Ponemon INSTITUTE

ENTRUST

You are here. Your data is there.
Threats are everywhere.

2021 GLOBAL ENCRYPTION TRENDS STUDY

Find out how organizations are protecting data across multiple clouds, and how your encryption strategy compares.

01 Executive Summary

PONEMON INSTITUTE PRESENTS THE FINDINGS OF THE 2021 GLOBAL ENCRYPTION TRENDS STUDY[1]

We surveyed 6,610 individuals across multiple industry sectors in 17 countries/regions – Australia, Brazil, France, Germany, Hong Kong, Japan, Mexico, Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), Netherlands, the Russian Federation, Spain, Southeast Asia, South Korea, Sweden, Taiwan, the United Kingdom, and the United States.[2]

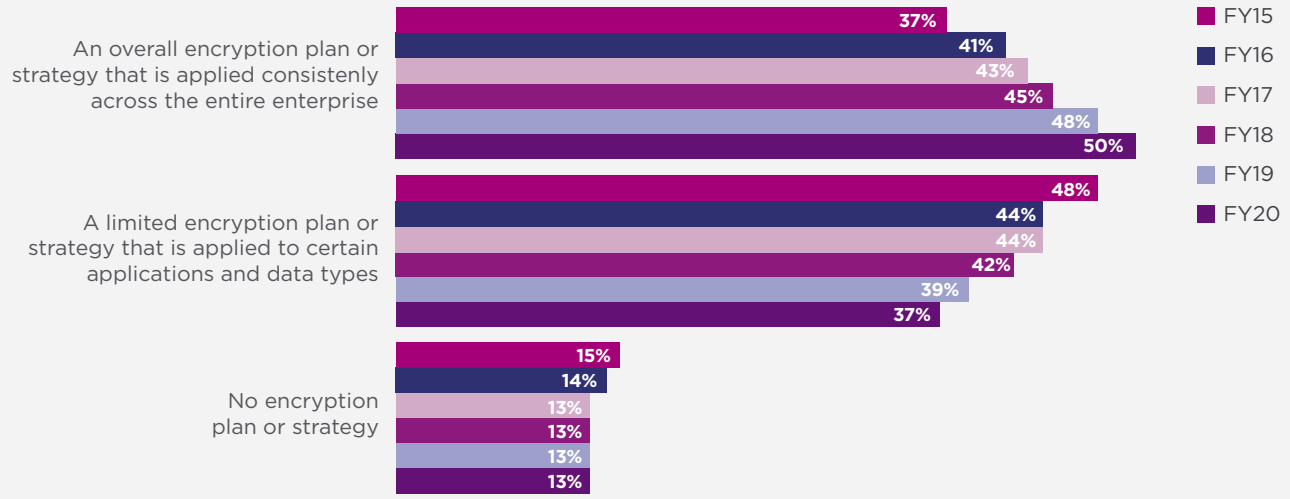
The purpose of this research is to examine how the use of encryption has evolved over the past 16 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a U.S. sample of respondents.[3]

Since then, we have expanded the scope of the research to include respondents in all regions of the world.

As shown in Figure 1, since 2015 the deployment of an overall encryption strategy has steadily increased. This year, 50 percent of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise, and 37 percent say they have a limited encryption plan or strategy that is applied to certain applications and data types, a slight decrease from last year.

Following are the findings from this year's research.

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



[1] This year's data collection was started in December 2020 and completed in January 2021. Throughout the report we present trend data based on the fiscal year the survey commenced rather than the year the report is finalized. Hence, we present the current findings as fiscal year 2020.

[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 16 years (since 2005).

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since conducting this study 16 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.

Certain countries have more mature encryption strategies. The prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany, the United States, Japan, and the Netherlands. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 50 percent.

The IT operations function is the most influential in framing the organization's encryption strategy over the past 14 years. However, in the United States the lines of business are more influential (35 percent of respondents). IT operations are most influential in Sweden, Korea and France.

TRENDS IN ADOPTION OF ENCRYPTION

The use of encryption increases in all industries. Results suggest a steady increase in all industry sectors, with the exception of communications and service organizations.

50% of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise.

The most significant increases in extensive encryption usage occur in manufacturing, hospitality, and consumer products.

The extensive use of encryption technologies increases. Since we began tracking the enterprise-wide use of encryption in 2005, there has been a steady increase in the encryption solutions extensively used by organizations.

THREATS, MAIN DRIVERS AND PRIORITIES

Employee mistakes continue to be the most significant threats to sensitive data. The most significant threats to the exposure of sensitive or confidential data are employee mistakes.

In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) significantly outweigh concerns over actual attacks by temporary or contract workers and malicious insiders.

The main driver for encryption is the protection of customers' personal information. Organizations are using encryption for the purpose of protecting customers' personal information (54 percent of respondents), to protect information against specific, identified threats (50 percent of respondents), and for the protection of enterprise intellectual property (49 percent of respondents).

A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization. Sixty-five percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. Forty-three percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-four percent cite classifying which data to encrypt as difficult.

DEPLOYMENT CHOICES

No single encryption technology dominates in organizations. Organizations have very diverse needs. Internet communications, databases, and internal networks are the most likely to be deployed and correspond to mature use cases. For the fourth year, the study tracked the deployment of encryption of IoT devices and platforms. Sixty-one percent of respondents say encryption of IoT devices and 61 percent of respondents say encryption of IoT platforms have been at least partially deployed.

65% of respondents say discovering where sensitive data resides in the organization is the number one challenge.

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.

Which data types are most often encrypted? Payment-related data and financial records are most likely to be encrypted as a result of high-profile data breaches in financial services. 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.

ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management? Fifty-six percent of respondents rate key management as very painful, which suggests respondents view managing keys as a very challenging activity.

The highest percentage pain threshold of 69 percent occurs in Spain. At 37 percent, the lowest pain level occurs in France. No clear ownership and lack of skilled personnel are the primary reasons why key management is painful.

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

Organizations in the U.S., Germany, and Japan are more likely to deploy HSMs. The United States, Germany, and Japan are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 49 percent.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and and will be in the next 12 months. Forty-one percent of respondents say their organizations own and operate HSMs on-premise, accessed real-time by cloud-hosted applications; and 39 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. The use of HSMs with Cloud Access Security Brokers and the ownership and operation of HSMs on-premise are expected to increase significantly.

The overall average importance rating for HSMs, as part of an encryption and key management strategy in the current year, is 66 percent. The pattern of responses suggests the United States, the Middle East, and the Netherlands are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

60% of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted.

What best describes an organization's use of HSMs? Sixty-one 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). Thirty-nine 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.

What are the primary purposes or uses for HSMs? The three top uses are application-level encryption, TLS/SSL, followed notably by container encryption/signing services. There will be a significant increase in the use of database encryption 12 months from now.

CLOUD ENCRYPTION

Sixty 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 24 percent 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? Thirty-eight percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 36 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty-one percent of respondents are using some form of Bring Your Own Key (BYOK) approach.

What are the top three encryption features specifically for the cloud? The top three features are support for the KMIP standard for key management (59 percent of respondents), SIEM integration, visualization and analysis of logs (59 percent of respondents), and granular access controls (55 percent of respondents).

Since first conducting this study 16 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise.

02 Key Findings

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

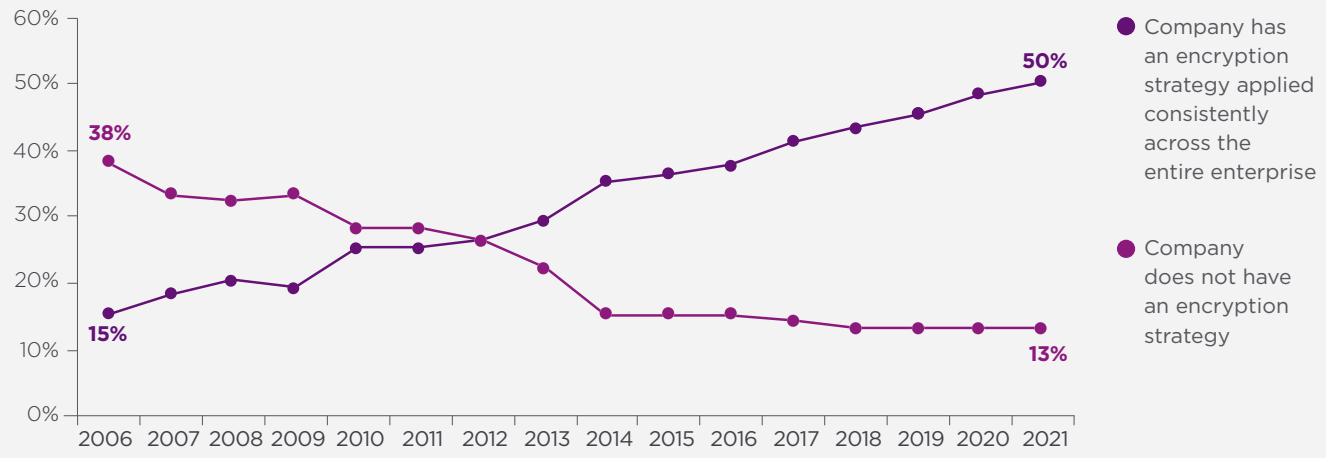
We have organized the report according to the following themes:

- Strategy and adoption of encryption
- Trends in adoption of encryption
- Threats, main drivers and priorities
- Deployment choices
- Encryption features considered most important
- Attitudes about key management
- Importance of hardware security modules (HSMs)[4]
- Cloud encryption

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since first conducting this study 16 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 have more mature encryption strategies. According to Figure 3, the prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany, the United States, Japan and the Netherlands. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 50 percent.

Figure 4 shows that the IT operations function is 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. IT operations and IT security have a similar level of influence in the United Kingdom.

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

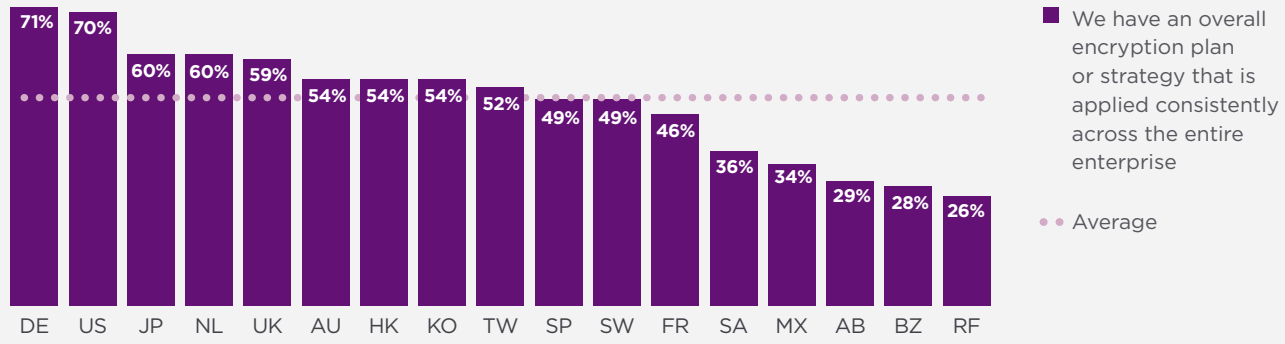
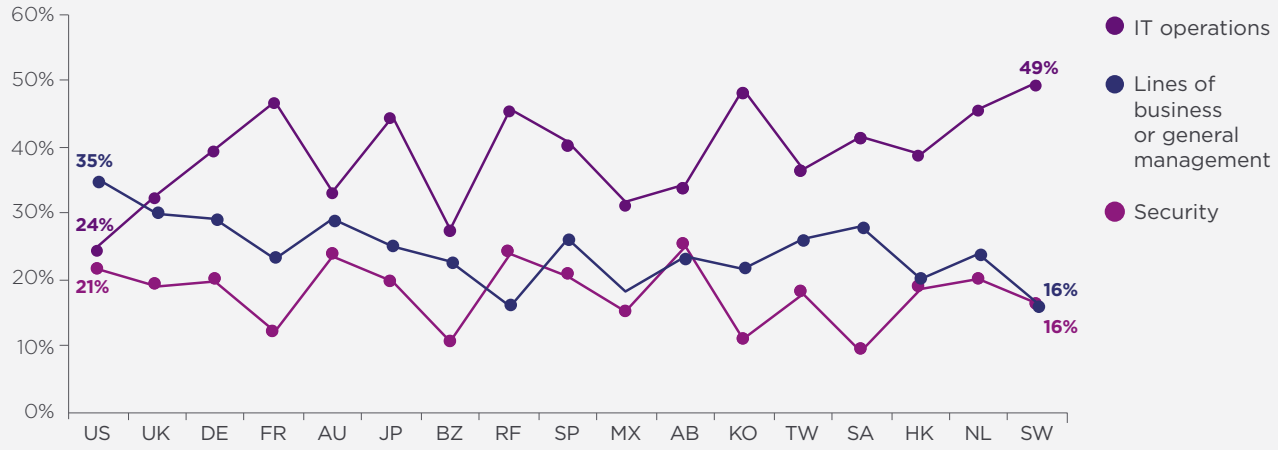


Figure 4. **Influence of IT operations, lines of business and security**
Country samples are consolidated



A possible reason why the lines of business are more influential than IT security in many countries is because of the growing adoption of Internet of Things (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.

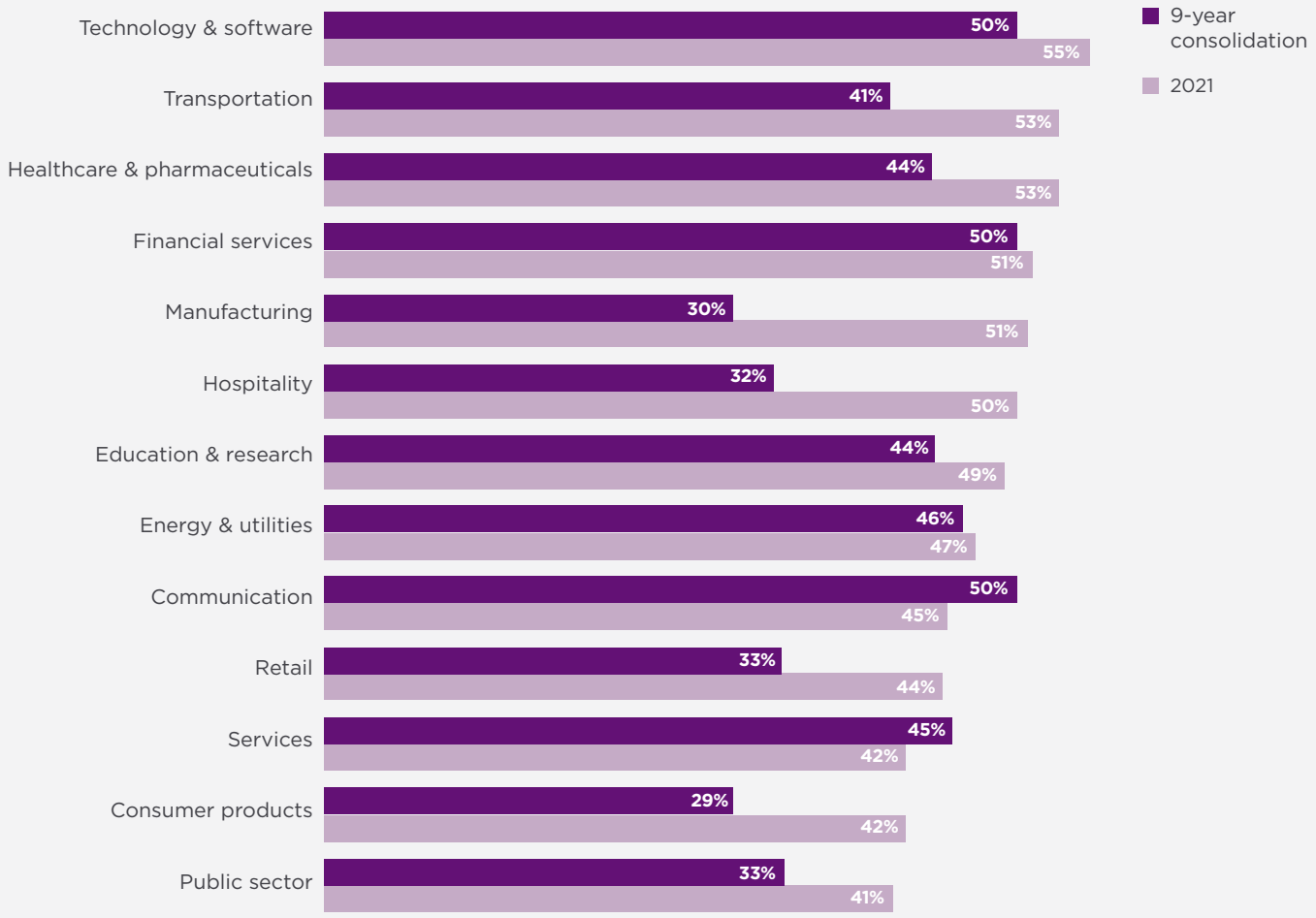
54% of respondents are using encryption to protect customers' personal information.

TRENDS IN ADOPTION OF ENCRYPTION

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 a steady increase in all industry sectors, with the exception of communication and service organizations. The most significant increases in extensive encryption usage occur in manufacturing, hospitality and consumer products.

Figure 5. **The extensive use of encryption by industry: Current year versus 9-year average**
Country samples are consolidated. Average of 15 encryption categories



THREATS, MAIN DRIVERS AND PRIORITIES

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.

In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) significantly outweigh concerns over actual attacks by temporary or contract workers and malicious insiders.

The main driver for encryption is protection of customers' personal information. Eight drivers for deploying encryption are presented in Figure 7 on the following page.

Compliance no longer leads the way

For the 4th year running regulatory compliance is not the top driver for encryption.

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 (54 percent, 50 percent and 49 percent of respondents, respectively).

This marks the fourth year that compliance with regulations has not been the top driver for encryption indicating that encryption is less of a "checkbox" exercise and is now used to safeguard targeted critical information.

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

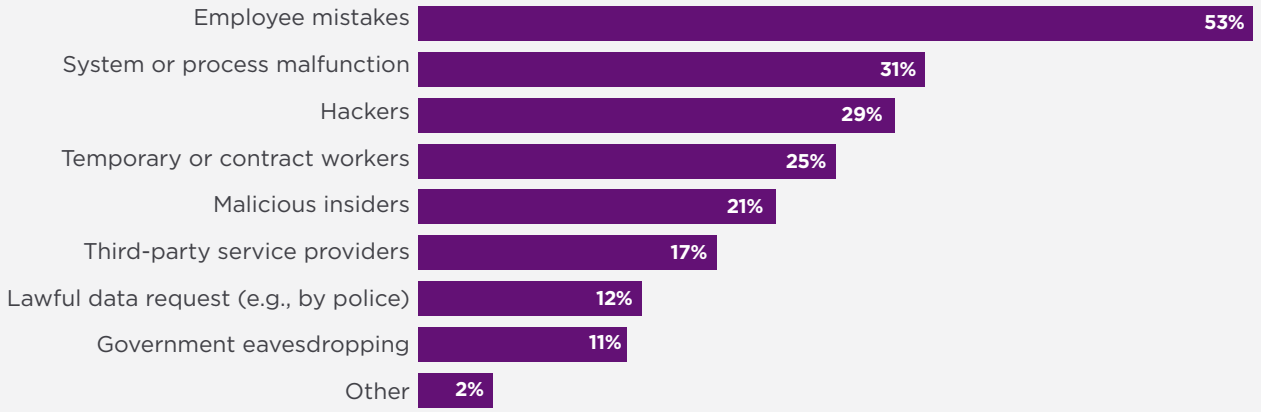
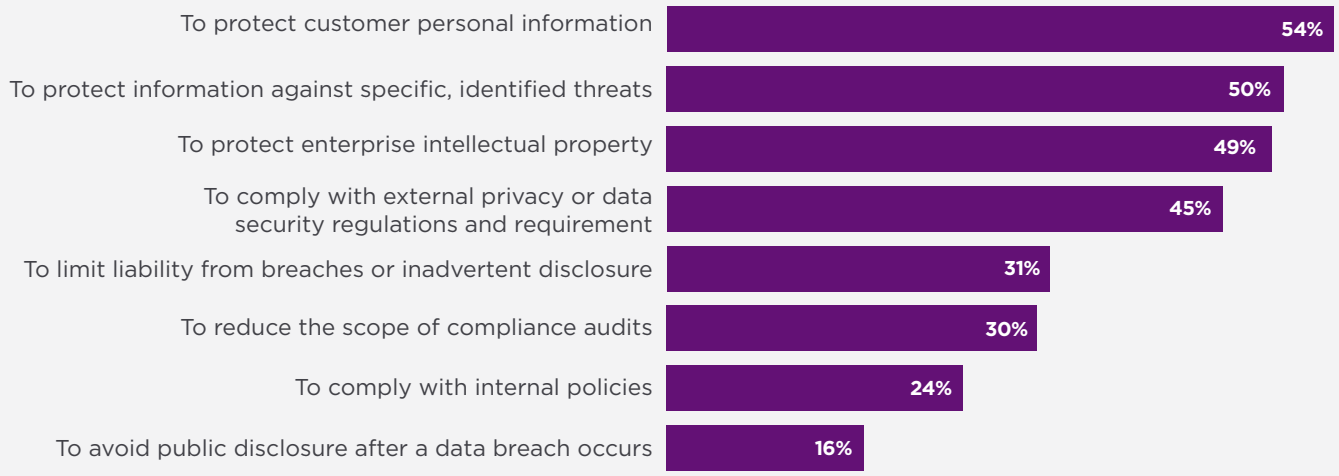
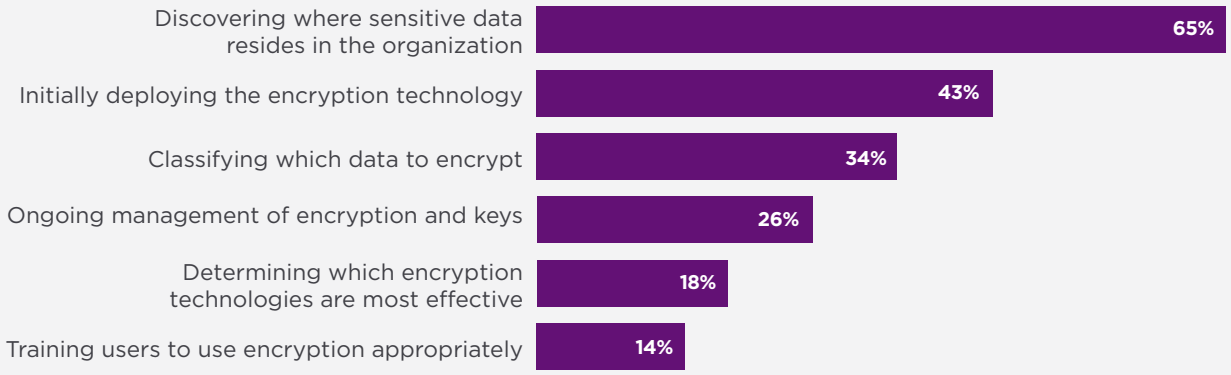


Figure 7. **The main drivers for using encryption technology solutions**
Country samples are consolidated. Three responses permitted



A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization. Figure 8 provides a list of six aspects that present challenges to an organization's effective execution of its data encryption strategy in descending order of importance. Sixty-five percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 43 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-four percent cite classifying which data to encrypt as difficult.

Figure 8. **Biggest challenges in planning and executing a data encryption strategy**
Country samples are consolidated. More than one choice permitted



DEPLOYMENT CHOICES

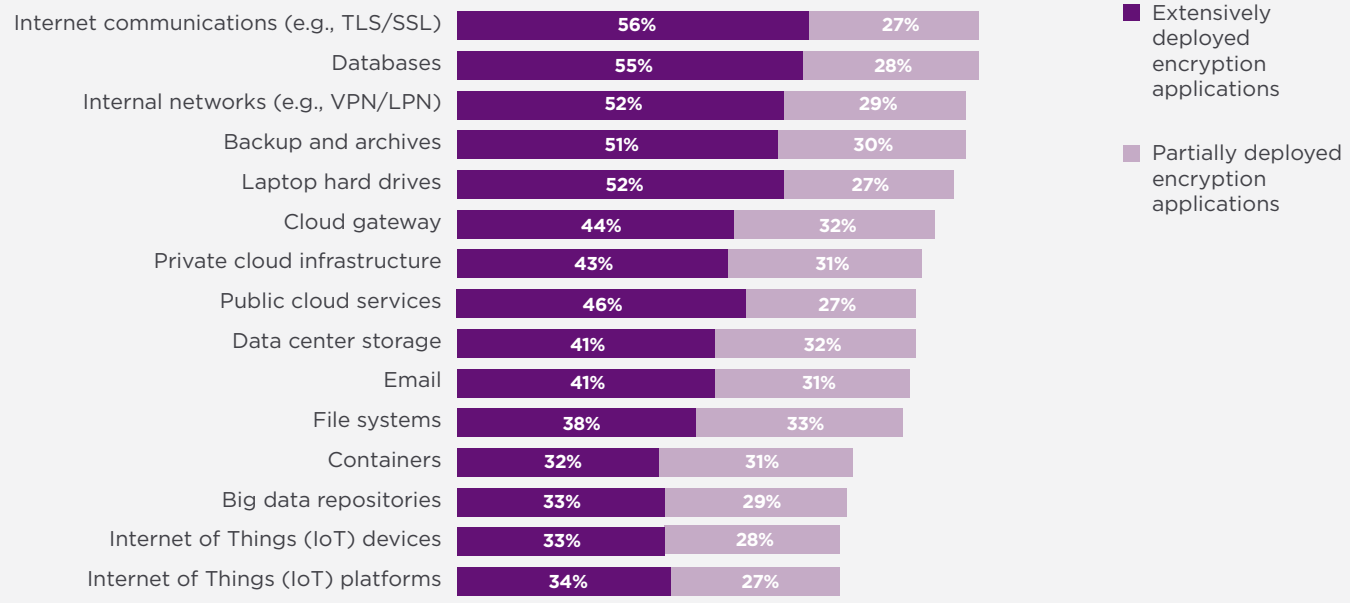
No single encryption technology dominates in organizations. We asked respondents to indicate if specific encryption technologies are widely or only partially deployed within their organizations. "Extensive deployment" means that the encryption technology is deployed enterprise-wide. "Partial deployment"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

As shown in Figure 9, no single technology dominates because organizations have very diverse needs. Internet communications, databases and internal networks are the most likely to be deployed and correspond to mature use cases.

61% of respondents say encryption has been partially deployed for both IoT platforms and devices.

For the fourth year, the study tracked the deployment of encryption of IoT devices and platforms. As shown, 61 percent of respondents say encryption of IoT platforms has been partially deployed and 61 percent of respondents say encryption of IoT devices has been partially deployed.

Figure 9. **Consolidated view on the use of 15 encryption technologies**
Country samples are consolidated

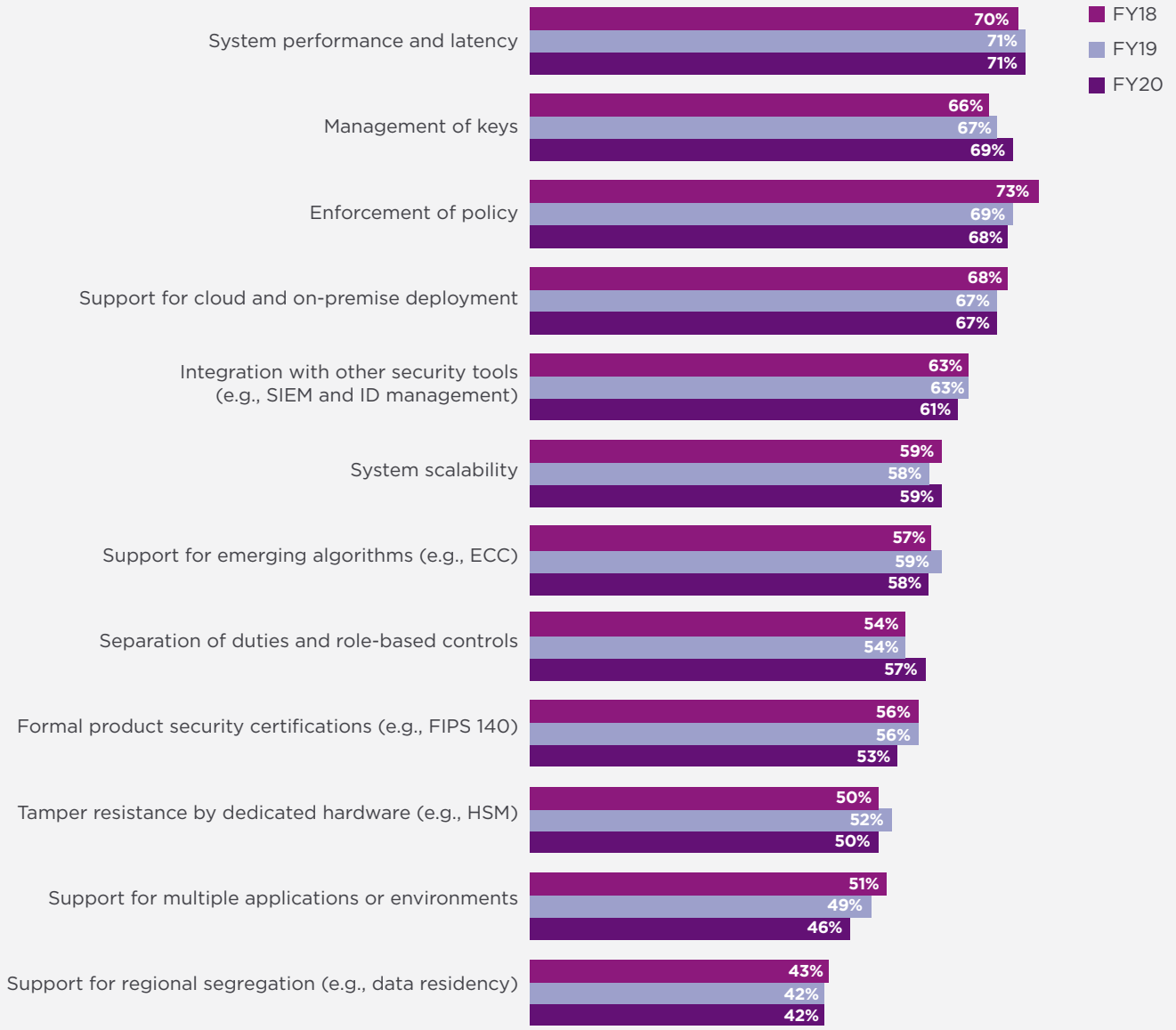


ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others. Figure 10 lists 12 encryption technology features. Each percentage defines the very important response (on a four- point scale). 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, management of keys and enforcement of policy are 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.

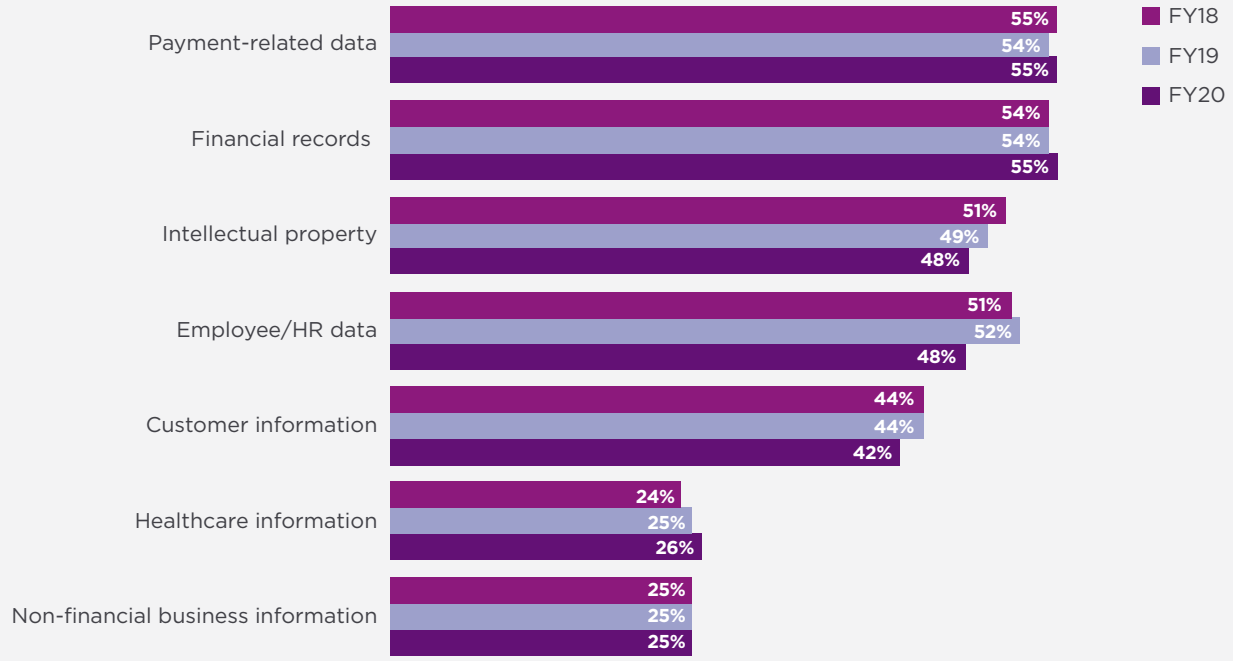
Figure 10. **Most important features of encryption technology solutions**
Country samples are consolidated. Very important and Important responses combined

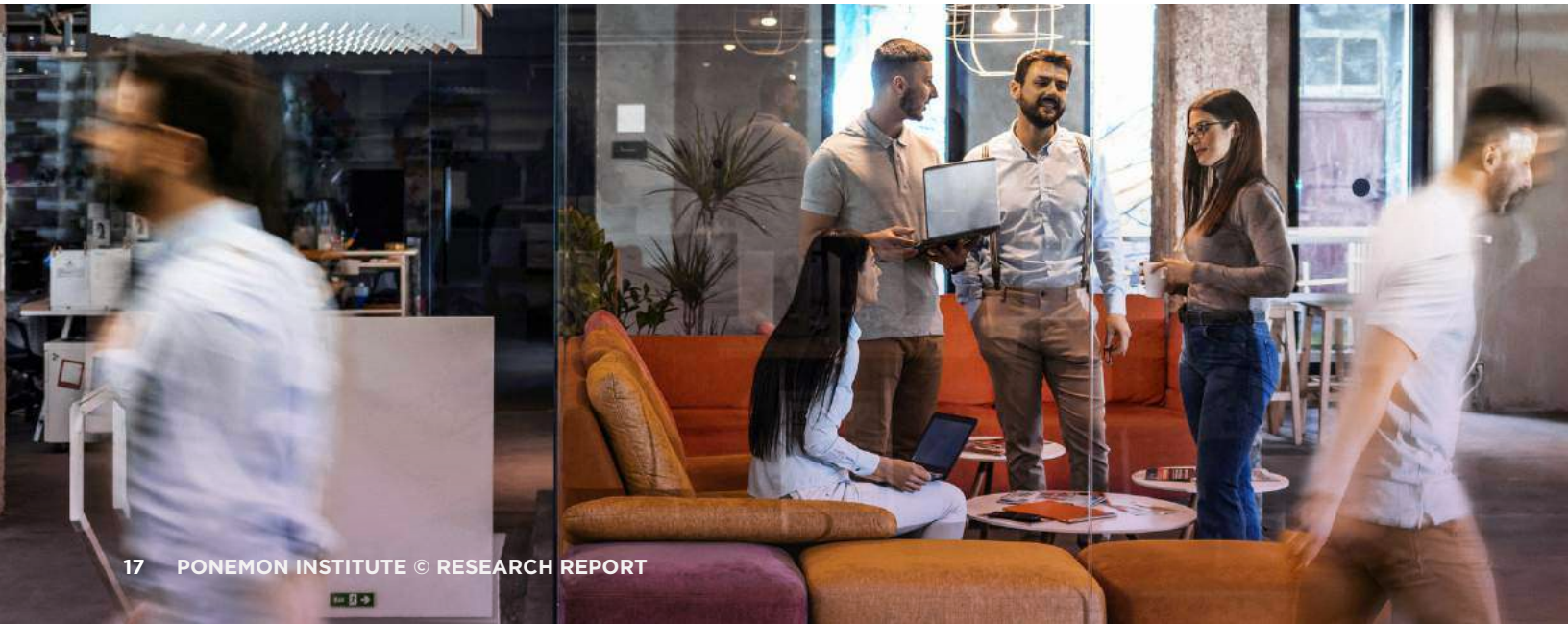


Which data types are most often encrypted? Figure 11 provides a list of seven data types that are routinely encrypted by respondents' organizations. As can be seen, payment-related data and financial records continue to be the most likely to be encrypted as a result of high-profile data breaches in financial services.

The least likely data type to be encrypted is health-related information and non-financial business information, which is a surprising result given the sensitivity of health information and the recent high-profile healthcare data breaches.

Figure 11. **Data types routinely encrypted**
Country samples are consolidated. More than one choice permitted





Most companies plan to use blockchain. Fifty-nine percent of respondents say their organizations will use blockchain. As shown in Figure 12, the two primary use cases are for cryptocurrency/wallets and asset transactions/management.

Respondents were asked when they think the solutions in Figure 13 will achieve mainstream enterprise adoption. The solution expected to achieve adoption the soonest is multi-party computation. Quantum algorithms will achieve adoption in eight years.

Figure 12. **What applications does your organization plan to use blockchain for?**
More than one response permitted

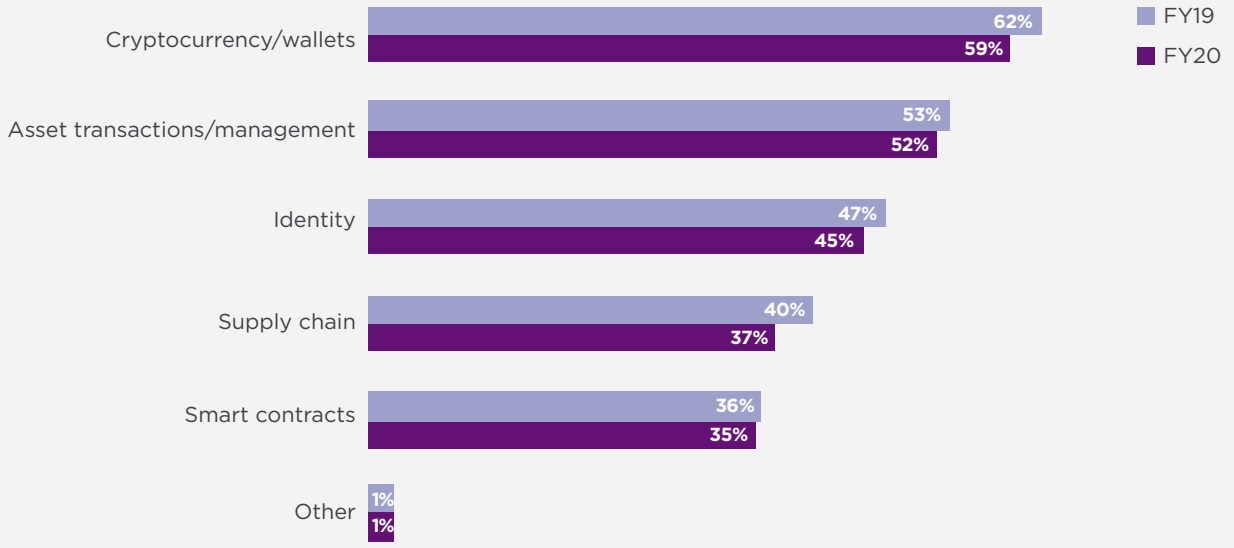
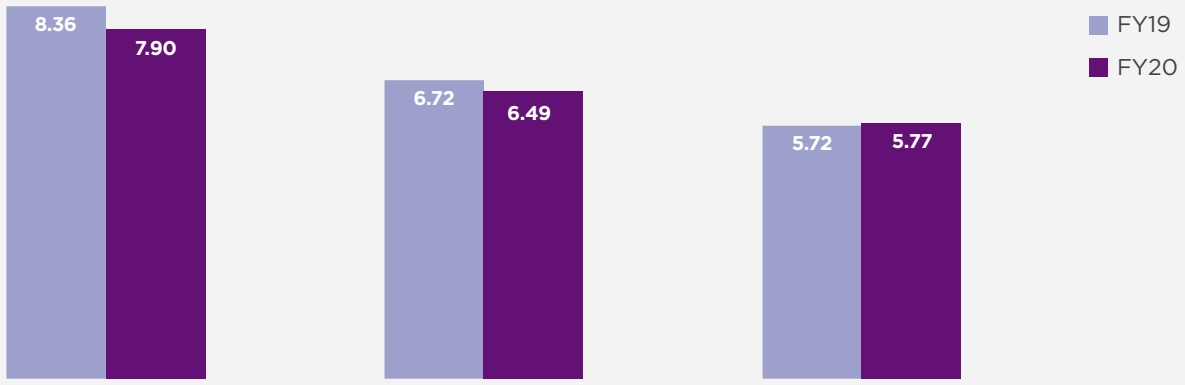


Figure 13. **When do you think the following solutions will achieve mainstream enterprise adoption?**
Extrapolated values in years



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 14 clearly shows that 56 percent of respondents chose ratings at or above 7; thus, suggesting a fairly high pain threshold.

Figure 15 shows the 7+ ratings on a 10-point scale for each country. As can be seen, the average percentage in all country samples is 56 percent, which suggests respondents view managing keys as a very challenging activity.

Figure 14. **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

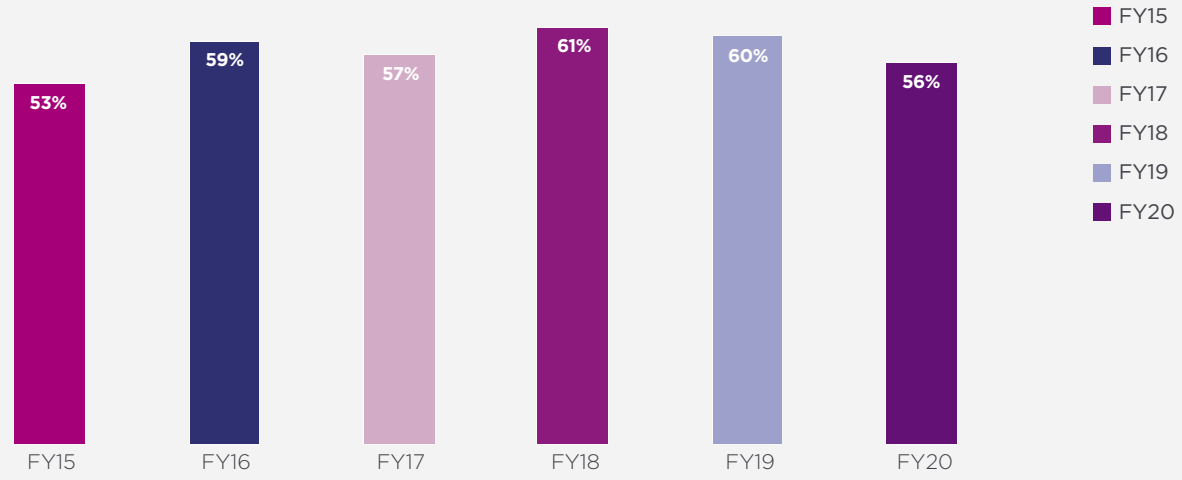
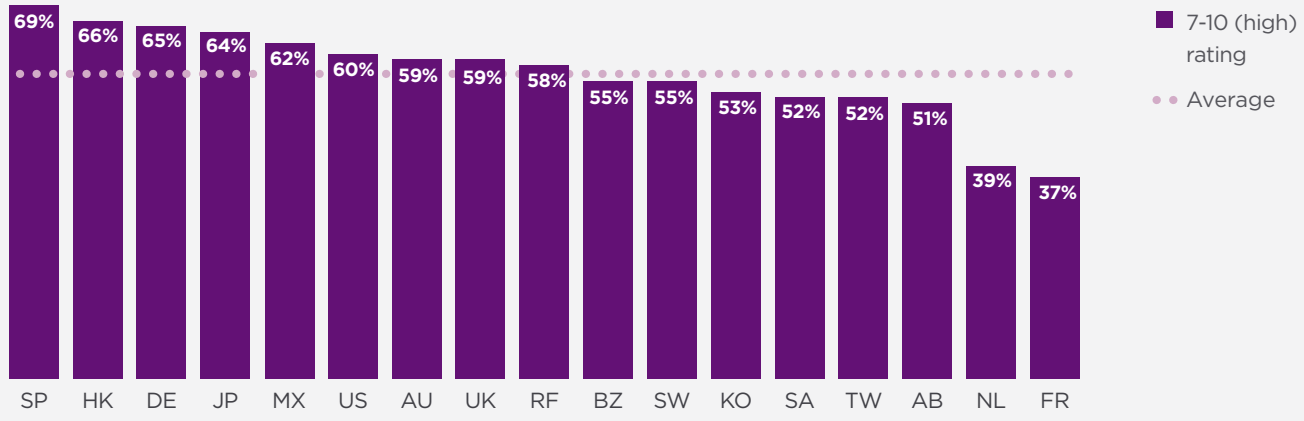


Figure 15. **Percentage "pain threshold" by country**
Percentage 7 to 10 rating on a 10-point scale



The highest percentage pain threshold of 69 percent occurs in Spain. At 37 percent, the lowest pain level occurs in France.

Why is key management painful? Figure 16 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) isolated or fragmented key management systems.

Which keys are most difficult to manage? In the top position on this list for the fourth year as the most difficult keys to manage, are keys for external cloud or hosted services.

As shown in Figure 17 on the following page, this is followed by SSH keys, signing keys, and end user encryption keys. The least difficult include: (1) encryption keys for archived data, (2) encryption keys for backups and storage and (3) embedded device keys.

Figure 16. **What makes the management of keys so painful?**
Country samples are consolidated. Three responses permitted

The top three reasons why key management is painful:

#1 No clear ownership of the key management function
#2 Lack of skilled personnel
#3 Isolated or fragmented key management systems

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)[5]

The United States, Germany and Japan organizations are more likely to deploy HSMs. Figure 18 summarizes the percentage of respondents that deploy HSMs. The United States, Germany and Japan are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 49 percent.

Figure 17. **Types of keys most difficult to manage**
Country samples are consolidated. Very painful and painful responses combined

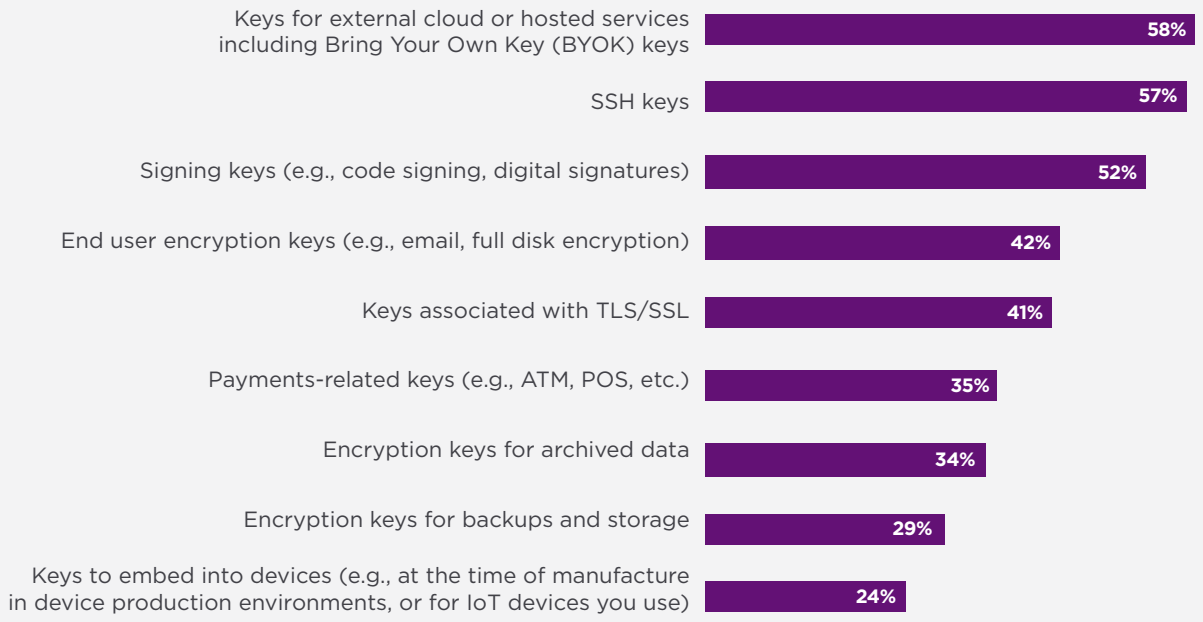
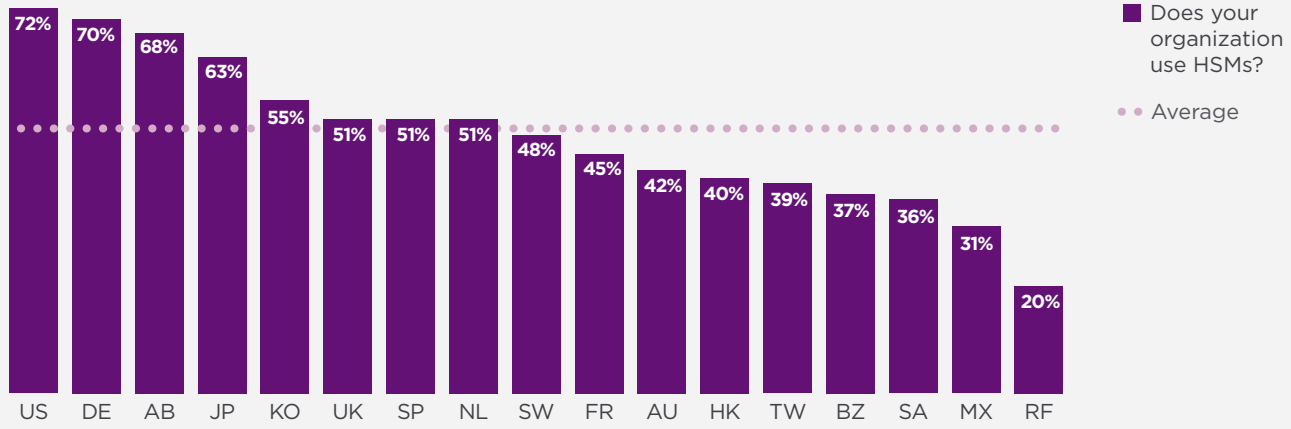


Figure 18. **Deployment of HSMs**
Yes responses presented



[5] 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 associated with server based applications 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.

Deployment of HSMs increases steadily. Figure 19 shows a nine-year trend for HSMs. As can be seen, the rate of global HSM deployment has steadily increased.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. As shown in Figure 20, 41 percent of respondents own and operate HSMs on-premise for cloud-based applications, and 39 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, respondents predict a significant increase in the ownership and operation of HSMs on-premise and the integration with a Cloud Access Security Broker to manage keys and cryptographic operations.

Figure 19. **HSM deployment rate over eight years**
Country samples are consolidated

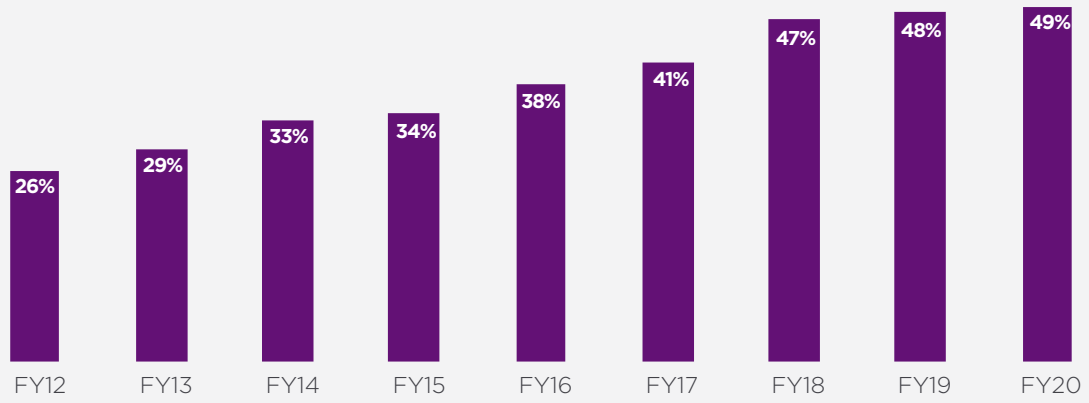


Figure 20. **Use of HSMs in conjunction with public cloud-based applications today and in the next 12 months**
More than one choice permitted

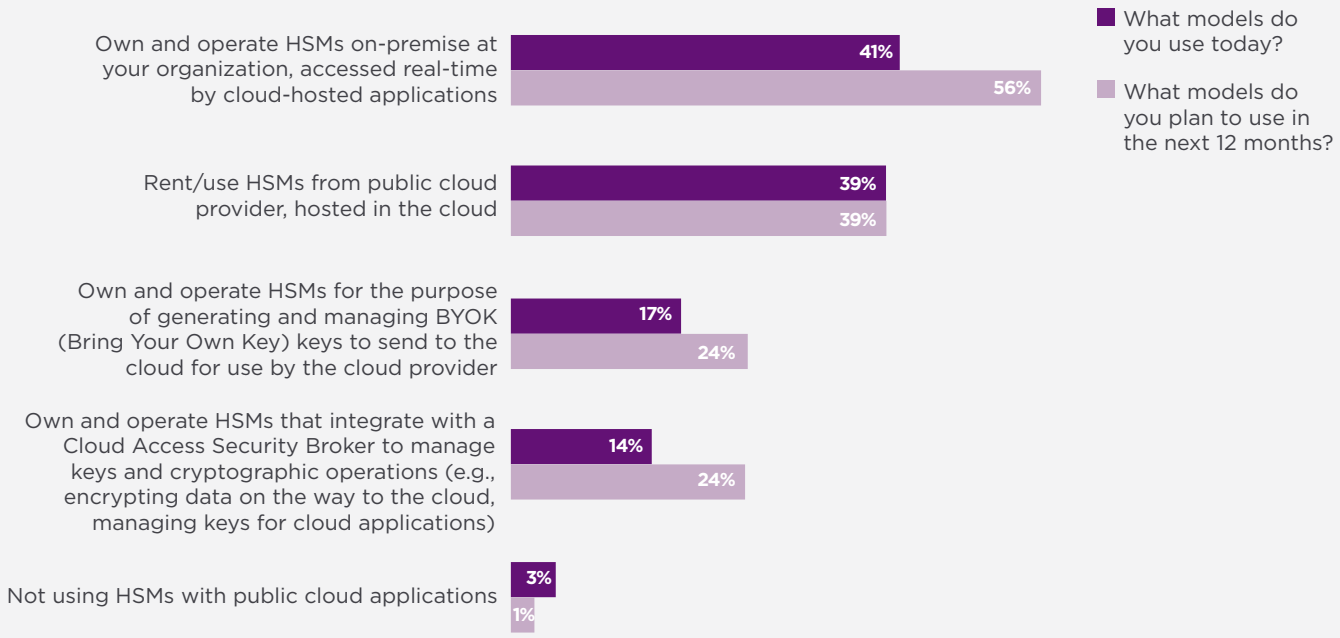


Figure 21 summarizes the percentage of respondents in 17 countries that rate HSMs as either very important or important to their organization's encryption or key management program or activities. The overall average importance rating in the current year is 66 percent. The pattern of responses suggests the United States, Middle East and the Netherlands are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

Figure 22 shows a nine-year trend in the importance of HSMs for encryption or key management, which has steadily increased over time.

Figure 21. **Perceived importance of HSMs as part of encryption or key management**
Very important & important responses combined

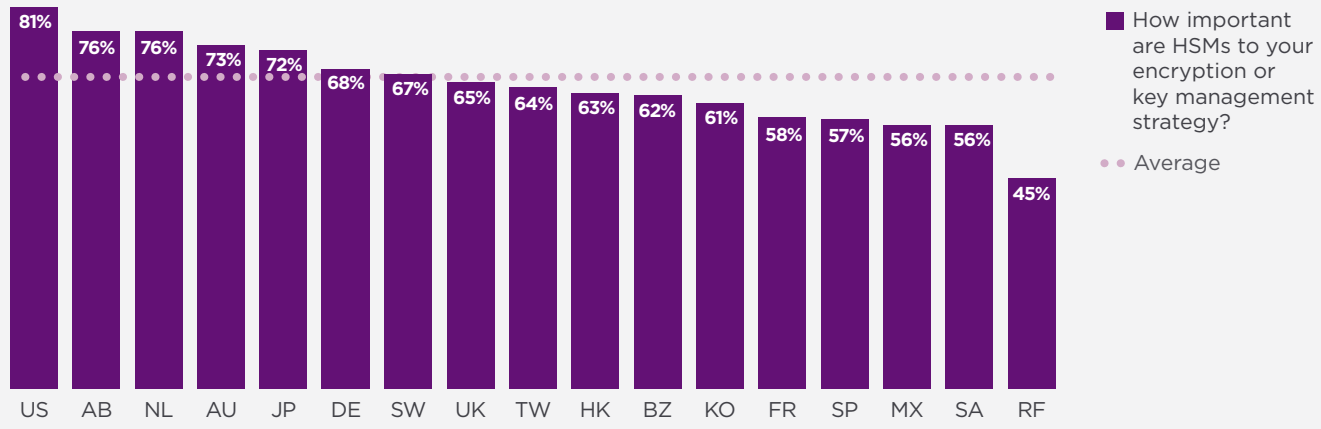
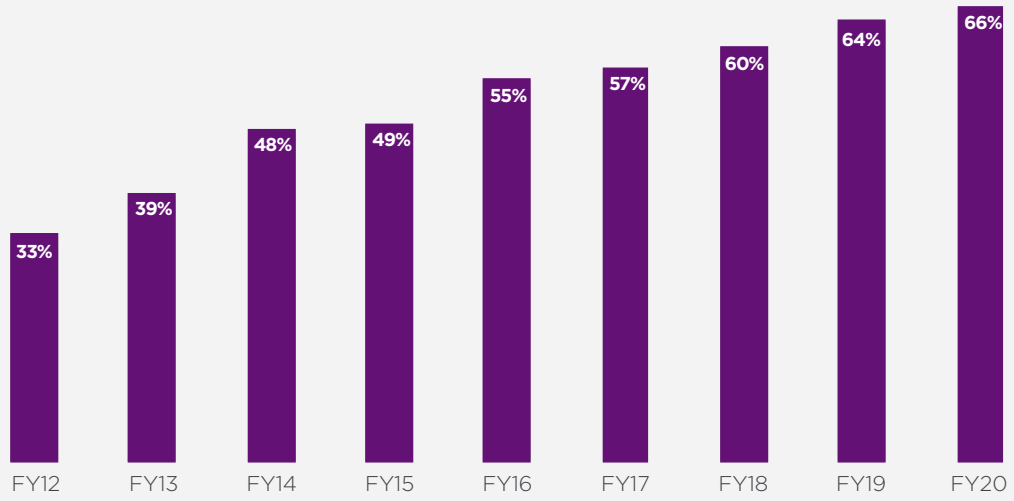
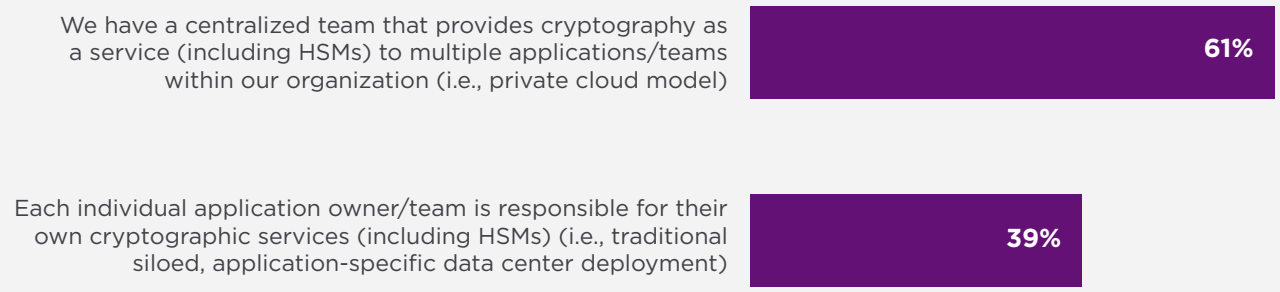


Figure 22. **Perceived importance of HSMs as part of encryption or key management over nine years**
Country samples are consolidated



What best describes an organization's use of HSMs? As shown in Figure 23, 61 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). Thirty-nine 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.

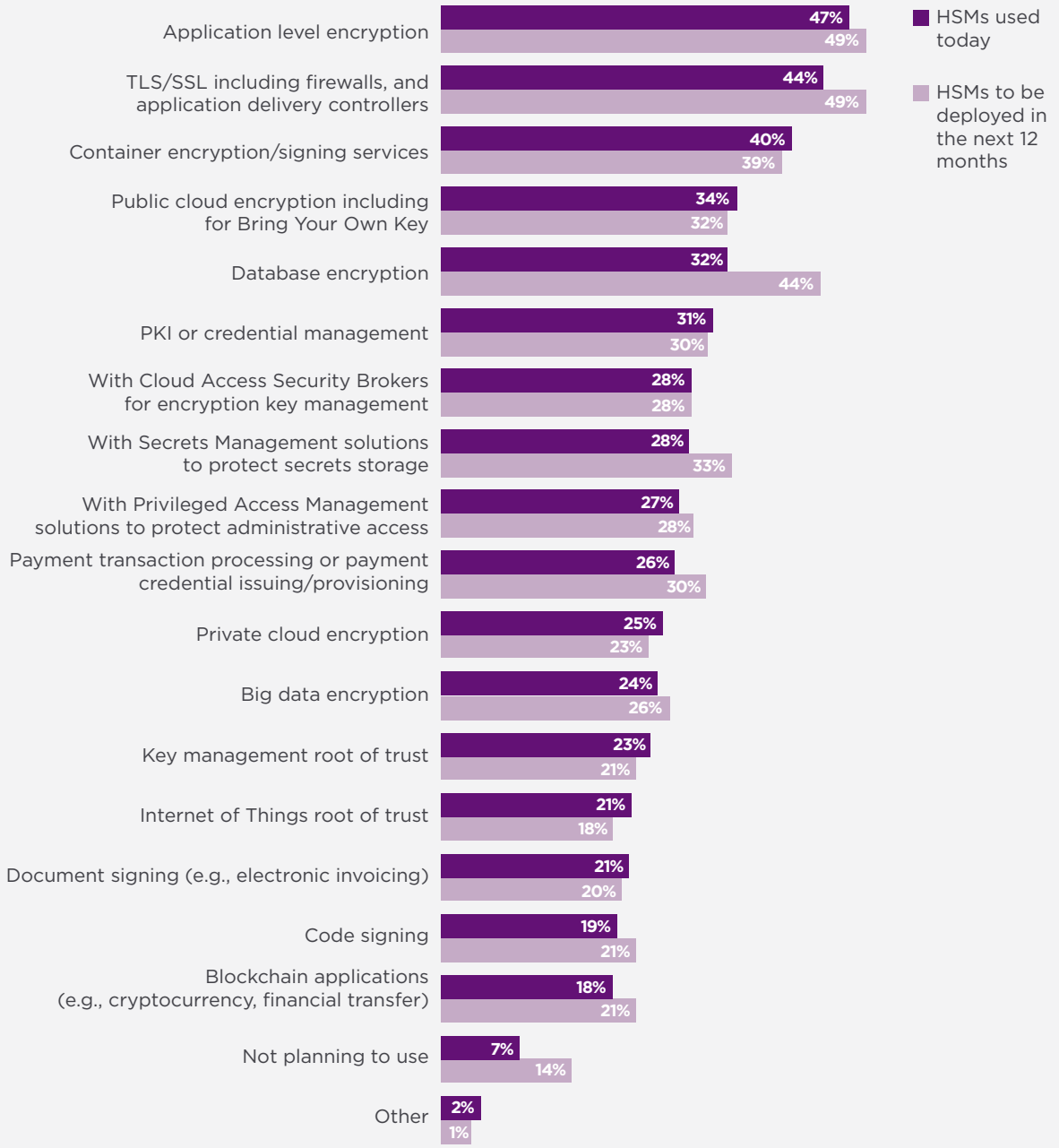
Figure 23. **Which statement best describes how your organization uses HSMs?**



What are the primary purposes or uses for HSMs? Figure 24 summarizes the primary purpose or use cases for deploying HSMs. As can be seen, the top three choices are application-level encryption, TLS/SSL, followed by container encryption/signing services. This chart shows a significant increase in the use of database encryption 12 months from now.

It is significant to note that HSM use for application-level encryption will soon be deployed in 49 percent of the organizations represented in this study.

Figure 24. **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 25, 60 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 24 percent 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.

According to Figure 26, with respect to the transfer of sensitive or confidential data to the cloud, the United States, Germany, Japan, the United Kingdom, and the Netherlands are more frequently transferring sensitive data to the cloud.

Figure 25. **Do you currently transfer sensitive or confidential data to the cloud?**
Country samples are consolidated

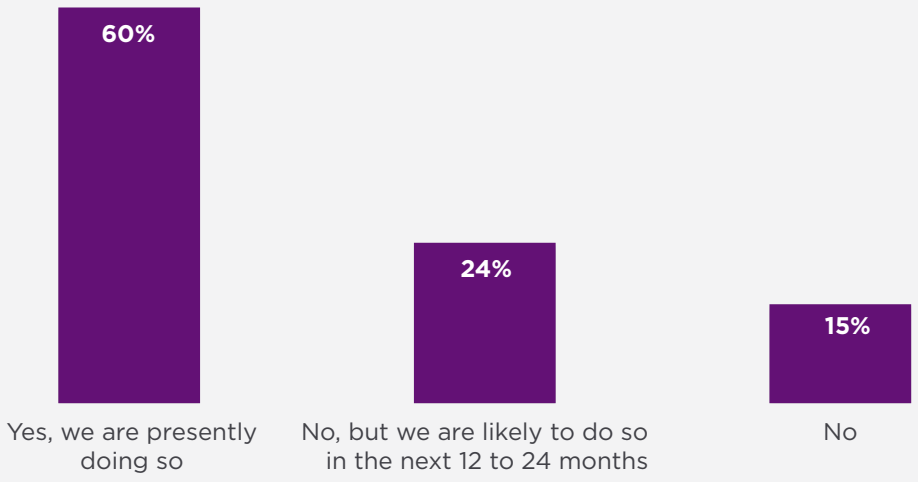
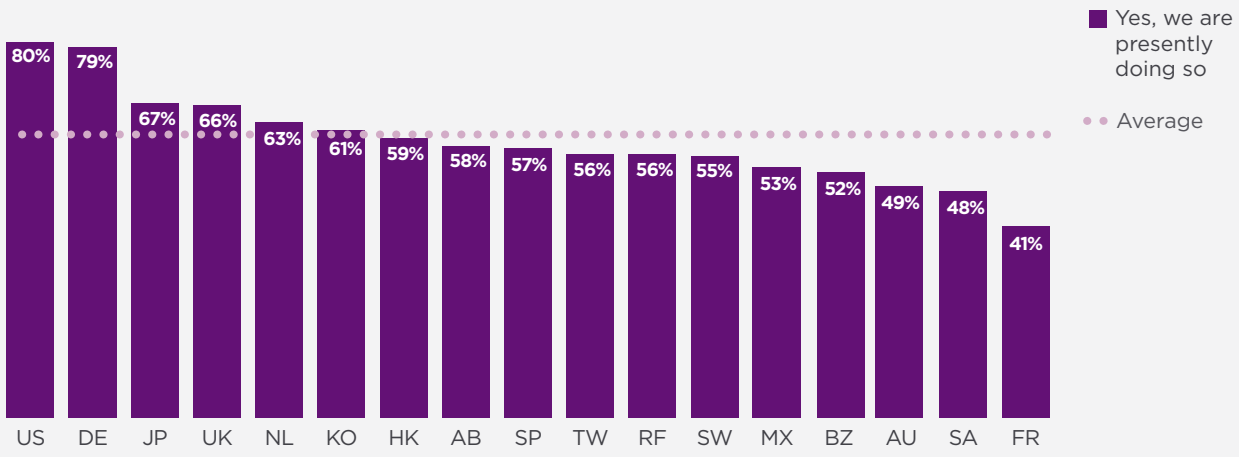


Figure 26. **Organizations that transfer sensitive or confidential data to the cloud by country**



How do organizations protect data at rest in the cloud? As shown in Figure 27, 38 percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 36 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty-one percent of respondents are using some form of Bring Your Own Key (BYOK) approach.

What are the top three encryption features specifically for the cloud? The top three features are support for the KMIP standard for key management (59 percent of respondents), SIEM integration, visualization and analysis of logs (59 percent of respondents) and granular access controls (55 percent of respondents), as shown in Figure 28.

Figure 27. **How does your organization protect data at rest in the cloud?**
Country samples are consolidated. More than one choice permitted

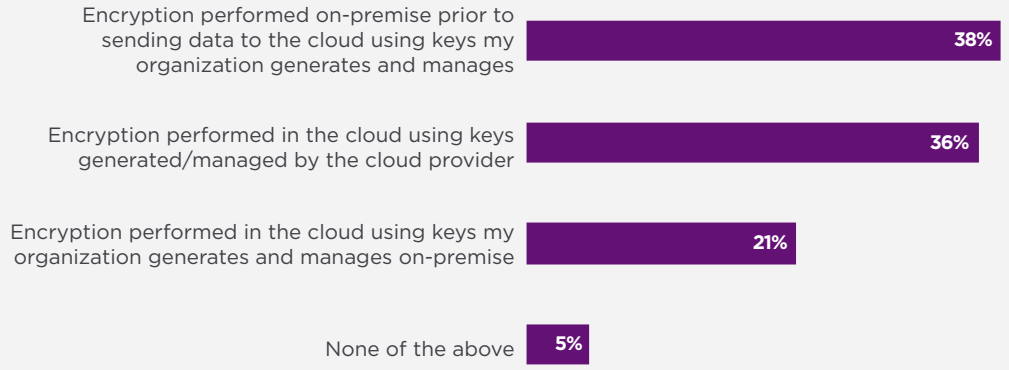
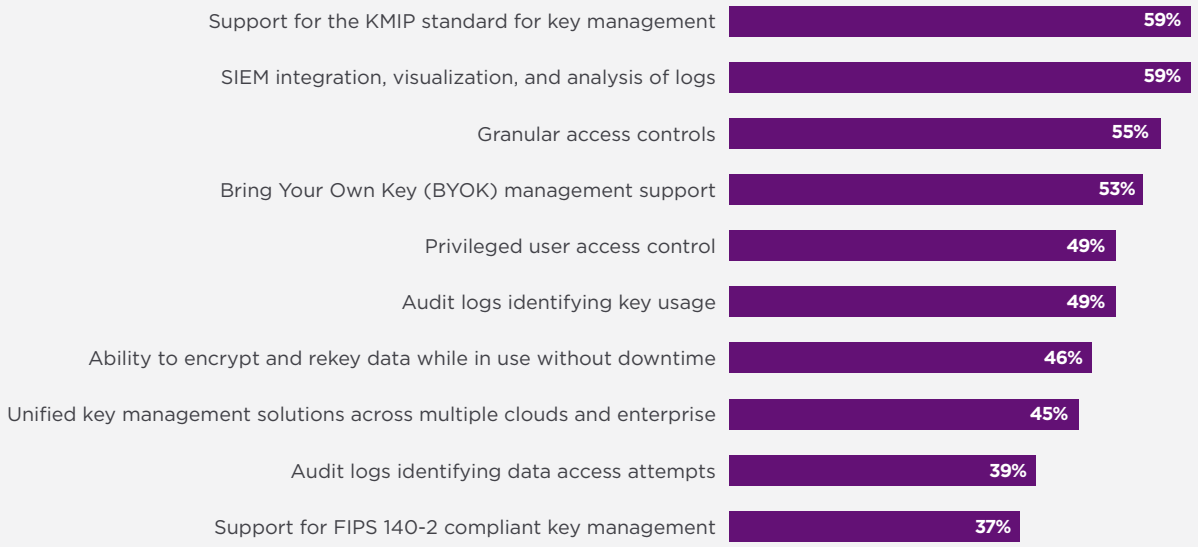


Figure 28. **How important are the following features associated with cloud encryption to your organization?**
Very important and Important responses combined



APPENDIX
Methods & Limitations

Table 1 reports the sample response for 17 separate country samples. Data collection was started in December 2020 and completed in January 2021. Our consolidated sampling frame of practitioners in all countries consisted of 161,607 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 7,331 returns of which 721 were rejected for reliability issues.

Our final consolidated 2020 sample was 6,610, thus resulting in an overall 4.1% 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 samples. Trend analysis was performed on combined country samples. This year we added Spain.

Table 1. Survey response in 17 countries

Legend	Survey response	Sampling frame	Final sample	Response rate
AB	Middle East	9,875	373	3.8%
AU	Australia	6,595	317	4.8%
BZ	Brazil	13,046	553	4.2%
FR	France	10,981	451	4.1%
DE	Germany	11,400	467	4.1%
HK	Hong Kong	5,660	267	4.7%
JP	Japan	11,130	487	4.4%
KO	Korea	9,337	406	4.3%
MX	Mexico	10,551	369	3.5%
NL	Netherlands	7,992	322	4.0%
RF	Russian Federation	6,195	211	3.4%
SA	Southeast Asia	7,500	276	3.7%
SP	Spain	9,224	459	5.0%
SW	Sweden	6,901	275	4.0%
TW	Taiwan	6,895	292	4.2%
UK	United Kingdom	10,330	408	3.9%
US	United States	17,995	677	3.8%
	Consolidated	161,607	6,610	4.1%

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

Table 2. Sample history over 14 years

Legend	FY20	FY19	FY18	FY17	FY16	FY15	FY14	FY13	FY12	FY11	FY10	FY09	FY08	FY07
AB	373	342	340	308	316	368								
AU	317	325	327	315	331	334	359	414	938	471	477	482	405	
BZ	553	471	517	507	463	460	472	530	637	525				
FR	451	354	332	370	345	344	375	478	584	511	419	414		
DE	467	473	531	543	531	563	564	602	499	526	465	490	453	449
HK	267	267	317											
JP	487	504	502	468	450	487	476	521	466	544				
KO	406	321	325	317										
MX	369	353	499	468	451	429	445							
NL	322	302												
RF	211	216	226	196	206	201	193	201						
SA	276	276	268											
SP	459													
SW	275	277												
TW	292	302												
UK	408	389	402	468	460	487	509	637	550	651	622	615	638	541
US	677	689	683	710	701	758	789	892	531	912	964	997	975	768
Total	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	1,758

Figure 29 reports the respondent's organizational level within participating organizations. By design, 55 percent of respondents are at or above the supervisory levels and 43 percent of respondents reported their position as associate/staff/technician. Respondents have on average 9.8 years of security experience with approximately 6.7 years of experience in their current position.

Figure 30 identifies the organizational location of respondents in our study. Over half (52 percent) of respondents are located within IT operations. This is followed by security at 21 percent of respondents, compliance (10 percent of respondents) and lines of business (9 percent of respondents).

Figure 29. **Distribution of respondents according to position level**
Country samples are consolidated

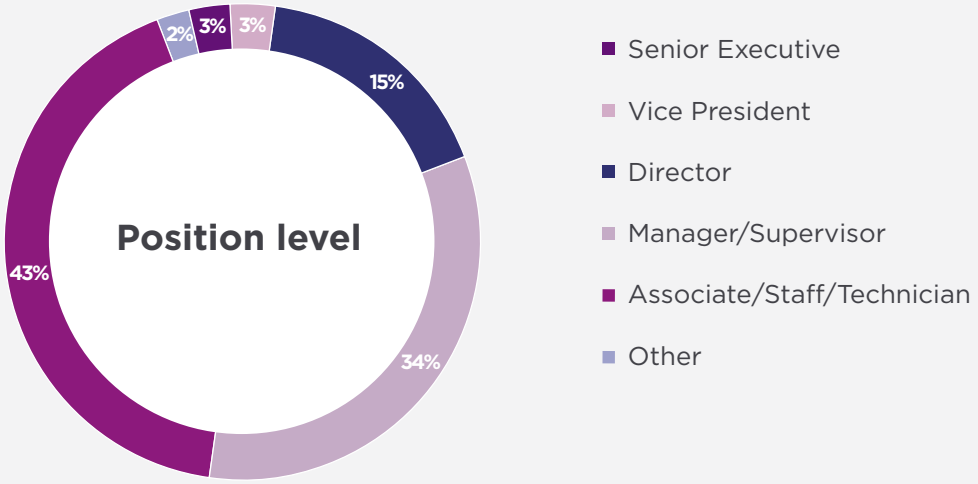


Figure 30. **Distribution of respondents according to organizational location**
Country samples are consolidated

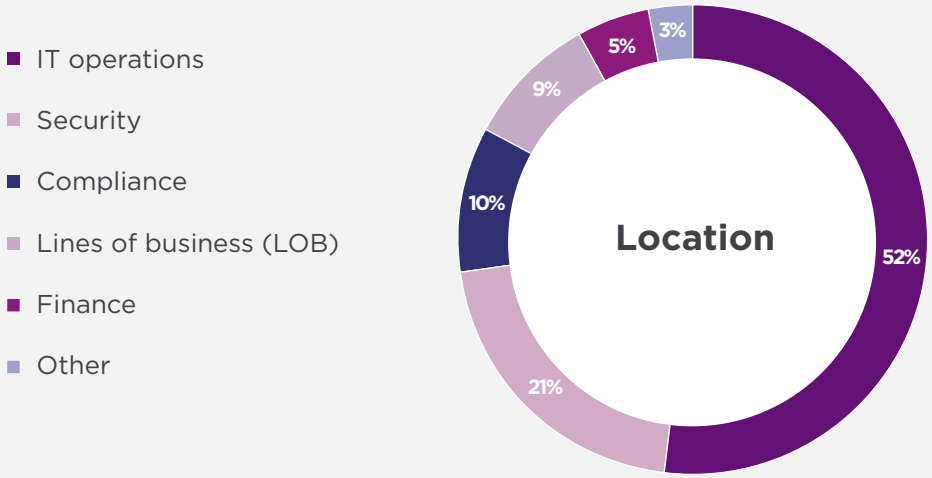


Figure 31 reports the industry classification of respondents' organizations. Fifteen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Twelve percent of respondents are located in manufacturing and industrial organizations, 9 percent of respondents are in service organizations, nine percent are located in the technology and software sector.

According to Figure 32 more than half (58 percent) of respondents are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 31. **Distribution of respondents according to primary industry classification**
Country samples are consolidated

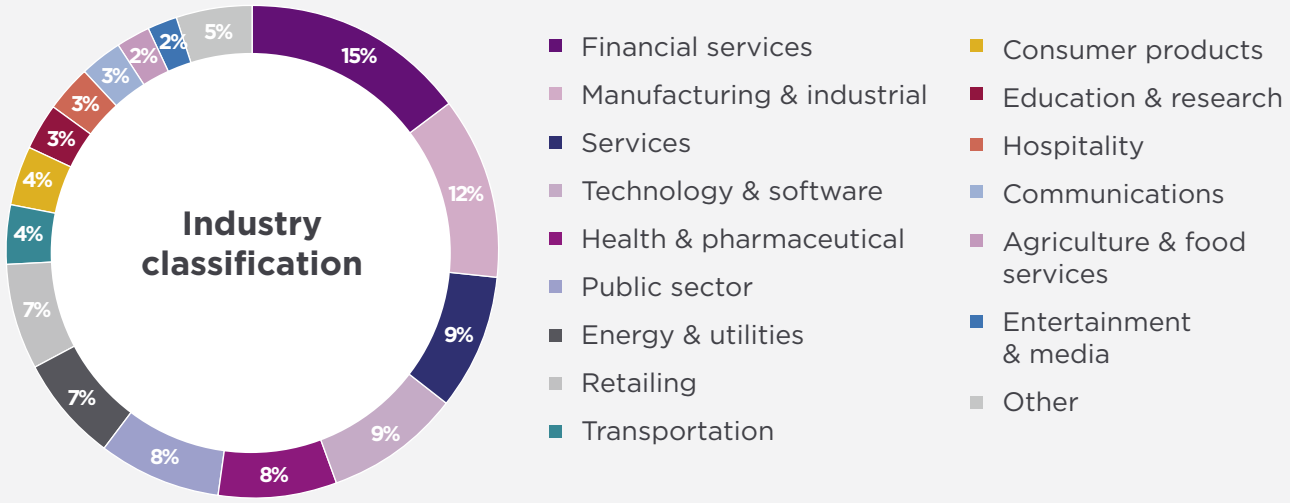
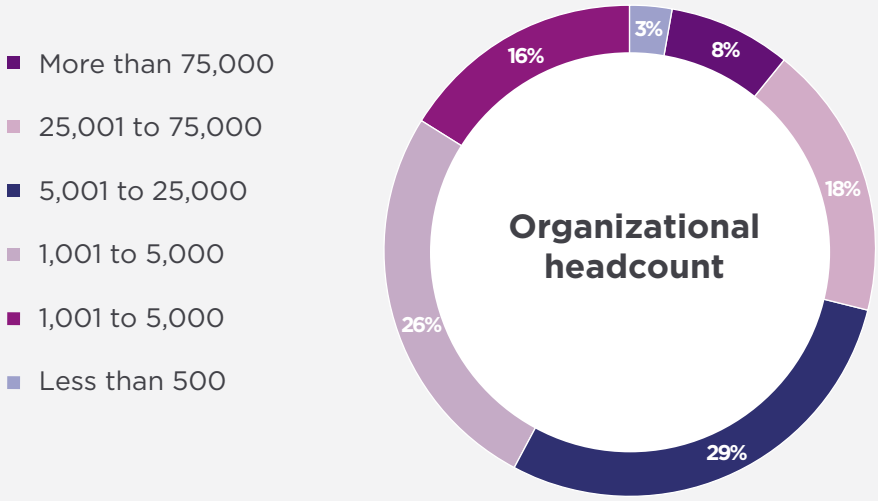


Figure 32. **Distribution of respondents according to organizational headcount**
Country samples are consolidated



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 2021 Global Encryption Trends Study consolidated findings at:
Entrust.com/go/2021-GETS-findings

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.

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