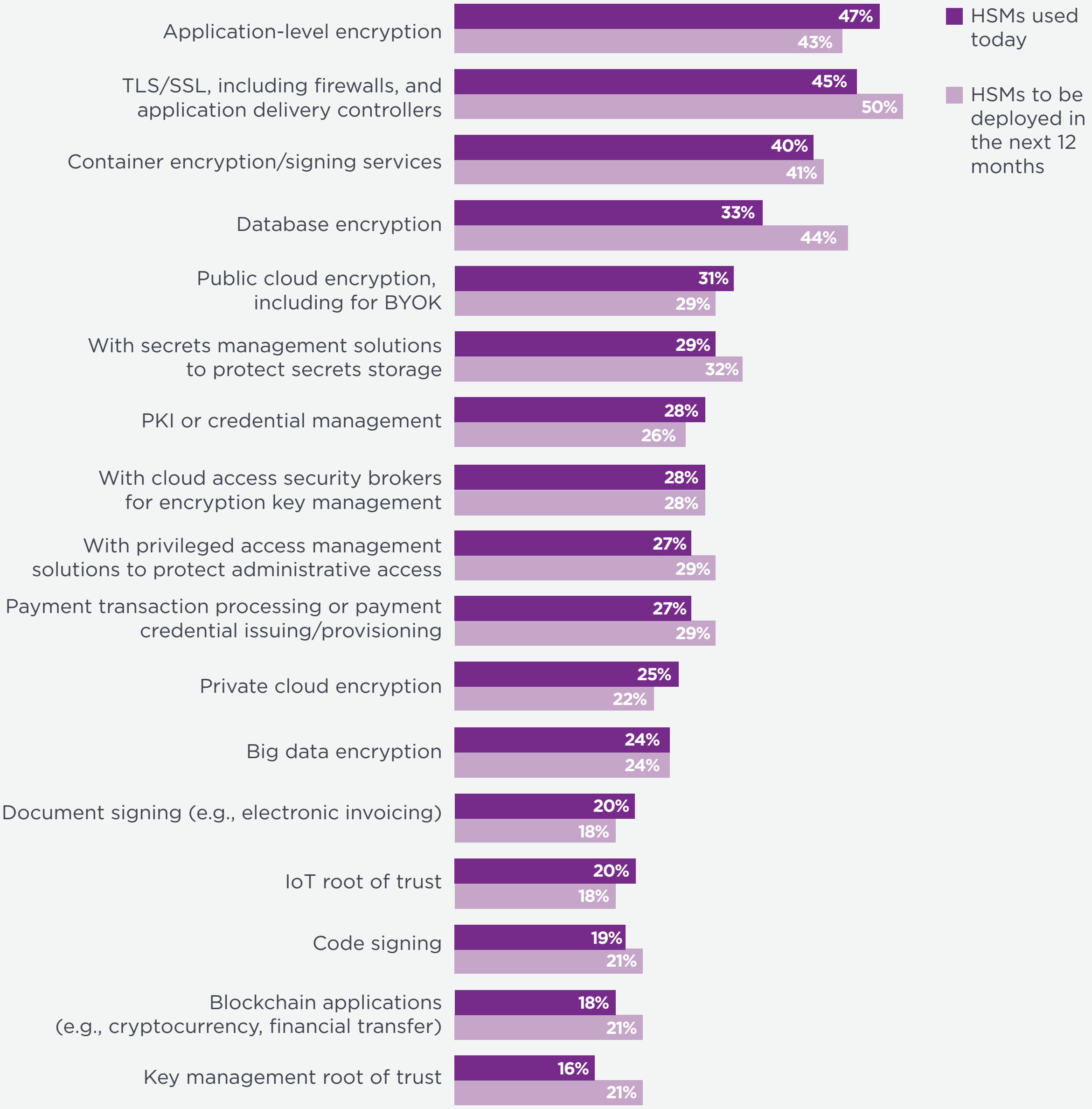
What best describes an organization's use of HSMs? As shown in Figure 24, 55% of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model). Forty-five percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional siloed application-specific data center deployment approach.

Figure 24. **Which statement best describes how your organization uses HSMs?**



What are the primary purposes or uses for HSMs? Figure 25 summarizes the primary purpose or use cases for deploying HSMs. As shown, the top three choices are application-level encryption, TLS/SSL, followed by container encryption/signing services. In the next 12 months, the use of HSMs for database encryption will increase significantly.

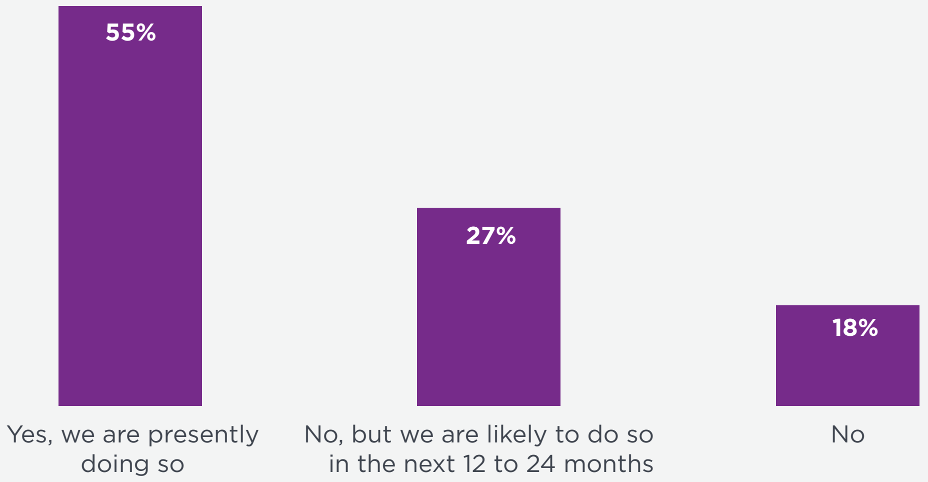
Figure 25. **How HSMs are deployed or planned to be deployed in the next 12 months**
Country samples are consolidated. More than one choice permitted.



CLOUD ENCRYPTION

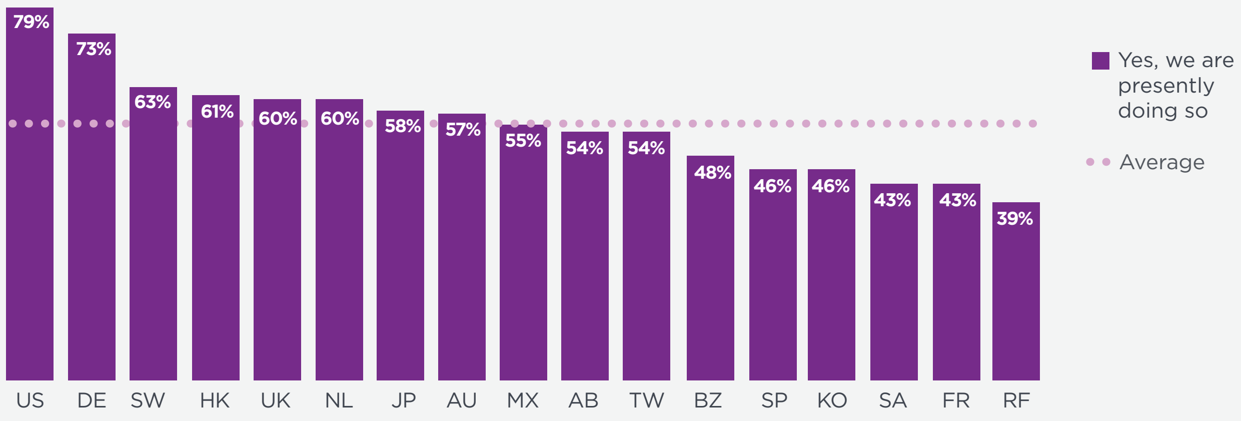
According to Figure 26, 55% of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking. Another 27% of respondents expect to do so in the next one to two years. These findings indicate that the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

Figure 26. **Do you currently transfer sensitive or confidential data to the cloud?**
Country samples are consolidated.



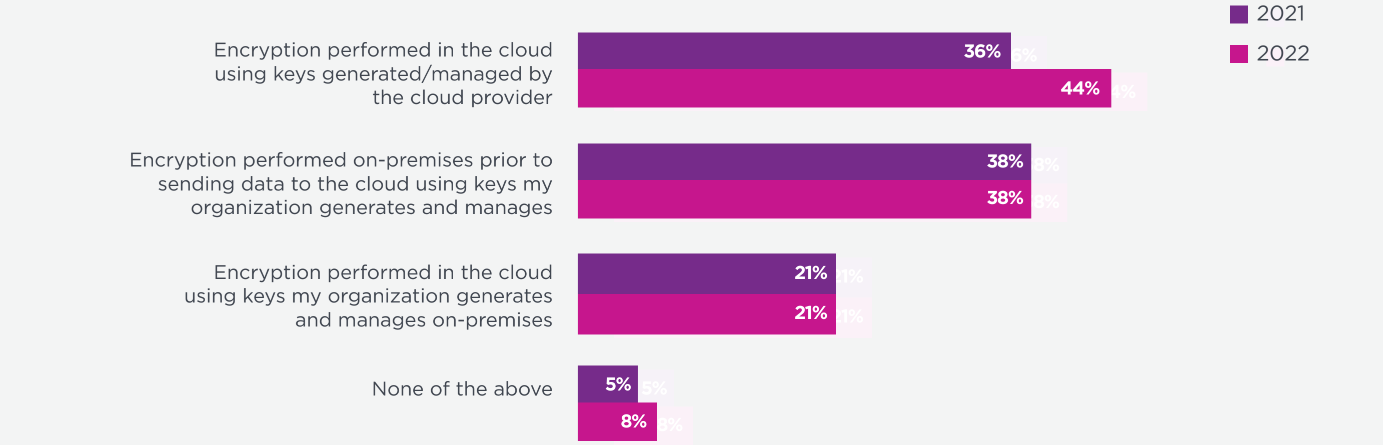
According to Figure 27, with respect to the transfer of sensitive or confidential data to the cloud, organizations in the United States, Germany, and Sweden are more frequently transferring sensitive data to the cloud.

Figure 27. **Organizations that transfer sensitive or confidential data to the cloud by country/region**



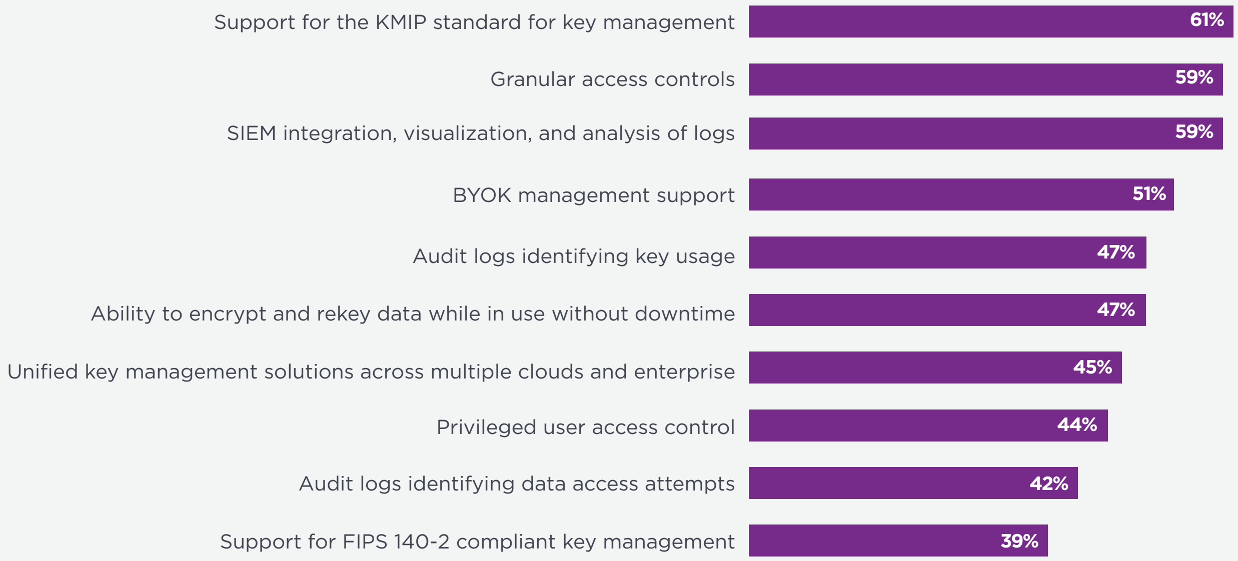
How do organizations protect data at rest in the cloud? As shown in Figure 28, 38% of respondents say encryption is performed on-premises prior to sending data to the cloud using keys their organization generates and manages. However, 44% of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty-one percent of respondents are using some form of BYOK approach.

Figure 28. **How does your organization protect data at rest in the cloud?**
Country samples are consolidated. More than one choice permitted.



What are the top three encryption features specifically for the cloud? The top three features are support for the KMIP standard for key management (61% of respondents), SIEM integration, visualization, and analysis of logs (59% of respondents), and granular access controls (59% of respondents), as shown in Figure 29.

Figure 29. **How important are the following features associated with cloud encryption to your organization?**
Very important and Important responses combined.



APPENDIX Methods & Limitations

Table 1 reports the sample response for 17 separate country/region samples. Data collection was started in December 2021 and completed in January 2022. Our consolidated sampling frame of practitioners in all countries consisted of 162,436 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 7,056 returns of which 792 were rejected for reliability issues. Our final consolidated 2022 sample was 6,264, thus resulting in an overall 3.9% response rate.

The first encryption trends study was conducted in the United States in 2005. Since then, we have expanded the scope of the research to include 17 separate country/region samples. Trend analysis was performed on combined country/region samples.

Table 1. Survey response in 17 countries/regions

Country/ region	Survey response	Sampling frame	Final sample	Response rate
AU	Australia	6,709	279	4.2%
BZ	Brazil	12,124	486	4.0%
FR	France	10,001	333	3.3%
DE	Germany	11,859	478	4.0%
HK	Hong Kong	6,087	253	4.2%
JP	Japan	12,257	514	4.2%
KO	Korea	8,794	365	4.2%
MX	Mexico	10,135	308	3.0%
AB	Middle East	9,191	313	3.0%
NL	Netherlands	9,152	253	3.8%
RF	Russian Federation	7,108	216	3.0%
SA	Southeast Asia	7,043	206	2.9%
SP	Spain	9,770	420	4.3%
SW	Sweden	7,628	231	3.0%
TW	Taiwan	7,299	315	4.3%
UK	United Kingdom	9,366	368	3.9%
US	United States	17,913	833	4.7%
	Consolidated	**162,436**	**6,264**	**3.9%**

Table 2 summarizes our survey samples for 17 countries/regions over a 14-year period.

Table 2. Sample history over 14 years

Country/ region	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009
AB	313	373	342	340	308	316	368							
AU	279	317	325	327	315	331	334	359	414	938	471	477	482	405
BZ	486	553	471	517	507	463	460	472	530	637	525			
FR	333	451	354	332	370	345	344	375	478	584	511	419	414	
DE	478	467	473	531	543	531	563	564	602	499	526	465	490	453
HK	253	267	267	317										
JP	514	487	504	502	468	450	487	476	521	466	544			
KO	365	406	321	325	317									
MX	308	369	353	499	468	451	429	445						
NL	253	322	302											
RF	216	211	216	226	196	206	201	193	201					
SA	206	276	276	268										
SP	420	459												
SW	231	275	277											
TW	315	292	302											
UK	368	408	389	402	468	460	487	509	637	550	651	622	615	638
US	833	677	689	683	710	701	758	789	892	531	912	964	997	975
Total	**6,264**	**6,610**	**6,457**	**5,856**	**5,252**	**4,802**	**5,009**	**4,714**	**4,275**	**4,205**	**4,140**	**2,947**	**2,998**	**2,471**

Figure 30 reports the respondent's organizational level within participating organizations. By design, 57% of respondents are at or above the supervisory levels and 40% of respondents reported their position as associate/staff/technician. Respondents have on average 9.2 years of security experience with approximately 7.0 years of experience in their current position.

Figure 31 identifies the organizational location of respondents in our study. Half (50%) of respondents are located within IT operations. This is followed by security at 21% of respondents, compliance (12% of respondents), and lines of business (8% of respondents).

Figure 30. **Distribution of respondents according to position level**
Country samples are consolidated.

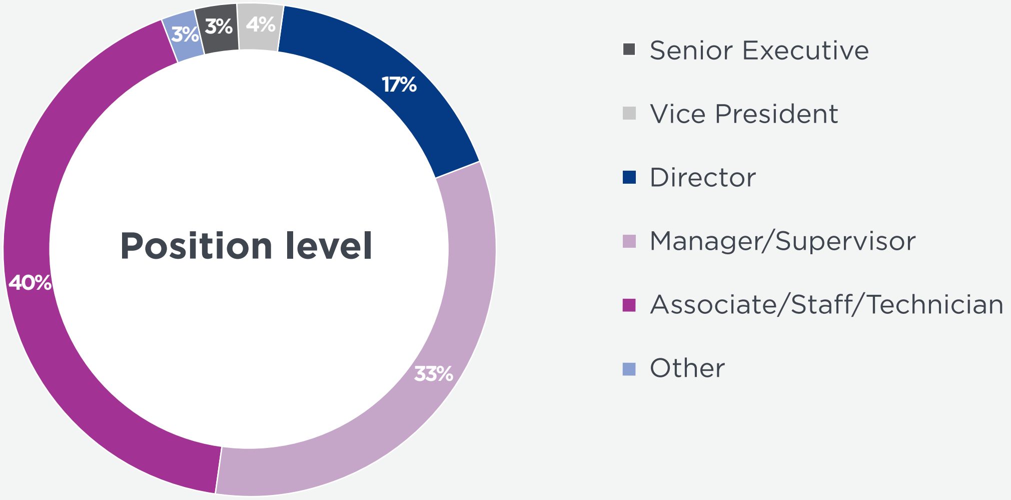


Figure 31. **Distribution of respondents according to organizational location**
Country samples are consolidated.

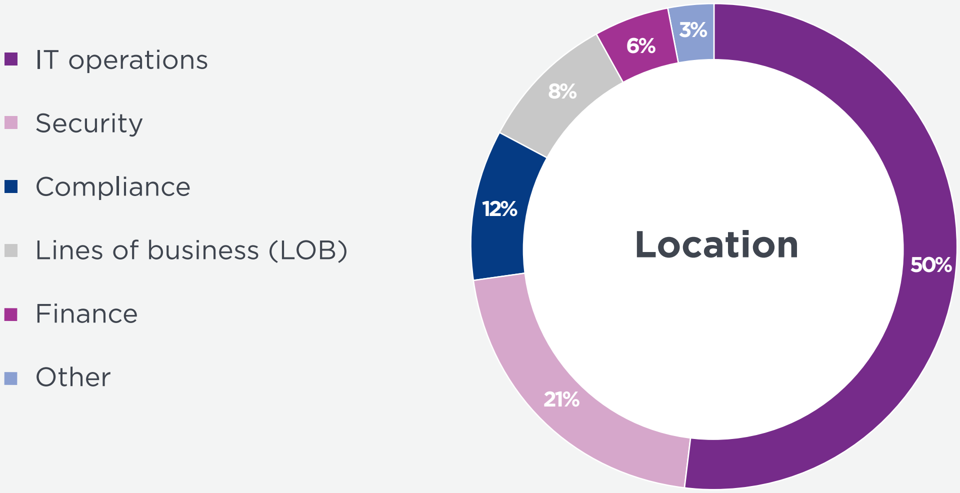


Figure 32 reports the industry classification of respondents' organizations. Thirteen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments, and credit cards. Twelve percent of respondents are located in manufacturing and industrial organizations, 10% of respondents are in technology and software. This is followed by services, public sector, and health and pharmaceuticals (each at 8% of respondents).

According to Figure 33 more than half (53%) of respondents are located in organizations with a global headcount of more than 1,000 employees.

Figure 32. **Distribution of respondents according to primary industry classification**
Country samples are consolidated.

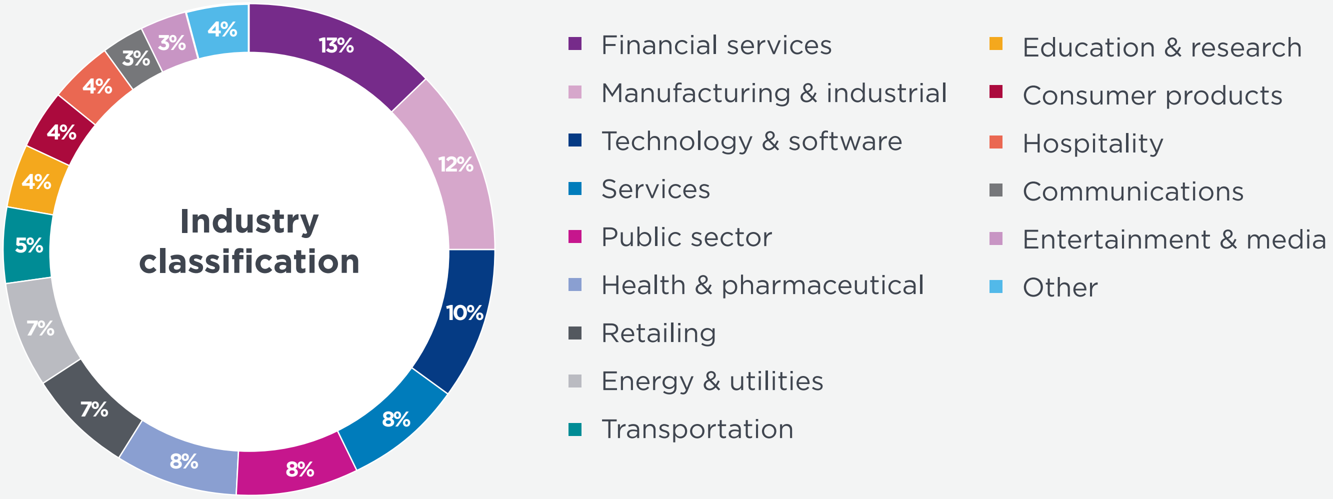
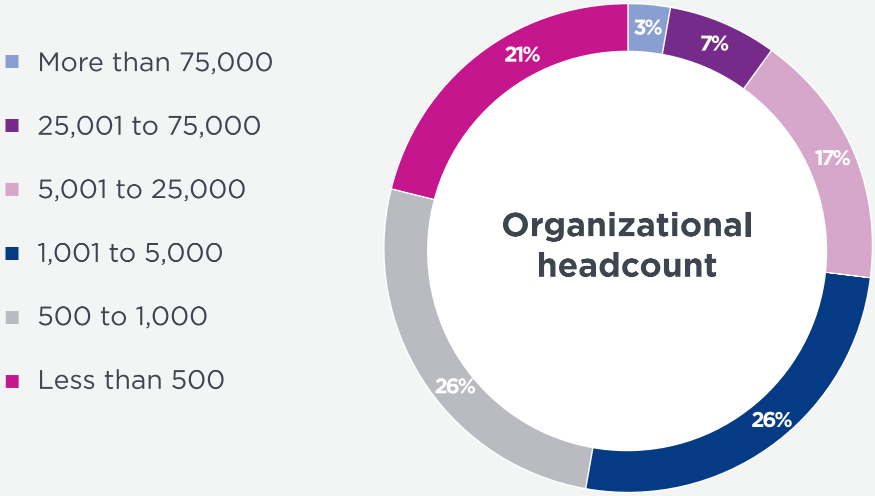


Figure 33. **Distribution of respondents according to organizational headcount**
Country samples are consolidated.



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 17 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 17 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.

View the full 2022 Global Encryption Trends Study consolidated findings at:

Entrust.com/go/2022-GETS-findings

Ponemon INSTITUTE

ABOUT 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.

ENTRUST
SECURING A WORLD IN MOTION

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. For more information, visit **entrust.com**

Entrust offers an unrivaled portfolio of data protection solutions that use trusted identities, applied cryptography, PKI, and other advanced security technologies to minimize threats and enable digital transformation. By delivering a foundation of trust, organizations are empowered to adopt new technologies and opportunities with the highest level of assurance available.

ENTRUST

SECURING A WORLD IN MOTION

Learn more at entrust.com