



360° Encryption Services

Encryption Consulting Study on Global Encryption Trends – 2022

Compare your organization's encryption strategy with our global firm's trends and understand data protection strategies across multi-dimensional platform analysis.



Part 1. MANAGEMENT SUMMARY	03
Part 2. DEEP DIVE ANALYSIS	08
Encryption Strategy Adoption	10
Trend Analysis	12
Futuristic Encryption Trends	13
Development Options	14
Key Drivers for Encryption	15
Barriers for Encryption	15
Encryption Features & Data Types	16
Kubernetes Security	18
Key Management Analysis	19
Importance of Hardware Security Modules (HSMs) ...	21
Cloud Encryption	26
ABOUT ENCRYPTION CONSULTING	28



A.

Management Summary

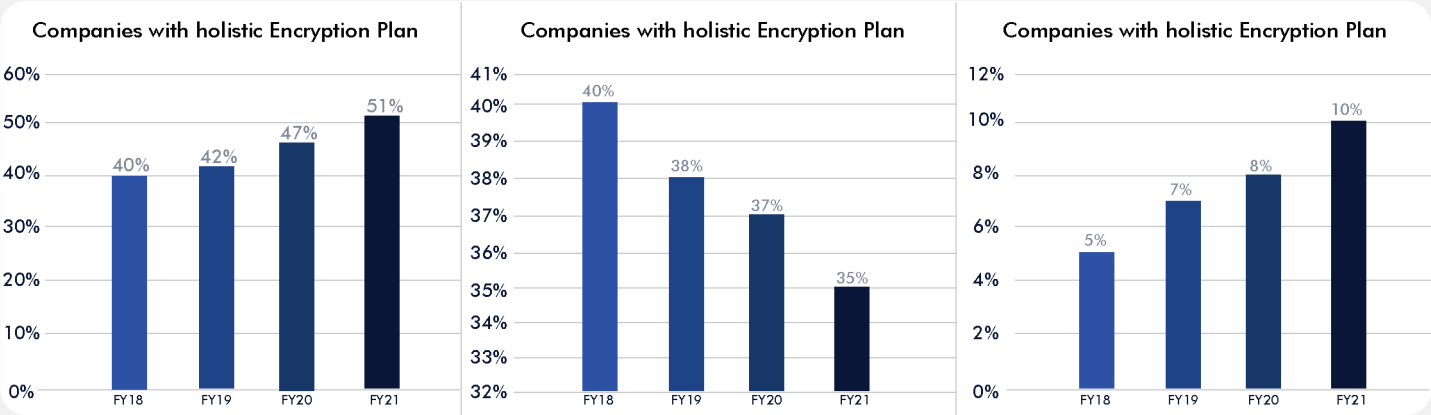
ENCRYPTION CONSULTING FINDINGS

FROM THE GLOBAL TRENDS STUDY 2022

A survey has been performed with 3,250 encryption/data protection experts across multiple industry sectors in multiple countries which includes United States, the Middle East, Spain, Germany, Japan, Hong Kong, Mexico, the United Kingdom, South Korea, and Taiwan as major targets. The major focus of this survey is to understand the encryption strategy of various firms across industries. Encryption has become an important part of data protection strategies over the years. It has since evolved into a critical aspect in the security posture of firms across various sectors and industries. Encryption Consulting's survey considered the nature of firms under different jurisdictions and geographies to better understand their encryption trends. Figure 1 below shows results of the

survey performed to understand the nature of encryption strategies followed by the target research audience. The survey results clearly indicated that firms are becoming more conscious about their encryption strategy with the steady increase in numbers for the first response. This year's responses to our survey from those in the encryption field are made up of 50% who use an overarching encryption strategy, as opposed to a partial encryption strategy. There is a decreasing trend seen in organizations with a localized partial encryption strategy and they are moving towards a holistic encryption strategy for their firms. Following are the findings from the research performed about encryption strategy:

Figure 1. Companies response to survey about Encryption Strategy



1. This year's data collection was started and completed in 2021.
2. Country-level results are abbreviated as follows: Australia(AU),Brazil(BZ),France(FR),Germany(DE),HongKong(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 4 years (since2018).

SURVEY TREND ANALYSIS

The results from the survey (as seen above) conclude that there has been better awareness in organizations regarding encryption strategy. There is a steady increase in the percentage of respondents with an overarching encryption strategy. In turn, there has been a steady decline in organizations not having an encryption plan strategy. Also, one good sign observed from the responses is the number of organizations across the globe spending on research and knowledge of futuristic encryption trend possibilities for planning ahead to implement strategies for the future.

The geographic aspect and country/state laws played a major role in shaping the encryption strategy of the firms. Demographics with mature laws & regulations forced the companies to have a more advanced encryption strategy. 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.

As per the survey conducted by the Ponemon Institute, it is evident that 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 influential. IT operations are most influential in Sweden, Korea and France.

51% of the responding organizations have an overall encryption strategy deployed in their firms and it is a 11% increase when compared to the trend from FY18.

FUTURE ENCRYPTION TRENDS

Cloud computing has become a top priority for many organizations that participated in the survey. One interesting finding from the survey is that almost 10% of the respondents are already preparing their strategies with upcoming encryption trends. A major focus is on the following four options: Bring Your Own Encryption (BYOE), Blockchain technology, Homomorphic Encryption and Quantum crypto-agile solutions.

COMPANIES PREFERRED DEPLOYMENT OPTIONS

There is no major inclination towards any of the deployment options for encryption in the organizations. However, most respondents are prioritizing data-at-rest encryption and cloud encryption slightly higher when compared to the rest. One good sign is the respondents looking at the futuristic encryption trends and at least started partial deployment in domains such as IoT. This is a good trend considering the ever-increasing threat landscape for sensitive data.

We can infer from the above conclusion that companies are not inclined to any one particular deployment option, but are focused on implementing encryption holistically across the organization.

KEY DRIVERS FOR ENCRYPTION

The major motivational driver for implementing encryption is the protection of customers' personal information. Around 60% of the respondents using encryption for the purpose of protecting customers' personal information, 50% of the respondents mentioned that they use encryption to protect information against specific, identified threats, and 49% use it for the protection of enterprise intellectual property. Compliance is one of the key business drivers for adoption of encryption technology. The encryption of consumer data is one of the fundamental requirements for all these regulations, with both in-transit data as well as data-at-rest being covered within the scope for encryption. While the choice of encryption algorithms, technologies and vendors is left to the enterprise, non compliance can lead to significant penalties, especially in the event of data breaches.

BARRIERS FOR ENCRYPTION

Data discovery is a key barrier identified during our survey for about 65% of the respondents for implementing encryption. About 49% of the respondents mentioned a lack of technical skill for implementing and managing encryption as a barrier.



Along with these two critical barriers, the third most critical barrier is the classification of the organization's sensitive data. An Interesting finding is that organizations are willing to hire expert resources or trusted consulting firms to over come these barriers and implement encryption across the crown jewel business functions.

TOP PRIORITY ENCRYPTION FEATURES AND DATA TYPES

Encryption Consulting's survey focused on identifying the priority features respondents look for while developing their encryption strategy and here are the findings. As per the survey findings, Key Management, System Performance, and Policy Enforcement are considered to be more critical and given higher priority when compared to other encryption features.

Highest priority is given to customers' sensitive data by the organizations. Supported by this parameter, we've understood the foremost important data types targeted for encryption. In the Financial industry, the highest priority is to encrypt payment-related data an monetary records, because of high-profile data breaches.

Non-financial information is the least preferred data to be encrypted. Surprisingly, some of the respondents did not give deserved priority to health care information for encryption. When asked "what are the two most important and critical encryption modules?", we received an unanimous response pointing to 1. Key Management 2. Hardware Security Modules (HSMs). Here is our analysis about those two modules.

KEY MANAGEMENT ANALYSIS

Key Management is considered one of the critical encryption options to implement and management. Over 60% of the respondents reported that Key Management is the most challenging activity. Key Management is painful for many firms because of no clear possession of the keys and a shortage of professional employees.

ANALYSIS ON HARDWARE SECURITY MODULES (HSMs)

Organizations have begun realizing the importance of Hardware Security Modules (HSMs) in recent years. The global deployment rate of these devices has risen from 43% in 2018 to 52% in 2021 according to our research performed on hetero demographic respondents. With ever-changing technologies, organizations must keep up to be successful. These changes can lead an organization down two paths. One may lead to growth and prosperity, but the other may lead to destruction and despair.

55% of the total respondents mentioned that privacy and data protection compliance is the main driving force HSM implementation.

HSM USAGE BY ORGANIZATIONS:

Companies have various ways of usage when it comes to HSMs. The majority of the respondents – about 61%– mentioned that they use cryptography-as-a-service, including HSMs, for their internal business functions and units leveraging the private cloud model. Around 39% responded that they follow the conservative approach of vesting the ownership of cryptographic services with the individual application owner.

CRITICAL USES OF HSMs:

55% of organizations have said compliance with privacy and data security requirements is their top driver for implementing HSMs. The top three uses are application-level encryption, TLS/SSL, and container encryption/signing services. One year from now there may be a significant increase in the usage of database encryption.

CLOUD ENCRYPTION

There has been a steady increase in organizations with an encryption strategy applied across the entire enterprise as Cloud Encryption is considered one of the most critical encryption options for most of the respondents. 63% of respondents say their organizations are leveraging cloud platforms (public and/or private) for storing & processing of their sensitive data. Out of these respondents, 52% are already implementing one or more encryption technologies to protect the sensitive data stored in the cloud. 31% of the respondents are planning to implement cloud encryption over the next two years.


How Do Organizations Protect Data At Rest In The Cloud?

Respondents usually prefer to encrypt one of the following options to encrypt data-at-rest in the cloud. These options are encryption performed on-premises before storing the data on the cloud, trusting the cloud provider to perform encryption, and a Bring Your Own Key (BYOK) approach. 40% of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages.

Also, a good percentage of respondents i.e 34% leverage the cloud provider's key management for performing encryption in the cloud. The BYOK approach is followed by 21% of the respondents.

What are the top three challenges faced by organizations regarding cloud encryption?

The top three challenges identified for cloud implementation are as follows: 59% of the respondents felt Key Management was the biggest challenge because the loss of encryption keys is a major concern, as it can render any encrypted data useless while poor key management can put critical data at risk. Technical expertise was next, chosen by 42% of the respondents, and finally 28% of respondents feel performance and integration issues are a major concern.



60% of the respondents are leveraging cloud platforms to store their sensitive and critical data.



Deep Dive Analysis

LET US DEEP DIVE INTO THE FINDINGS FROM THE SURVEY IN THIS SECTION.

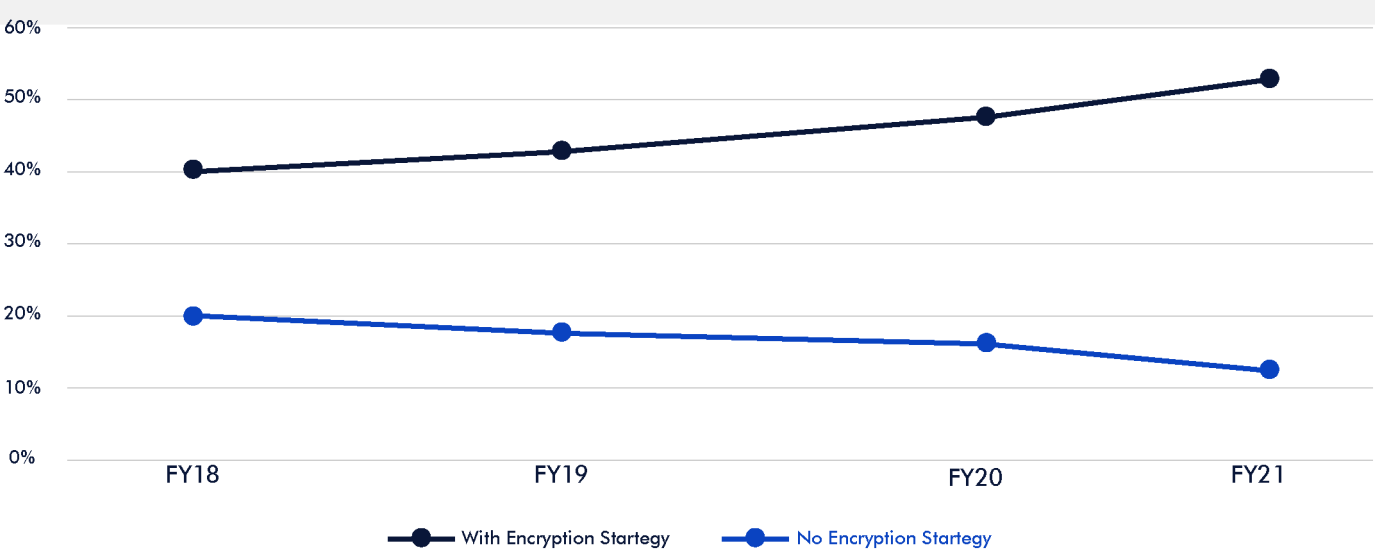
Key Focus Points

- Encryption Strategy Adoption
- High Level Trend Analysis
- Future Encryption Trend
- Deployment Options
- Key Drivers For Encryption
- Barriers For Adoption
- Top Priority Encryption Features And Data Types
- Key Management Analysis
- High Level View On HSMs*
- Cloud Encryption

Encryption Strategy Adoption

There has been a positive outcome with the encryption adoption trend by organizations across the globe. Many organizations are now trending towards adopting a holistic encryption strategy across their firm. This can be seen in the steady increase in percentage from the past four years. Also, there has been a decrease in the companies focused on implementing encryption only to limited business functions, or worse no encryption. This shows the growing importance of encryption in the cybersecurity domain.

Figure 2. Holistic Strategy vs No Strategy



*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.

According to our survey (Figure 3), Germany reported high awareness and adoption of Encryption followed by the United States, Japan and the Netherlands. Respondents from Brazil reported the lowest adoption rate for a holistic enterprise level encryption strategy. This shows the discrepancy in the level of encryption adoption across geographies and how the demographics impact the decision making. The global average of adoption is about 50 percent.

According to Figure 4, it is evident that IT Operations take the top priority in influencing the firm's encryption strategy development. Next to IT operations is the business function that shapes the encryption strategy of many organizations. Surprisingly, IT security took a backseat in the shaping of an encryption strategy for most of the respondents. This trend is seen across the United States and the United Kingdom.

Figure 3. Encryption Adoption Across The Globe

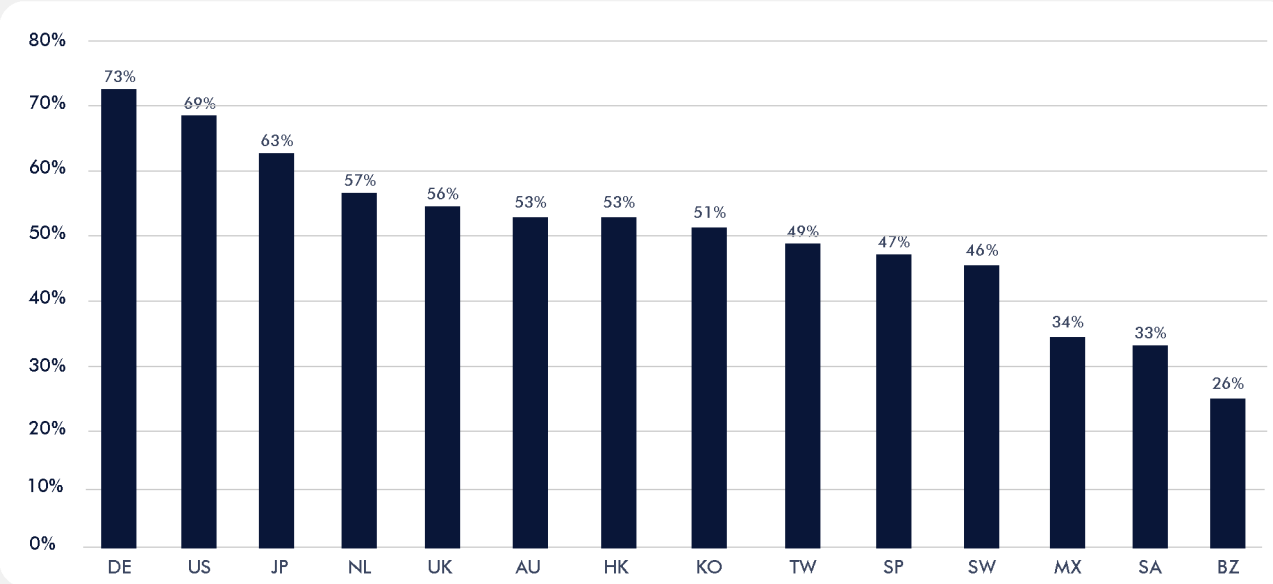
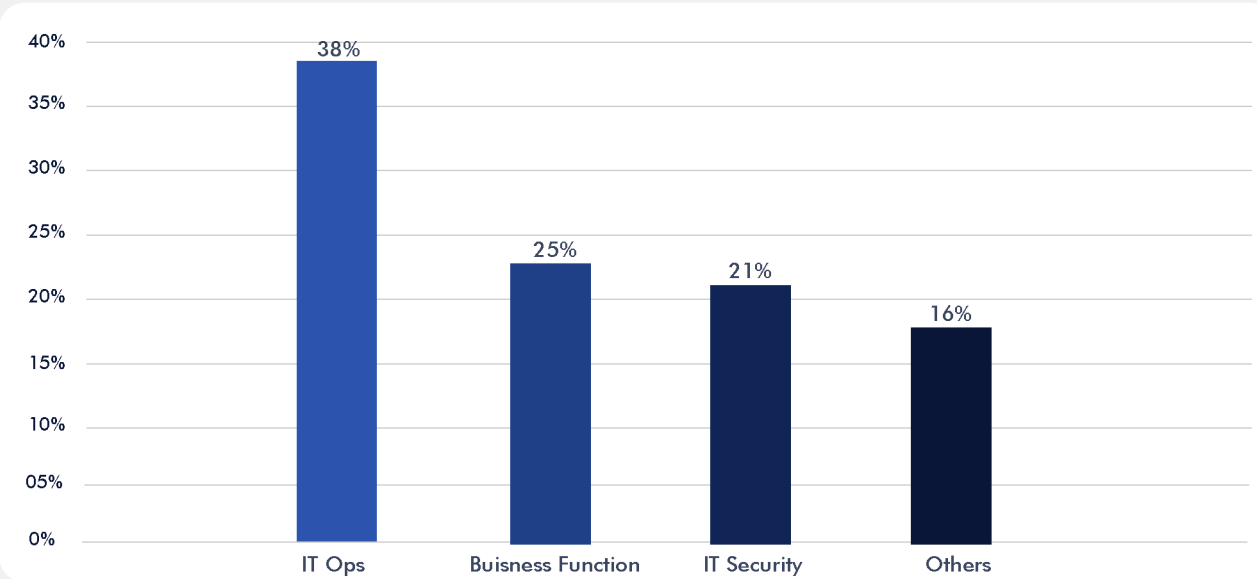


Figure 4. Factors Influencing Encryption Strategy



Because of the increased accountability of business functions with the growing adoption of Internet of Things (IoT), business functions take priority over IT Operations & IT security in most of the countries. Proliferation of employee owned devices across the organizations is another major reason for this trend.

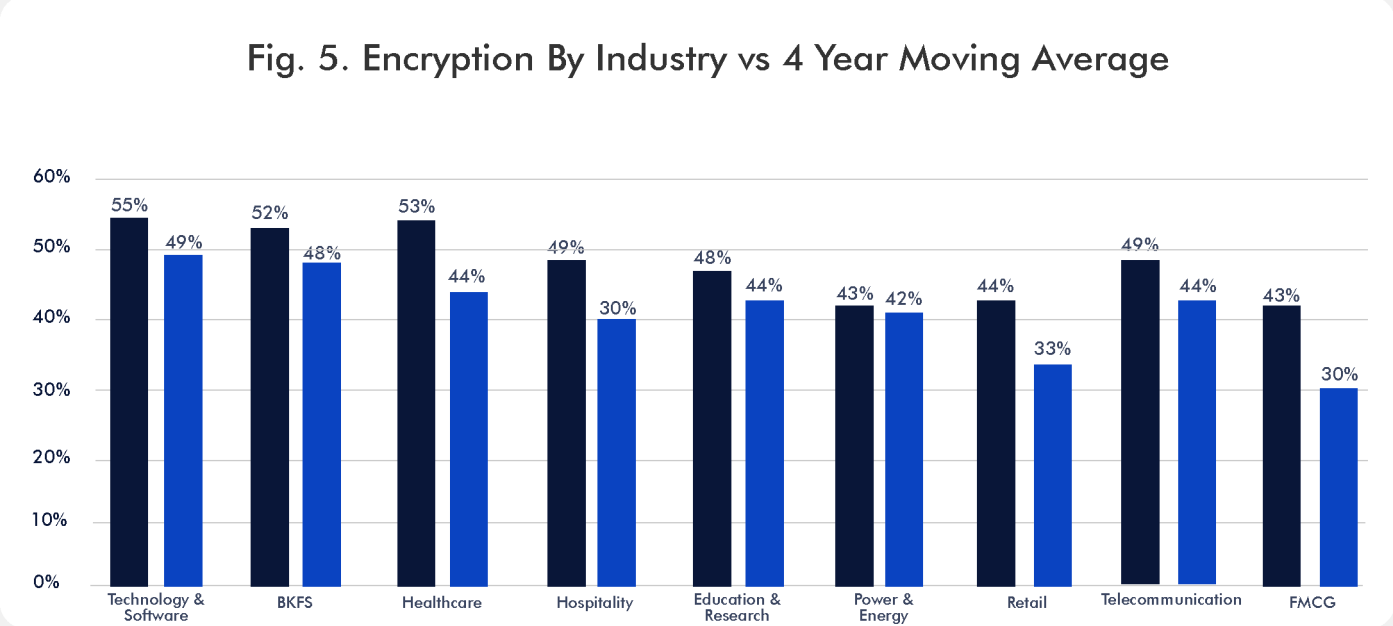
TREND ANALYSIS - ENCRYPTION ADOPTION

There is a definite increasing trend in encryption adoption and usage. Organizations across the globe are now prioritizing encryption for securing their sensitive data.

60% of survey respondents mentioned that Encryption is majorly used for protecting customers PII.

Figure 5 clearly shows the increase in the encryption adoption rate when compared with the last four years in various industrial 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. Encryption usage by industry: 2021 versus 4-year moving average



● 2021

● 4 Year Moving Average

FUTURE ENCRYPTION TRENDS

Cloud computing has become a top priority for many of the organizations who participated in the survey. One interesting finding from the survey is that almost 10% of the respondents are already preparing their strategies with upcoming encryption trends. Organizations mentioned that they are well-equipped to adopt futuristic encryption trends. As you can see in Figure 7 major focus is on "Bring Your Own Encryption(BYOE)", "Blockchain Technology", "Homomorphic Encryption" and "Quantum Crypto-Agile Solutions". There is a good steady increase in the organizations showcasing interest in researching and adopting futuristic encryption trends from FY18 to till date. Currently, about ten-percent of the respondents are already invested in Research and Development (R&D) on future trends mostly by hiring professional encryption consulting firms or by leveraging in-house talent.

38% of respondents adopting future encryption trends are focused on implementing "Bring Your Own Encryption (BYOE)"

Figure 7. projects the major point of focus organizations are placing when it comes to future trends of encryption. 38% of the respondents are focusing on "Bring Your Own Encryption (BYOE)" where the data owner generates and uses their own cryptographic keys for encryption. The second focus is on Blockchain technology with 32% followed by Homomorphic Encryption- 20% and Quantum crypto-agile solutions - 10%. We can deduce that as the threat landscape increases, companies will be cautious enough to focus on the upcoming trends of encryption for customer data protection.

Figure 6. **Year-on-year increase in the vision of organizations focusing on "Futuristic Encryption Trends"**

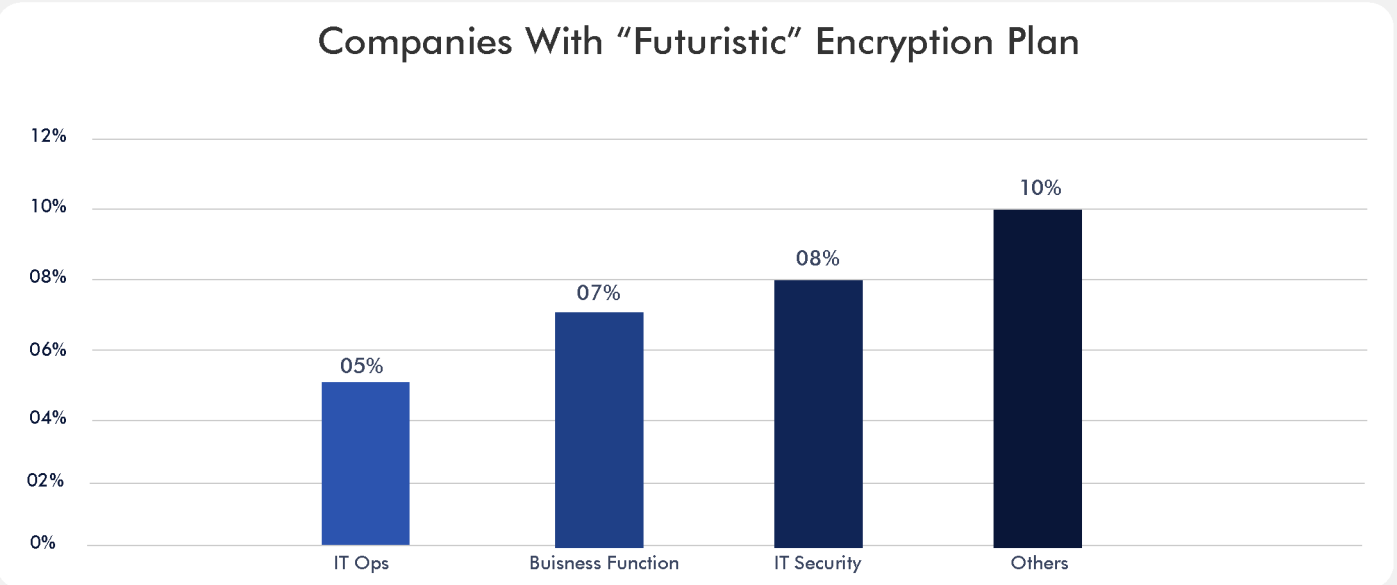
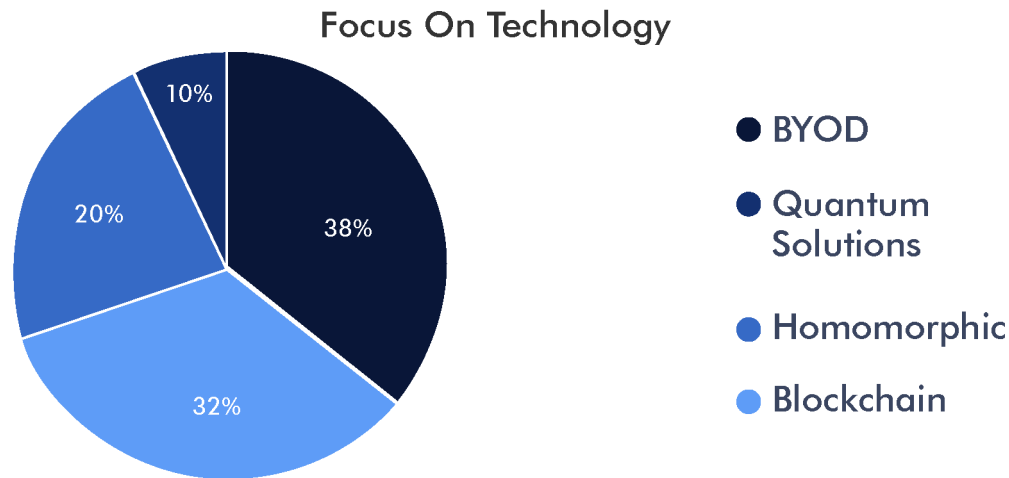


Figure 7. **Organizations major focus point regarding Future Encryption Trends**

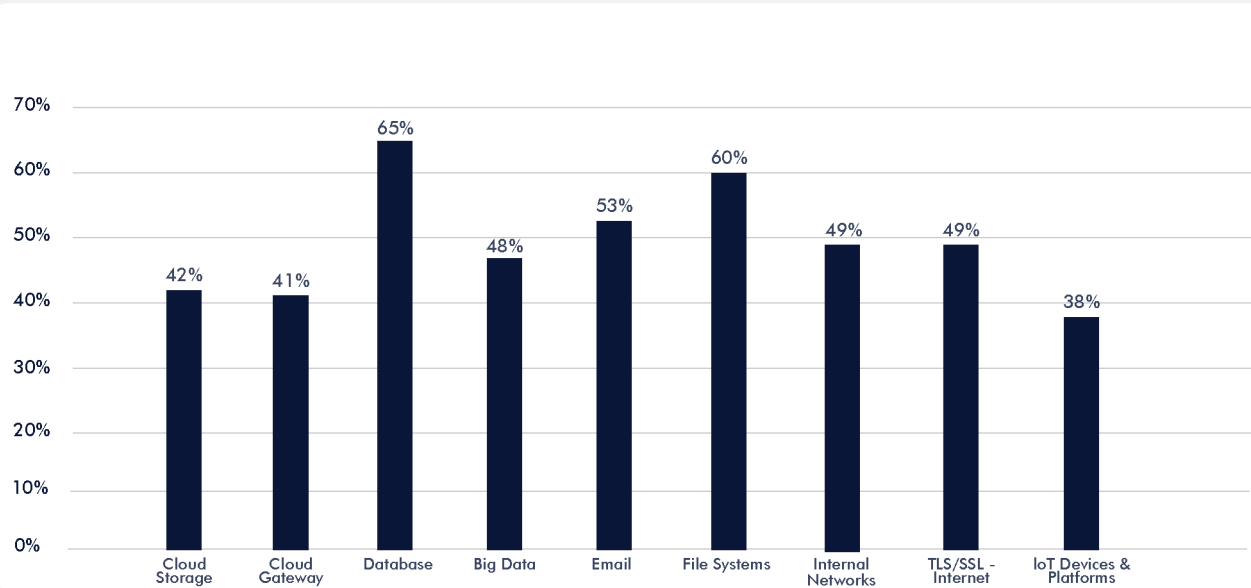


DEPLOYMENT OPTIONS

When asked about the preference in critical deployment options relevant to Encryption, most of the respondents didn't have any favorite as such but there is a definite inclination towards Data-at-rest encryption and Cloud encryption. One good sign is that organizations are already focusing on adoption encryption for IoT.

As shown in Figure 8, about 65% of respondents say encryption of IoT platforms has been partially deployed and 38% of respondents say encryption of IoT devices has been fully deployed. As it is clearly evident from the responses shown in Figure 8, all the encryption use cases are given equal priority as per their diverse needs and requirements.

Figure 8. **Holistic View On Encryption Usage Across Domains**



● Development Percentage

KEY DRIVERS FOR ENCRYPTION

The major motivational driver for implementing encryption is the protection of customer's personal information. Around 60% of the respondents using encryption for the purpose of protecting customer's personal information, 50% of the respondents mentioned that they use encryption to protect information against specific, identified threats, and 49% use it for the protection of enterprise intellectual property. Interestingly, responding organizations are least concerned about using encryption to avoid public disclosure during a data breach.

BARRIERS FOR ENCRYPTION

Data discovery is a key barrier identified during the survey for about 65% of the respondents for implementing encryption. About 49% of the respondents mentioned that lack of technical skill for implementing and managing encryption as a barrier. Along with these two critical barriers, the third most critical barrier is the classification of the organization's sensitive data. An interesting find is that organizations are willing to hire expert resources or trusted consulting firms to over come these barriers and implement encryption across the crown jewel business functions.

Figure 9. Key Drivers For Encryption Solution Implementation

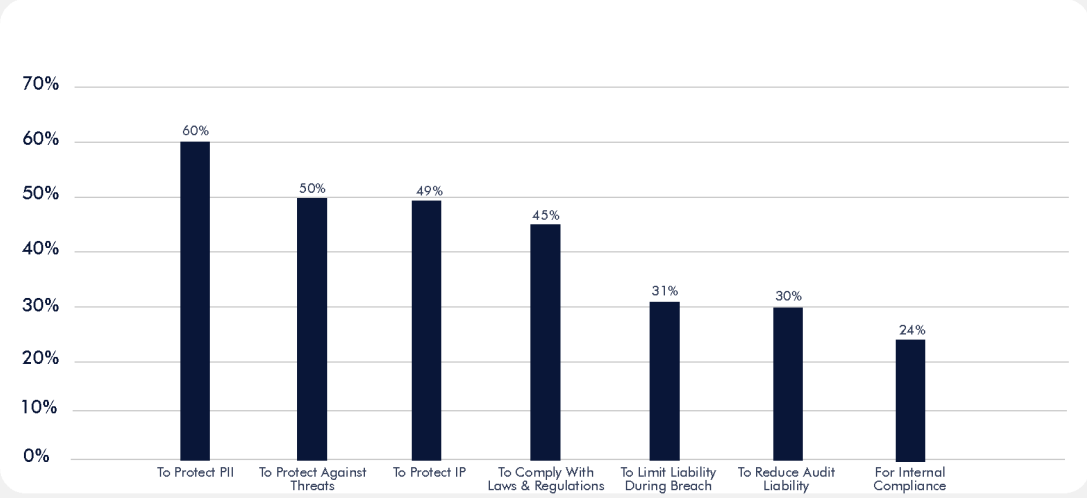
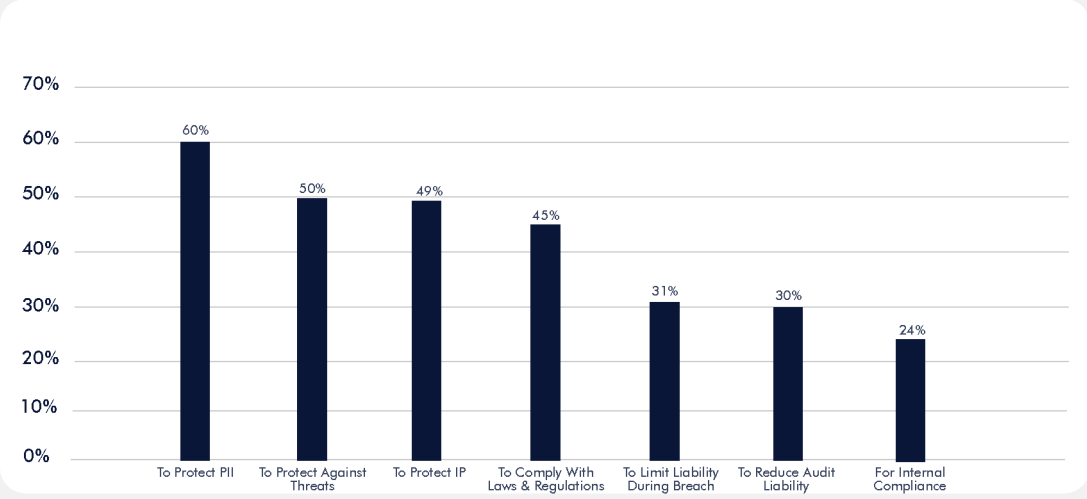


Figure 10. Entry Barriers For Planning Encryption Strategy



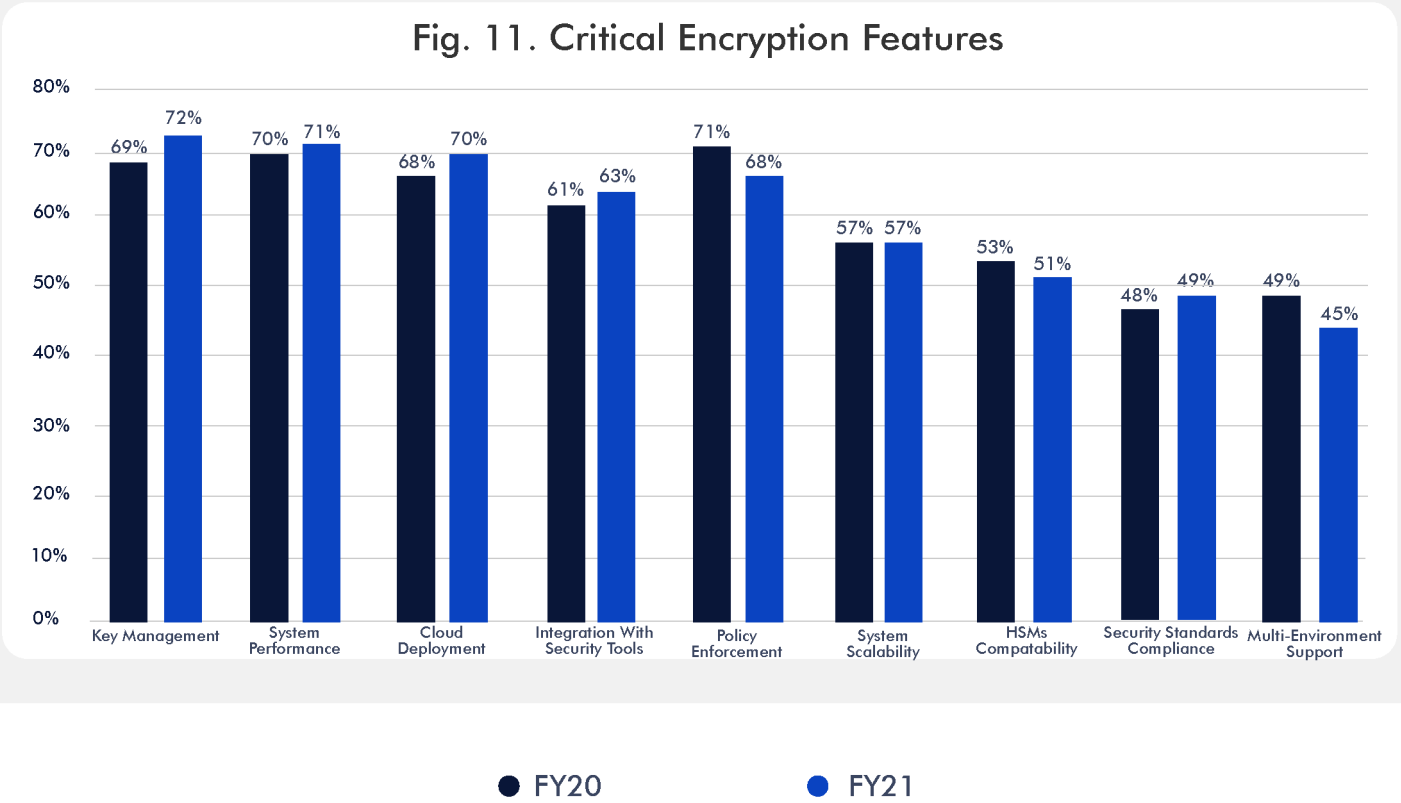
ENCRYPTION FEATURES AND DATA TYPES

We asked organizations participating in the survey to mark the level of criticality of nine encryption key features on a pointer scale. Figure 11 shows the responses for the nine features and how organizations prioritized each feature. Some of the encryption features are considered more critical and important when compared to others. These nine features are selected based on the popularity and importance in encryption technology for organizations across different industrial sectors and geographical locations as shown below.

As per the survey responses analysis we can deduce that the top three priority encryption features for maximum firms are Key management, System performance, and Policy enforcement. Preference given to performance finding is not surprising as the network latency is always a top priority factor for any organization. One of the most interesting finds from the survey is respondents considered "Key management (generation, storage, usage, deletion)" as most critical and also most painful to handle. Below figure 11 shows the comparison between responses from FY20 to FY21.

Figure 11. Critical Features In Encryption Technology Solutions

Fig. 11. Critical Encryption Features

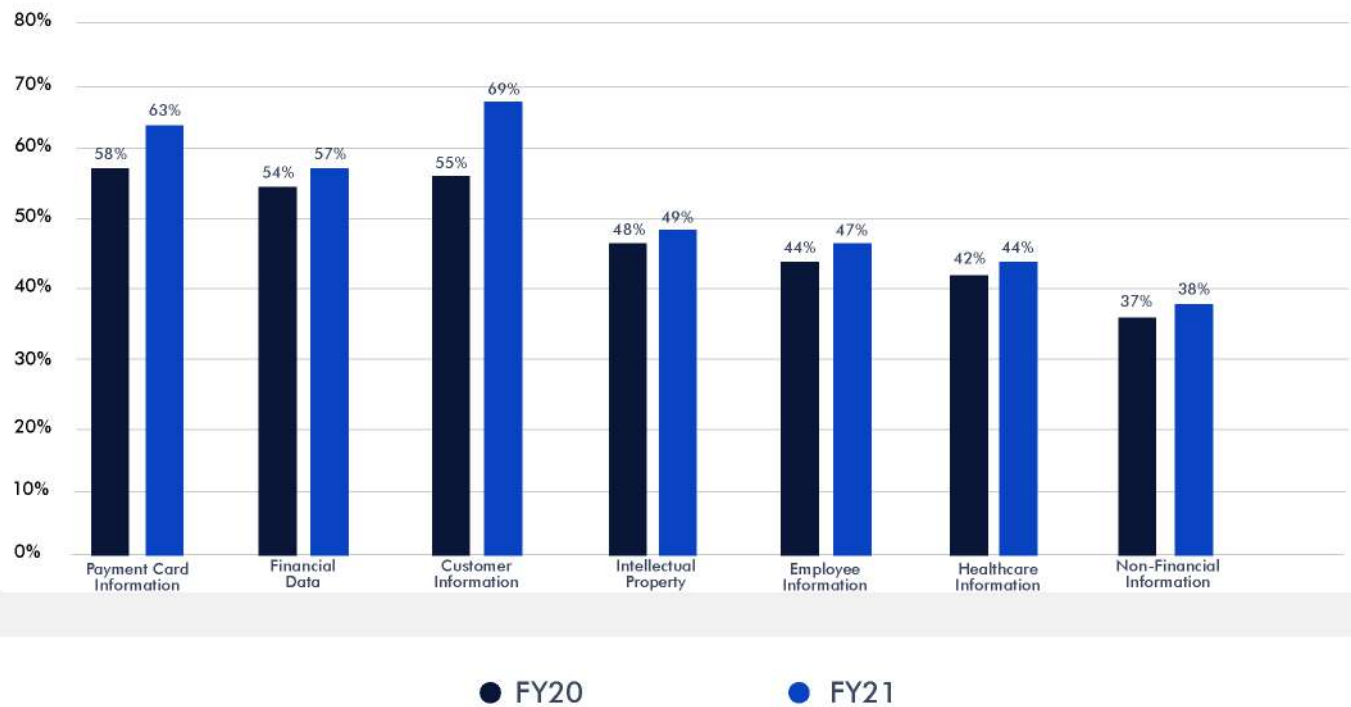


Most frequently encrypted data types: Organizations responded with the seven data types as shown in Figure 12 below and we asked them their preference. As it is clearly evident, payment card information and financial data are the top two priorities for the respondents. This shows the threat for financial data in the cyber world.

In spite of the sensitivity related to healthcare data, it is one of the least preferred data types for encryption among the respondents after non-financial information data type. Figure 12 represents a data comparison between FY20 and FY21.

Figure 12. Critical Features In Encryption Technology Solutions

Fig. 12. Critical Encryption Features



KUBERNETES SECURITY

Most companies are now planning to implement Kubernetes in cloud architecture. 59% of the organizations confirmed the use of Kubernetes in the near future. Figure 13 projects the various use cases for Kubernetes deployment and organizations priority percentage. Respondents are given a percentage scale to rate each Kubernetes deployment option.

We also asked respondents to provide insights about Kubernetes security and what are their major concerns. The analysis is projected in Figure 14. Three critical threats are identified - Pod Communication Failure, Technical Misconfiguration, Runtime Threats and respondents rated on scale of 0% to 100% based on criticality they feel in their work landscape.

Figure 13. Primary Use Cases For Kubernetes

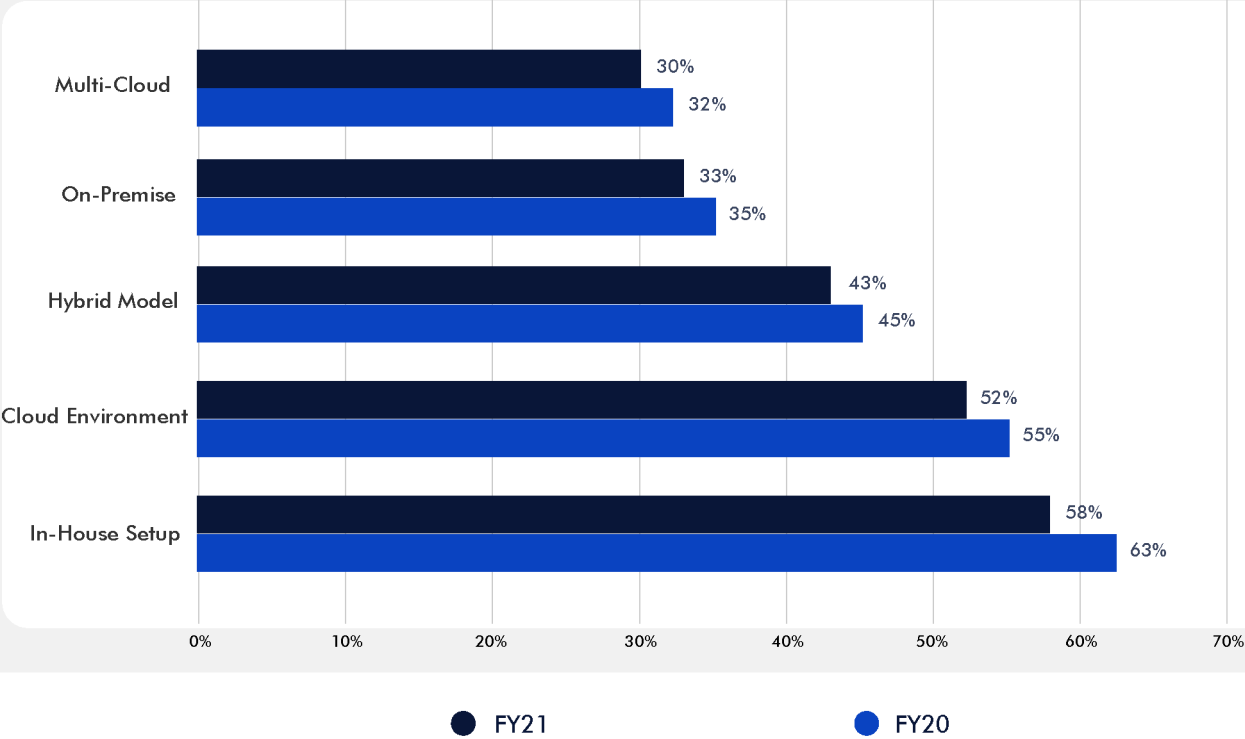
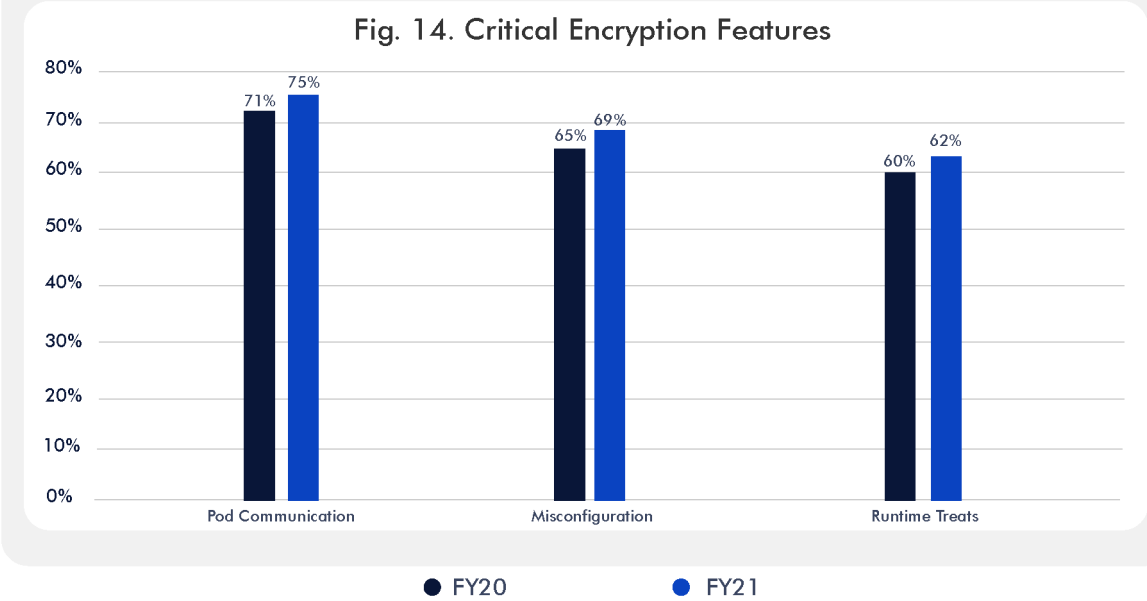


Figure 14. Critical Features In Encryption Technology Solutions



KEY MANAGEMENT ANALYSIS

Key Management is considered one of the most important, as well as the most painful and challenging, encryption technologies to handle by the majority of respondents. During the survey, we asked respondents to rate the "Challenging" nature of Key management on a scale of 0% to 100% and the results are shown in Figure 15 below where we provided the mean average of responses.

Figure 16 shows the organizations tending towards expert consulting/firms for handling Key management (Create, Manage, Destroy). This is mainly because of the heavy technical expertise requirement for managing keys and targeted ownership.

Figure 15. **Mean Average Rating On The Challenges Faced For Key Management**

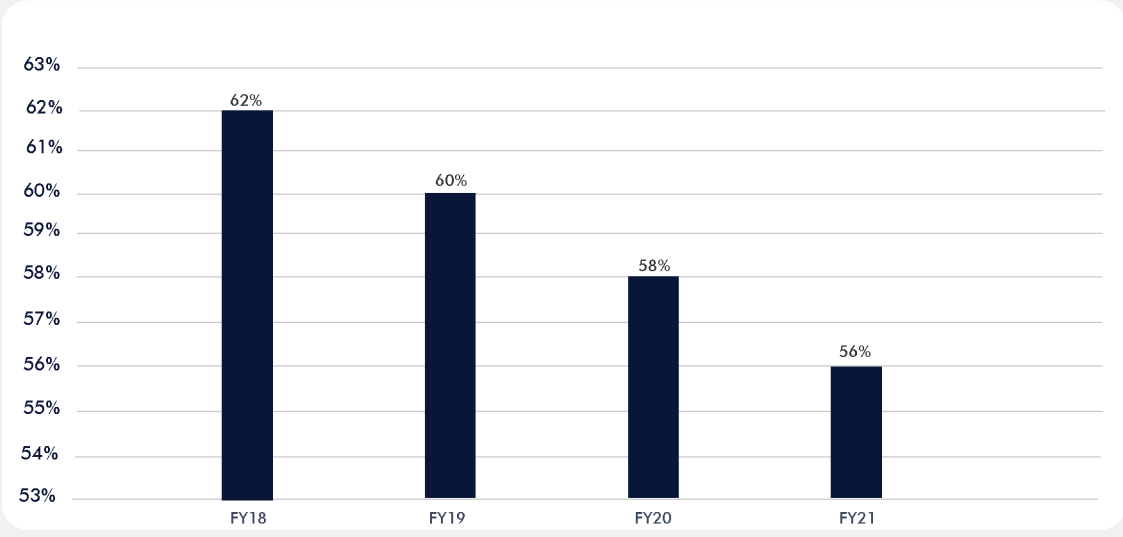
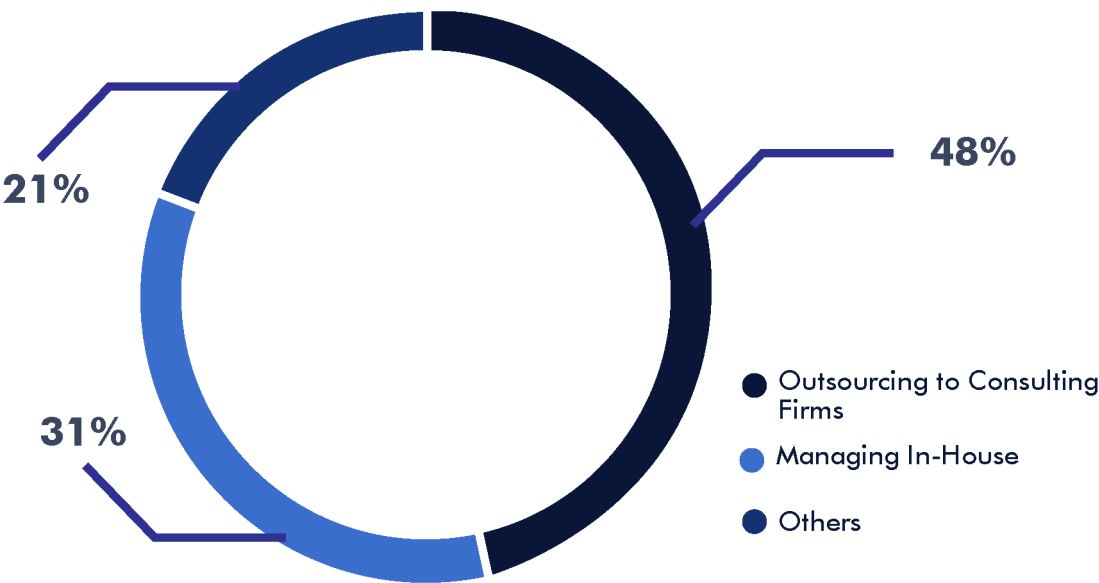


Figure 16. **Organizations inclining towards consulting/firms for technical expertise**



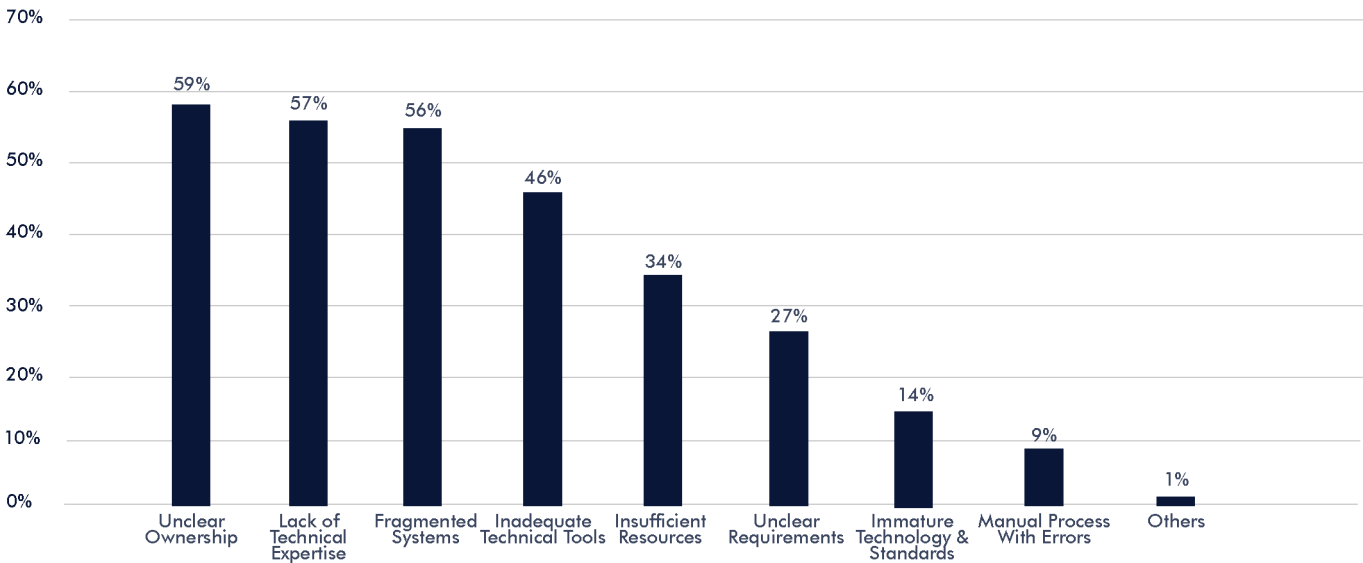
Major challenges of Key management
When asked to explain why key management tends to be so challenging, respondents gave various answers. The largest group (59 percent) said unclear ownership made key management difficult. That was the same proportion of respondents who labelled assets for external cloud or hosted services as the most difficult keys to manage.

Major challenges of Key management
When asked to explain why key management tends to be so challenging, respondents gave various answers. The largest group (59 percent) said unclear ownership made key

management difficult. That was the same proportion of respondents who labelled assets for external cloud or hosted services as the most difficult keys to manage.

Survey participants gave other reasons for their pain, too. More than half attributed the difficulty to skilled personnel and isolated and/or fragmented systems at 57 percent and 56 percent, respectively. At the same time, 46 percent said inadequate tools were to blame. 34 percent said unclear requirements were to blame. 27 percent said immature technology & standards were to blame. 14 percent said manual process with errors were to blame. 9 percent said others were to blame. 1 percent said others were to blame.

Figure 17. Major Challenges In Key Management



The top three reasons why key management is painful :

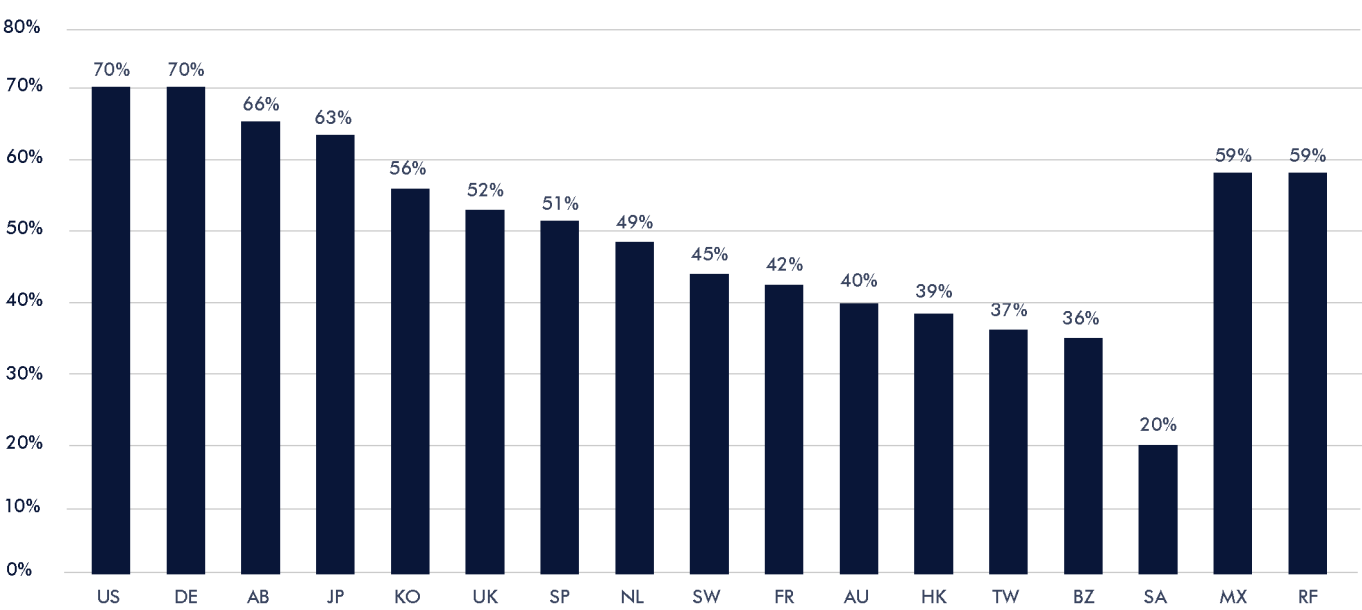
- 1. Unclear ownership of the key management function
- 2. Lack of technical expertise and skilled resources
- 3. Isolated or fragmented key management systems

ANALYSIS ON HARDWARE SECURITY MODULES

Hardware Security Modules (HSMs) are playing a crucial role in today's organization Cyber Security landscape. The global deployment rate of these devices has risen from 43% in 2018 to 52% in 2021 according to our research performed on hetero demographic respondents. With technology's ever-changing environment, organizations must keep up to be successful. These changes can lead an organization down two paths. One may lead to growth and prosperity, but the other may lead to destruction and despair. Figure 18 projects a clear picture about the deployment projections as per the respondents from the survey.

HSM deployment rate varied from country to country. In the near future, United States, German, Middle Eastern, and Japanese organizations are more likely to deploy HSMs with an average response as "Yes" by sixty seven percent of respondents. 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 forty nine percent. HSMs are tamper resistant hardware devices used prominently in key management. This trend shows few countries which are willing to go the extra mile to protect customers' sensitive information by preserving keys in hardware security modules.

Figure 18. Major Challenges In Key Management



*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 has increased steadily, as Figure 19 shows a four year trend for HSMs. As can be seen, the rate of HSM deployment has constantly increased across the globe.

HSM primary usage is key management for cloud based applications. We asked organizations about the operation of HSMs with cloud applications, and their responses are shown in Figure 20.

As shown in Figure 20, 53 percent of respondents own and operate HSMs on-premise for cloud-based applications, and 47 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. There is a significant increase in respondents who would like to handle the ownership and operation of HSMs on-premise and the integration with a Cloud Access Security Broker to manage keys and cryptographic operations for data-in-motion encryption.

Figure 19. HSM deployment rates over four years consolidated across countries

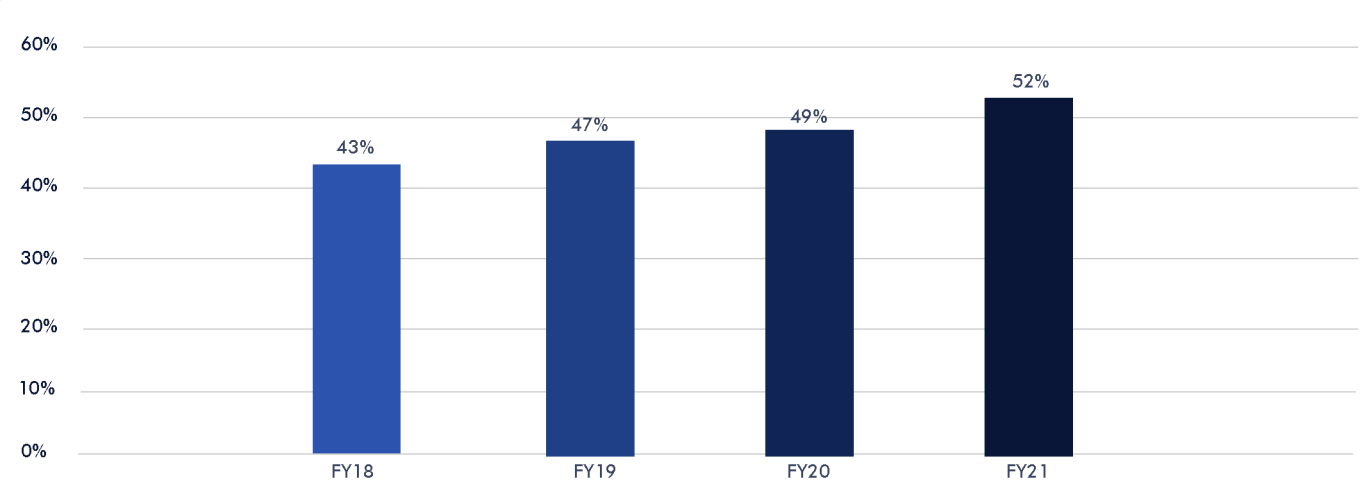
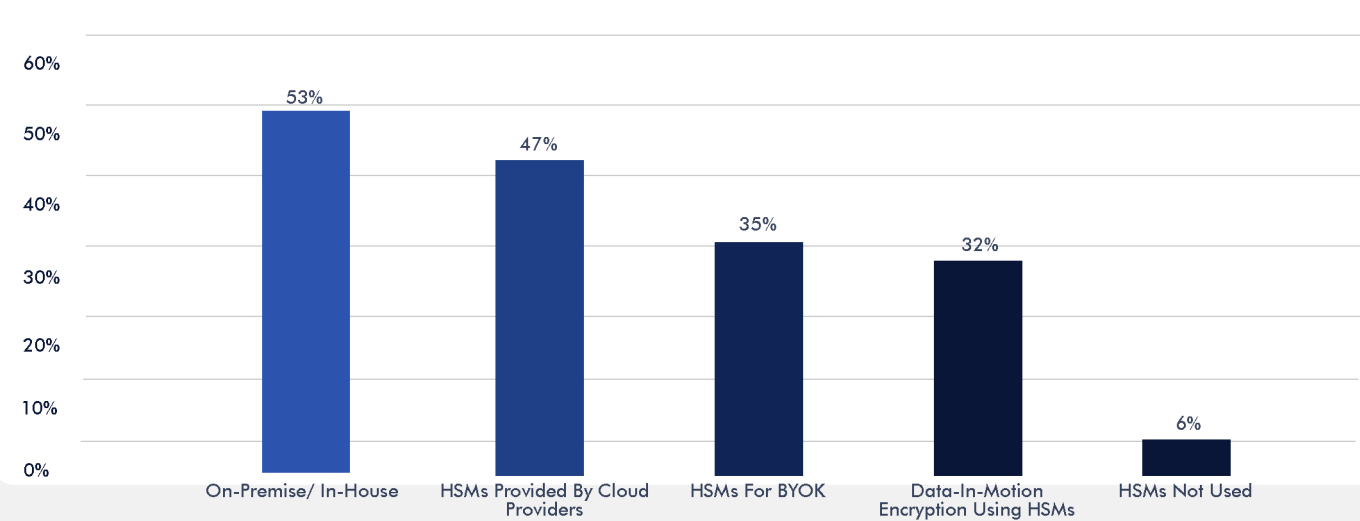


Figure 20. HSM Usage Trend With Cloud Applications



A similar study conducted by the Ponemon Institute revealed the following analysis on HSMs: 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

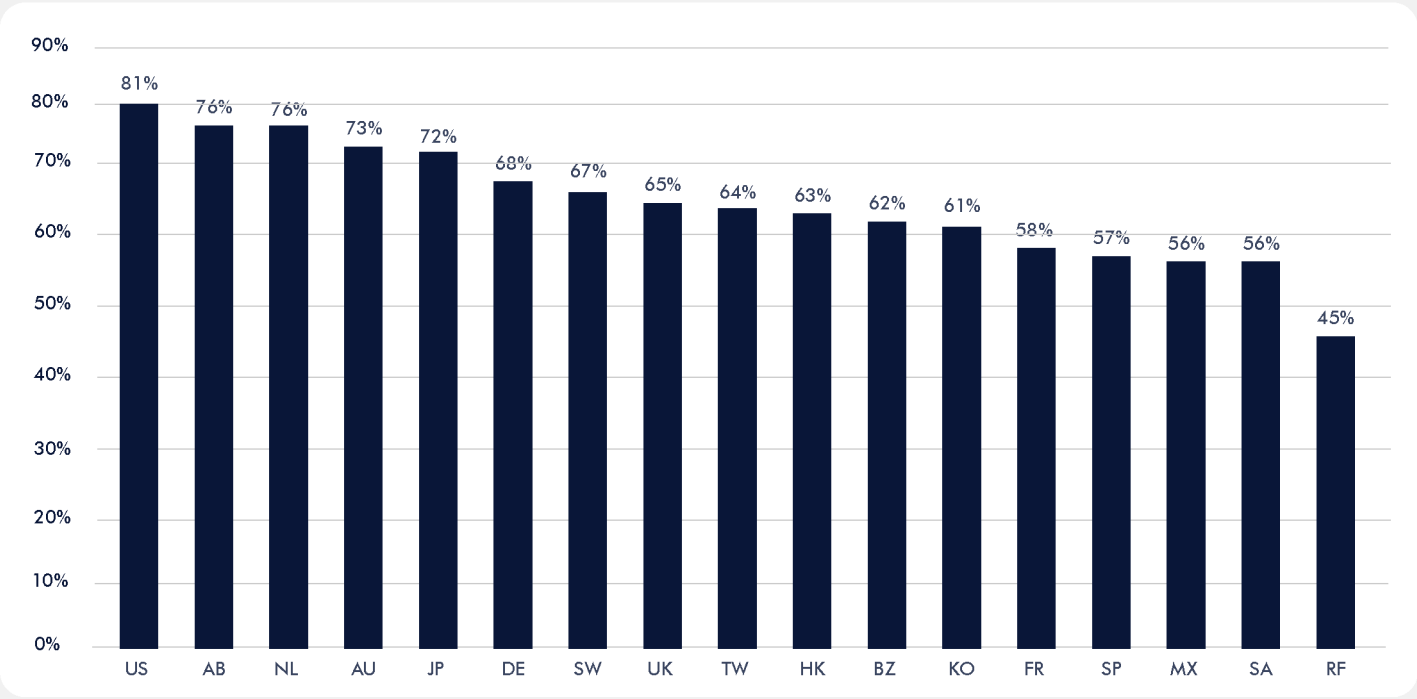


Figure 22. Perceived Importance Of HSMs As Part Of Encryption Or Key Management Over Nine Years

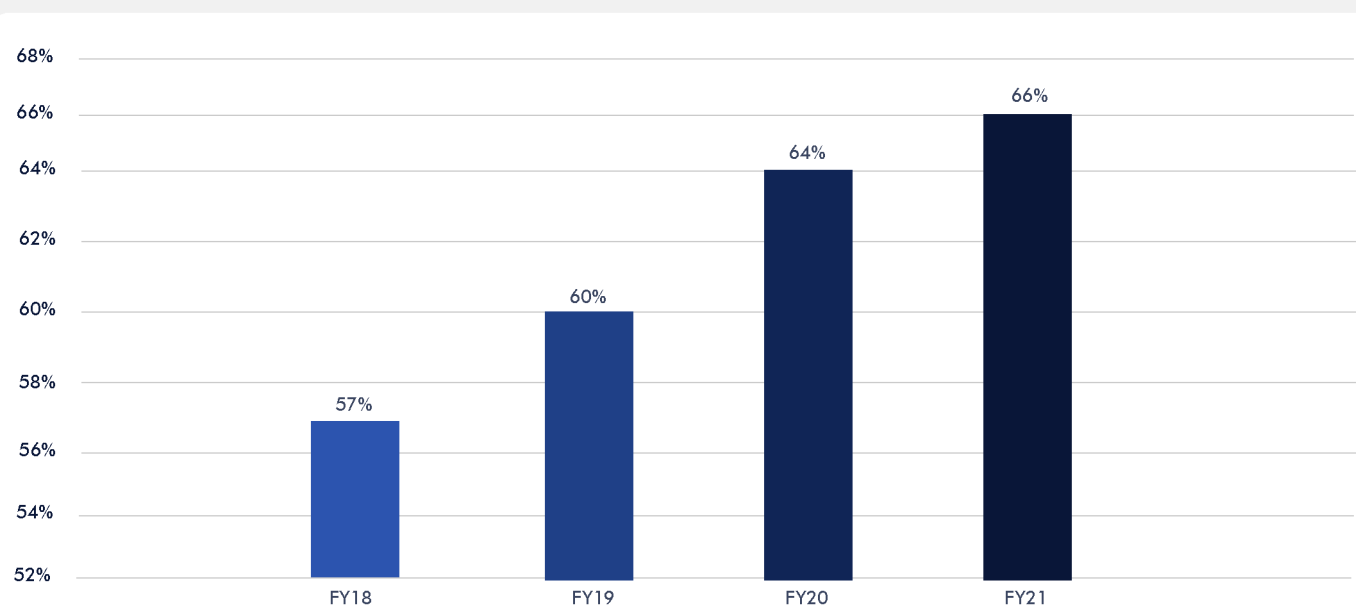
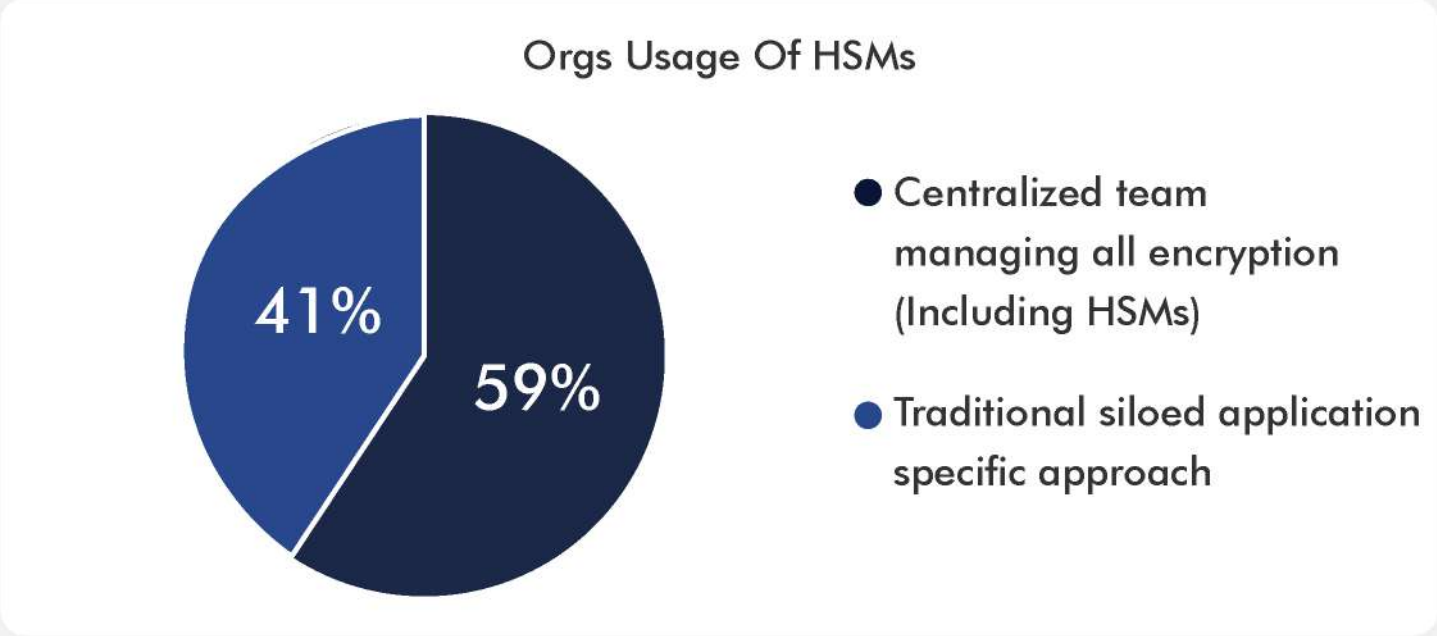


Figure 23 shows the HSMs usage, 59 percent of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/ teams within their organization (i.e., private cloud

model). 41% responded that each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional individual application-specific approach.

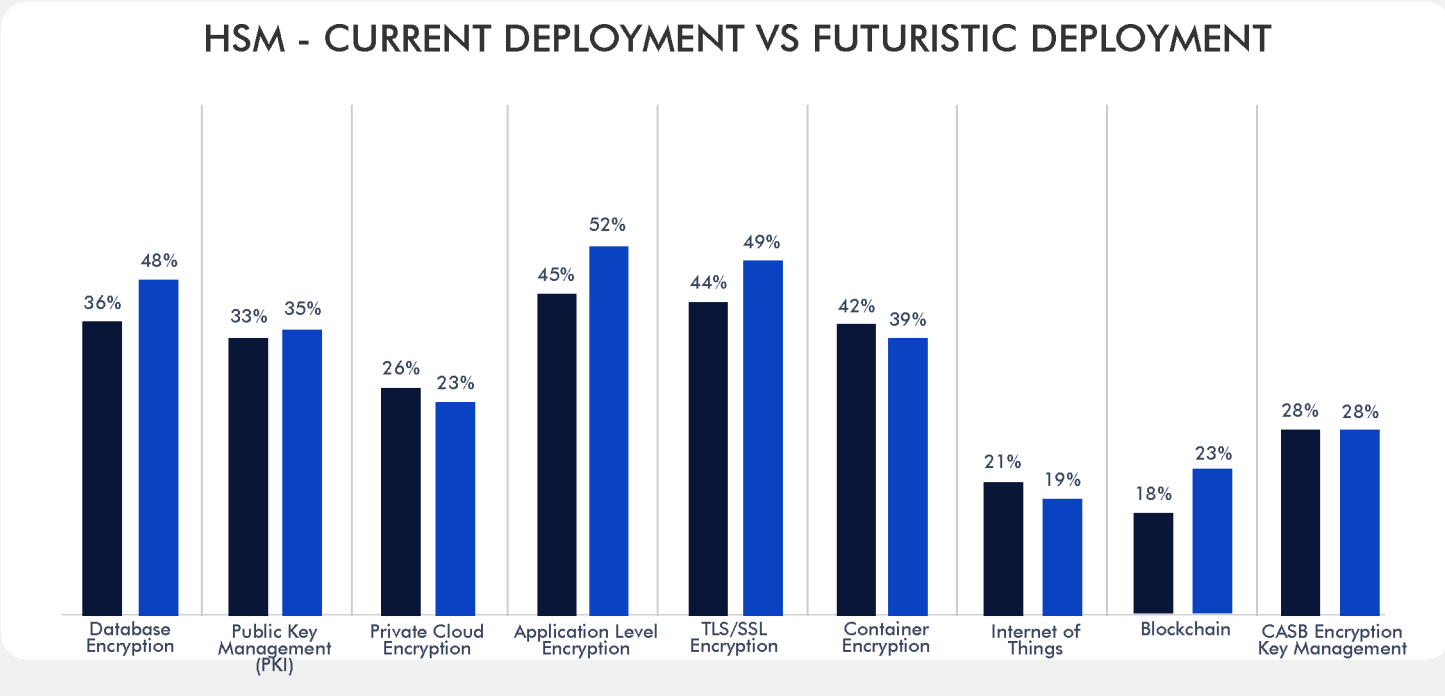
Figure 23. **Organizational Usage Of Hardware & Security Modules**



Important use cases of HSMs by various organizations are summarized in Figure 24. We surveyed the primary purpose or use cases for deploying HSMs currently versus future use. As can be seen, the top choices are database encryption, 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 which is a good indication for increasing trend of performing data-at-rest encryption. 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.

One of the significant observations from the survey outcome is the preference to increase the usage of HSMs for blockchain technology based applications and decrease in usage for Internet of Things (IoT). Increasing importance for blockchain technology can be attributed to many trending and budding factors such as decentralization and crypto currency invasion. It will be interesting to see how these new upcoming technologies impact encryption.

Figure 24. HSMs - Current Deployment vs Future Deployment



● Now ● Next

CLOUD ENCRYPTION

According to Figure 25, 50 percent of respondents say that more than 40% of their organization's data is on cloud. Another 44 percent of respondents confirmed that 60% of sensitive data is on cloud. Interesting fact is that only 17% reported that more than 50% of their data on cloud is encrypted. Organizations has to encrypt sensitive data on cloud. This shows

that the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

According to Figure 26, data types of sensitive data stored on cloud by various organizations. Financial records, Employee records and business data is the top three data types that is stored on cloud and as expected national security data is the least preferred.

Figure 25. Analysis On Data Stored On Cloud By The Respondents

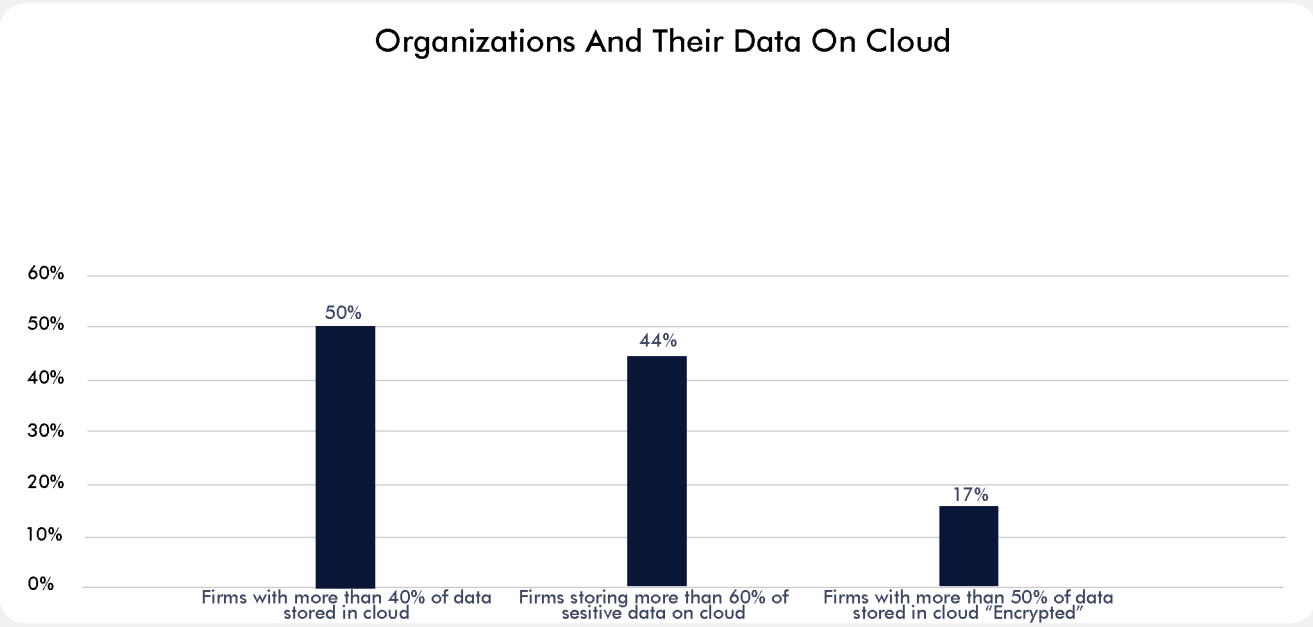
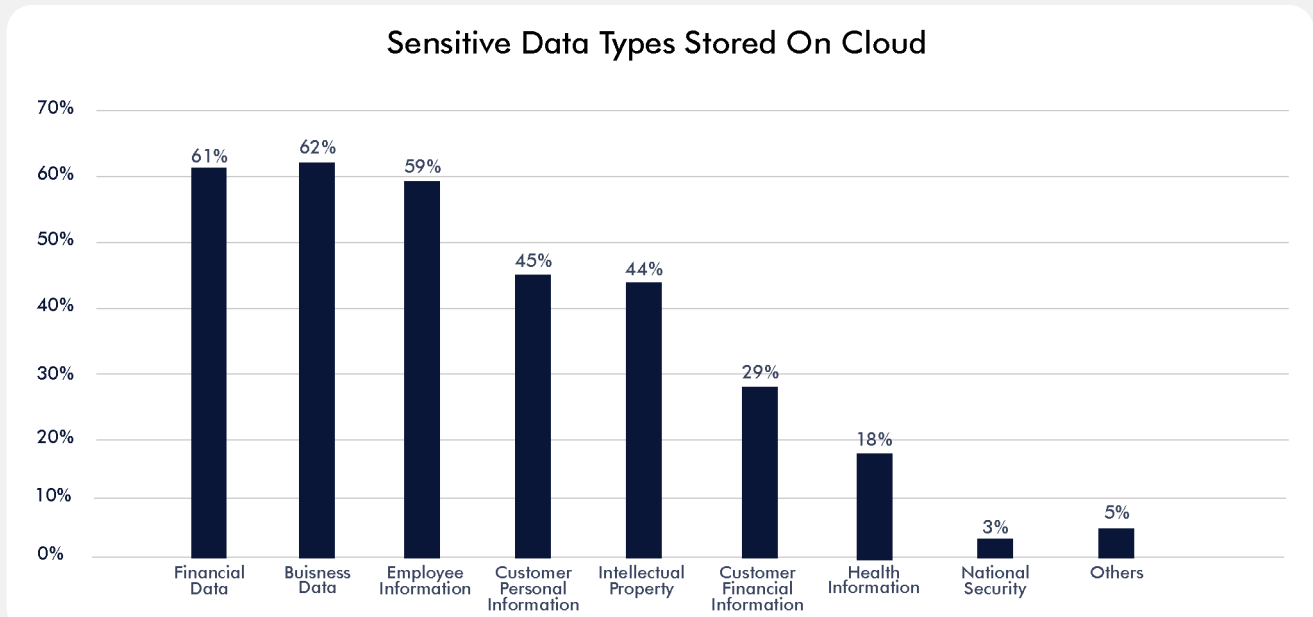


Figure 26. Analysis On Sensitive Data Types Stored On Cloud



We have more analysis from you from a different survey on cloud encryption by Entrust & Ponemon: 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

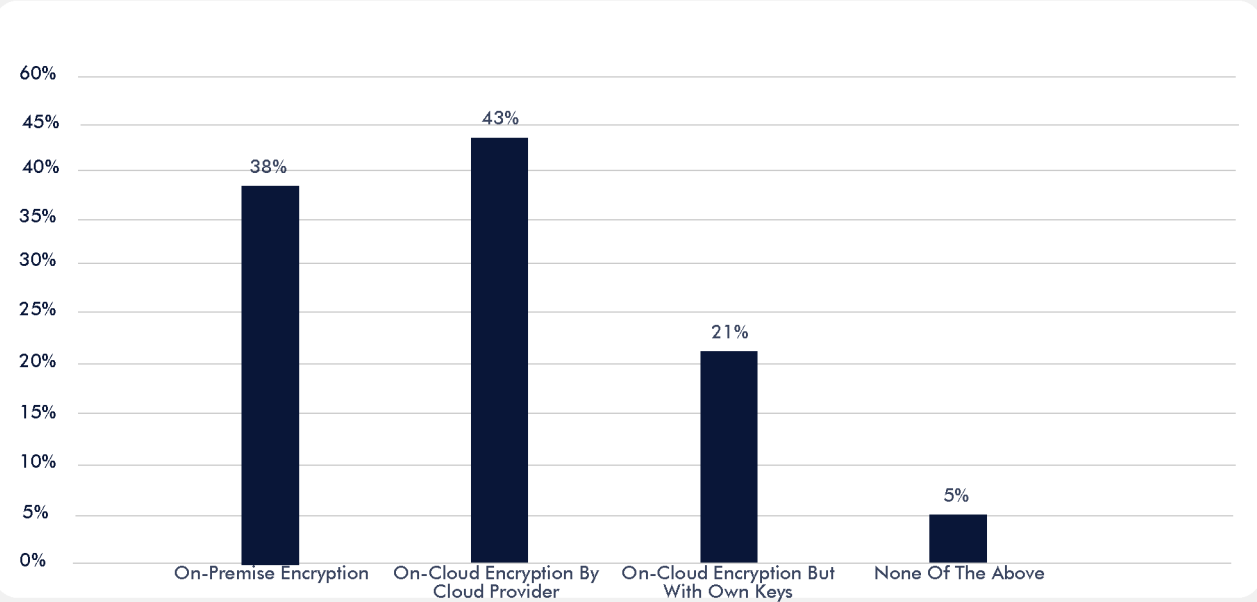
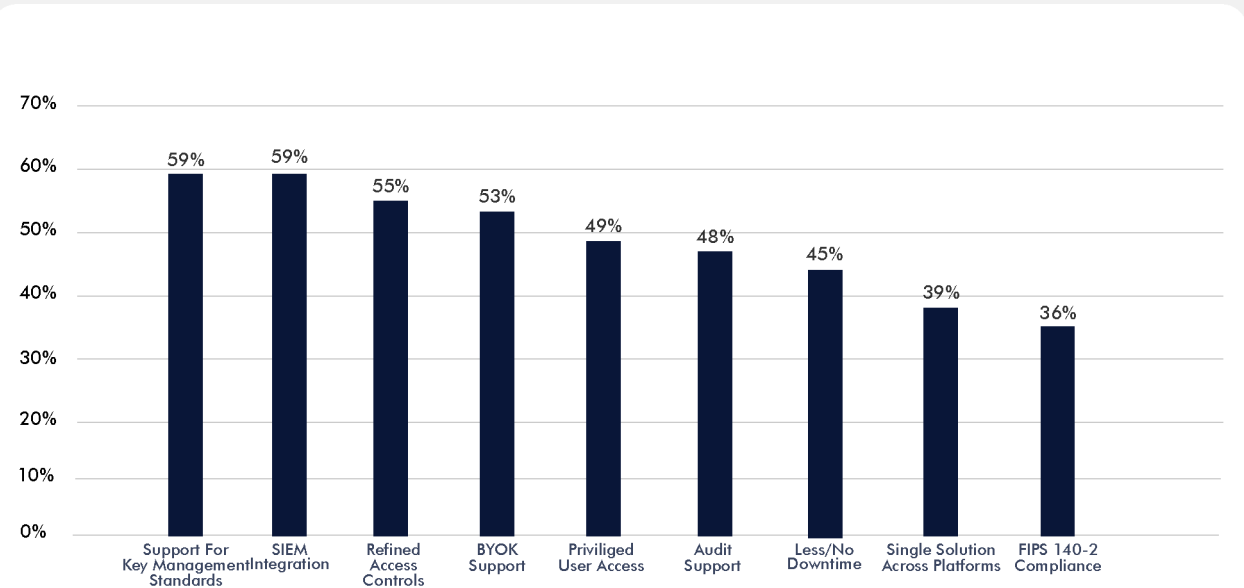


Figure 28. Critical Associated With Cloud Encryption





The image shows two women in a professional office setting. One woman, with short grey hair and glasses, is looking at a laptop screen. The other woman, with dark hair, is partially visible in the foreground, looking towards the same screen. The laptop displays a complex financial dashboard with various charts and graphs. A large dark blue circular overlay is positioned in the bottom left corner, containing the text 'About Encryption Consulting'.

About Encryption Consulting

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and integrating our solutions with their products and services. We also pride ourselves on our flexibility and are always open to help our clients achieve their data security success with the technology of their choice. If you have products and services already deployed or are considering, we'd be glad to help you evaluate these to get the most out of your investment.

CIPHER

nCipher Security, a leader in the general purpose hardware security module market, is now an Entrust Datacard company, delivering trust, integrity and control to business critical information and applications.

THALES

Thales-e-Security is a leader in encryption, advanced key management, tokenization, privileged user control and meets the highest standards of certification for high assurance solutions.

Fortanix

Fortanix is a leader in runtime encryption and it protects applications even when the infrastructure is compromised.

KEYFACTOR

Keyfactor has its roots in the trenches of IT security, deployment and operations. We understand how companies work because of our deep industry experience—we know firsthand the challenges of competing agendas, budget constraints and time pressures.

Microsoft

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington.

MICRO FOCUS

Micro Focus and HPE Software have joined to become one of the largest pure-play software companies in the world.

CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile.

gemalto security to be free

For those shaping the digital interactions of tomorrow, we provide the digital security that enables the trusted connections of today.

FORNETIX

Fornetix Key Orchestration TM is a scalable and flexible solution designed to simplify key management. Granular policy tools, user access controls, and powerful automation enable organizations to manage hundreds of millions of encryption keys while integrating seamlessly with existing technology investments.

appviewX

AppViewX is revolutionizing the manner in which NetOps and SecOps team.

PrimeKey

PrimeKey's technology is used by organizations and enterprises to securely implement PKI solutions used for ePassports, eBanking, ePayment, mobile/Internet security, IoT and more.

UNBOUND (MATH OVER MATTER)

Unbound protects secrets such as cryptographic keys, credentials or private data by ensuring they never exist in complete form

PrimeFactors™ — APPLIED DATA PROTECTION —

Prime Factors software products help business leaders implement and manage enterprise-wide data protection policies to secure sensitive information being used by or stored in virtually any application or system.

utimaco®

Utimaco is a leading manufacturer of Hardware Security Modules (HSMs) that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector.

protegrity

The Only Data-First Security Solution. Protect sensitive enterprise data at rest, in motion, and in use with Protegrity's best-in-class data discovery, de-identification and governance capabilities.

VENAFI

Venafi Cloud helps organizations prevent outages and secure their keys and certificates

comforte

Secure your data, minimise risk, and meet compliance and regulation requirements. Find out more about comforte's Data Security Services.

ENCRYPTION CONSULTING www.encryptionconsulting.com

Why Encryption Consulting LLC?



Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.



Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure



Hardware Security Module – HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.



Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases



Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?



Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us

