ENCRYPTION CONSULTING

Encryption Consulting Study On Global Encryption Trends - 2023

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

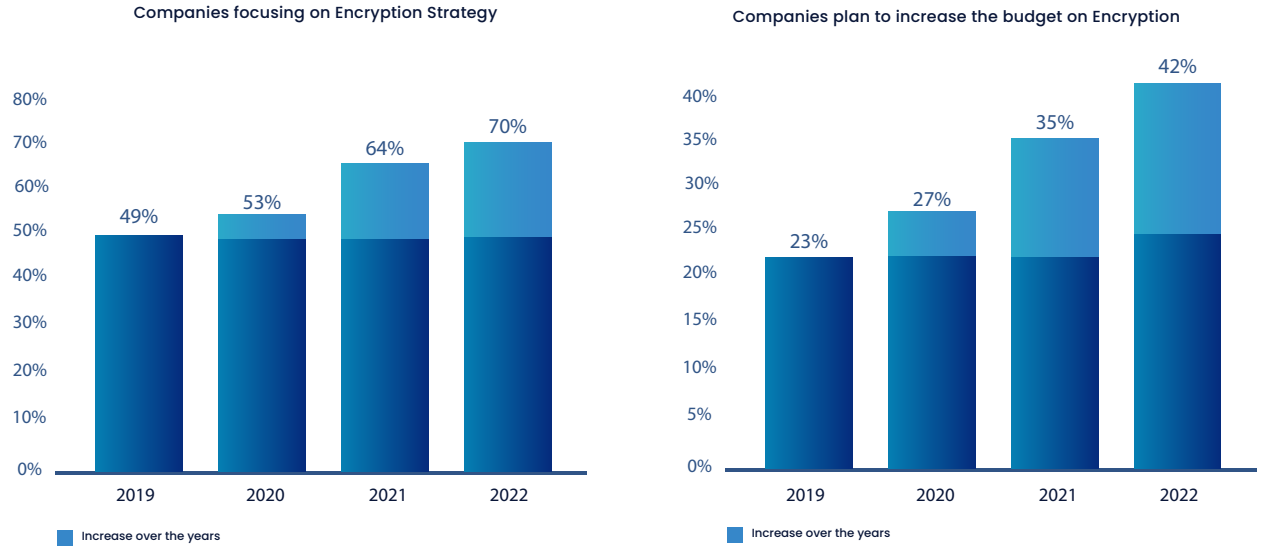
Contents

Encryption Consulting Findings From The Global Trends Study 2023

Encryption Consulting performed a survey on encryption global trends with around 4,125 experts across multiple industry sectors in various countries which include the 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 and evolved into a critical aspect in the security posture of firms across various sectors and industries. The Encryption Consulting survey considered the nature of firms under different jurisdictions and geographies to better understand their encryption trends.

Figure 1 below shows the outcome of the high level survey 2023 conducted on Encryption strategy by the respondents. As you can see, there is a big jump in the firms focusing on encryption strategy from FY21 & FY22. This can be attributed to the increased cyber threats and awareness post pandemic era. Also, many of the respondents are planning to increase their budget spending on Encryption implementation across domains for protecting their sensitive data. About 42% are confident on increasing the budget spending on Encryption in FY22-23. Following are the findings from the research performed about encryption strategy:

Fig. 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

Encryption Consulting survey on the Global trends in Encryption 2023 provided many insights into the leading organizations' strategies and stances on encryption across the globe. This year's survey projected better awareness in the firms on encryption and their plan to adopt encryption as a core data protection technology. An interesting find is the increasing focus on the migration of sensitive data onto the cloud. Also, there are a considerable amount of respondents willing to increase their budget spending on Encryption implementation. This spending includes data protection assessments, encryption implementation, and future trends as well.

70%

of the responding organizations are having Encryption strategy as the primary focus and it is a 17% increase when compared to the trend from FY20.

From our previous studies, we identified that 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 adoption is 50 percent.

50%

Global Average of Adoption

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

Future Encryption Trends

Organizations are prioritizing to cloud more than ever in FY22. This trend has been identified from our previous survey of 2022. Along with the cloud, several organizations that participated in the survey are focusing on the upcoming and futuristic trends in encryption such as Homomorphic Encryption, BYOE, Blockchain encryption. This can be attributed to the increasing prominence of data with the advent of Web3, Crypto and Metaverse. Detailed results from the survey can be observed in the following sections of the report.

Companies Preferred Deployment Options

There is no major inclination toward 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 anyone particular deployment option, but are focused on implementing encryption holistically across the organization.

Key Drivers For Encryption

Protection of the customer's PII still stands as a top key driver for implementing encryption for about 64% of the respondents for implementing encryption. This can be attributed to the reputational damage of the firm if they lose PII to a breach. Next on the list is the protection of IP which was opted by 53% of the respondents. About 52% of the respondents mentioned that compliance with the local laws and regulations is the key driver as any violation can cause severe financial damage through penalty. Compliance is one of the key business drivers for the 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 are 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 64% of the respondents for implementing encryption. About 53% 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 overcome these barriers and implement encryption across the crown jewel business functions.

65%

of the total respondents mentioned that protecting customer personal information is their top priority.

Top Priority Encryption Features And Data Types

Encryption Consulting identified nine critical encryption features to mark the level of criticality. 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 and 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 healthcare 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 47% in 2019 to 57% in 2022 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.

64%

respondents mentioned that "Data Discovery" is the major barrier for encryption adoption.

HSMs Usage By Organizations:

Companies have various ways of usage when it comes to HSMs. The majority of the respondents – about 63%- mentioned that they use cryptography- as-a-service, including HSMs, for their internal business functions and units leveraging the private cloud model.

Around 37% 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. **68% of respondents say their organizations are leveraging cloud platforms (public and/ or private) for storing & processing of their sensitive data**. Out of these respondents, 58% are already implementing one or more encryption technologies to protect the sensitive data stored in the cloud. 44% 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: 61% 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, followed by technical expertise in ensuring the encryption strategy transformed into implementation (45% of the respondents) and finally, 26% of respondents are feeling performance and integration issues as a major concern.

47%

of the firms store >60% of their sensitive data in Cloud platforms and protect it using encryption.

Deep Dive Analysis

This section focuses on the key findings and deep dive analysis from the “Survey 2023”

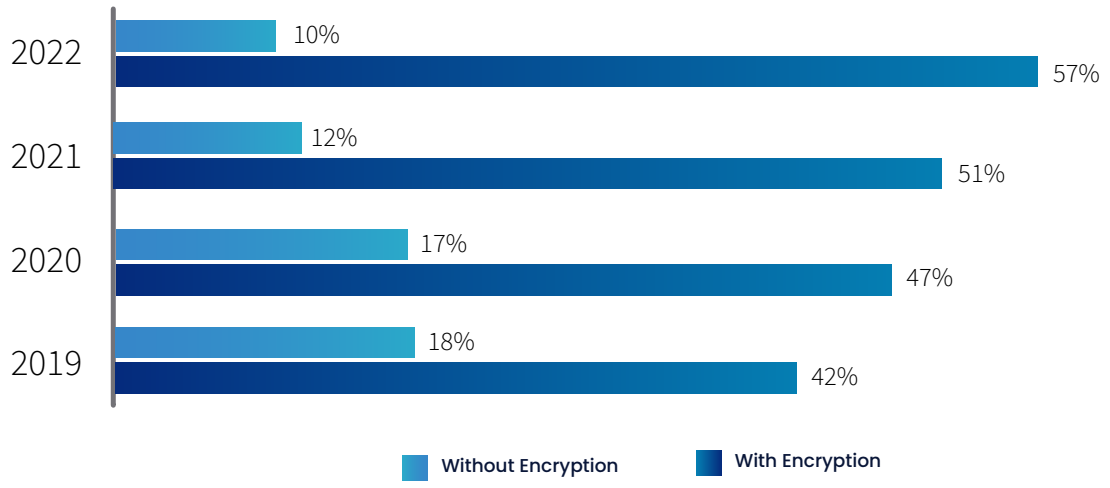
Key Focus Points

- 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
- **Future Focus: Homomorphic 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.

Fig. 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.

As per the survey report, the United States claimed the highest adoption of encryption dethroning Germany last year. However, Germany is just 0.5% behind the United States, and Japan stand as the leader in the Asian region with 66% adoption rate. 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 adoption is about 52 percent.

According to Figure 4, even this year 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. IT security percentage increased from 21% in FY21 to 23% in FY22 in shaping the encryption strategy for the respondents. This trend is seen across the demographics.

Fig. 3 - Encryption Adoption Across The Globe

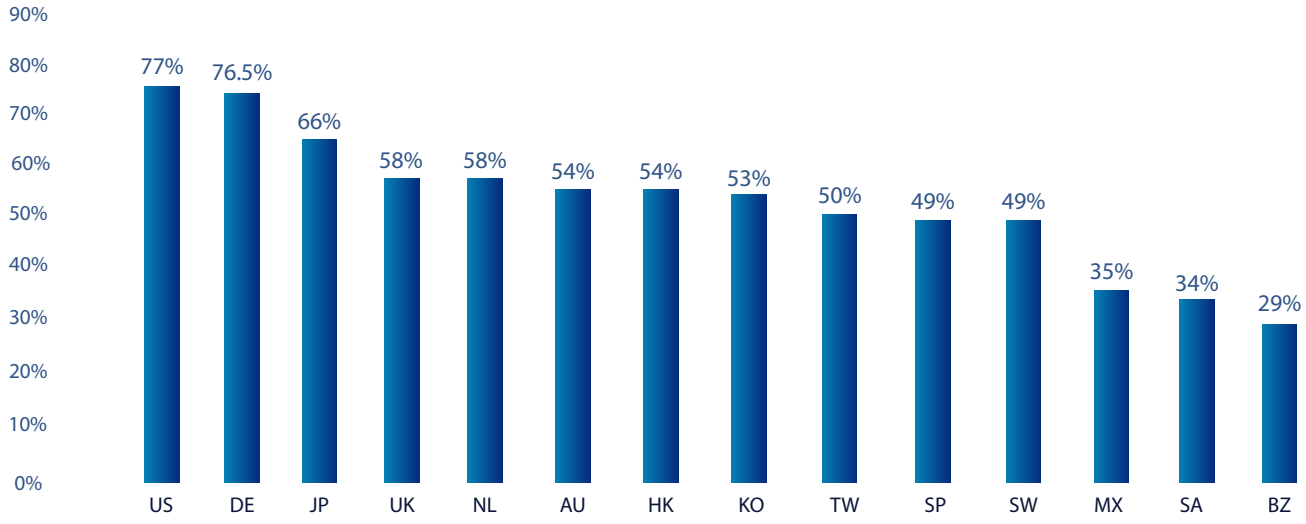
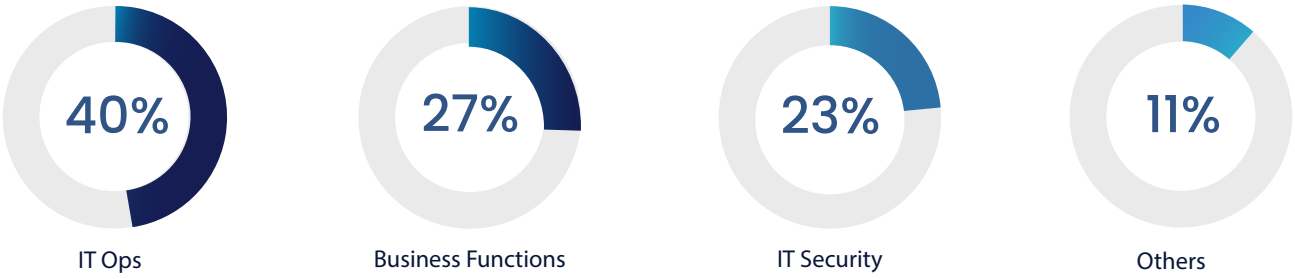


Figure 4 - Factors influencing Encryption Strategy



Respondents opting for business function clearly still shows the impact of Encryption on performance which might impact business operations. Also, this might be implied to the growing adoption of the latest encryption trends. Proliferation of employee - owned devices across the organizations is another major reason for this trend.

Trend Analysis - Encryption Adoption

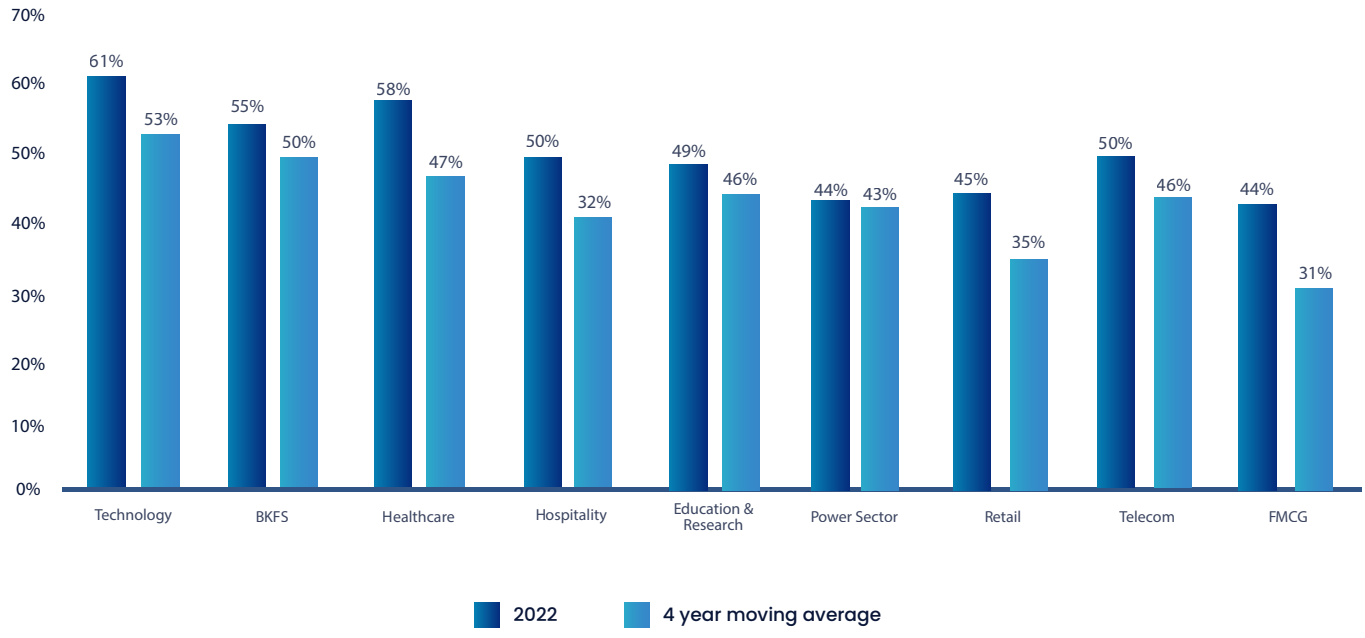
From the survey responses observed we can confidently say that there is an increasing adoption of encryption. Organizations across the globe are now prioritizing encryption for securing their sensitive data. Further, we surveyed on the sectors that are prioritizing encryption.

"Tech Sector"

is the pioneer in the Encryption Adoption for FY22

Figure 5 clearly shows the increase in the current year encryption adoption rate when compared with the last 4 years in various industrial sectors. Results suggest a steady increase in all industry sectors, with the exception of communication and service organizations. Technology sector is in the top and other sectors with significant increase in extensive encryption usage in BKFS, Healthcare.

Fig. 5 - Encryption Usage By Industry: 2022 Versus 4 Year Moving Average



Future Encryption Trends

Fig6. projects the responses from the survey regarding the focus on futuristic trends that are emerging in the encryption technology. There is five percent hike from previous year's figures which indicates companies are slowly focusing on the emerging trends to fight the unforeseen threats in the data protection landscape. Companies are hiring expert consulting firms to understand the trends and performing assessments to identify the requirement. As per our internal research primary trends In Encryption domain are "Bring Your Own Encryption (BYOE)", "Blockchain Technology", "Homomorphic Encryption" and "Quantum Crypto Agile Solutions". Organizations are focusing on these trends as well which is shown in Figure 7 with outcome.

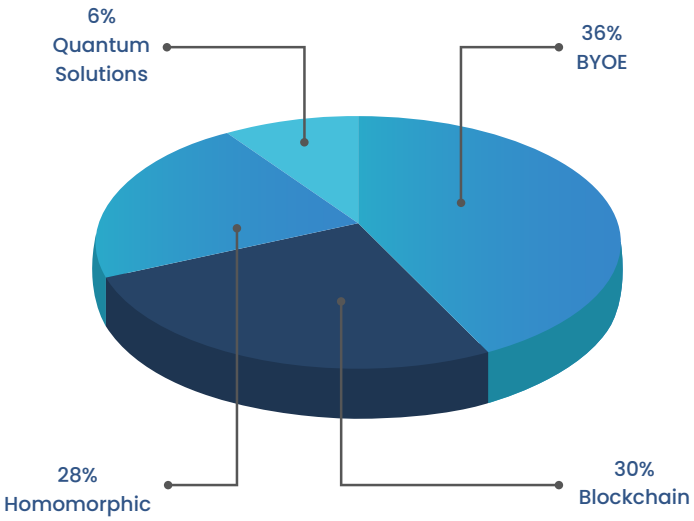
5% ↑ - FY22

Companies focusing on futuristic Encryption Trends

Figure 7, shows the focus areas of organizations regarding the futuristic encryption trends in FY22. Suprisingly, there is a decrease in the respondents focusing on BYOE and Blockchain Technologies when compared to FY21 and there is a good increase in focus on Homomorphic Encryption Technology in FY22. This might be attributed to the increasing focus on encryption data without keys. We can deduce that as the threat landscape is ever increasing companies are cautious enough to focus on the upcoming trends of encryption for customer data protection.

Fig. 6 - Organizations focusing on "Future Trends of Encryption"

Fig. 7 - Encryption Futuristic Technologies In Focus

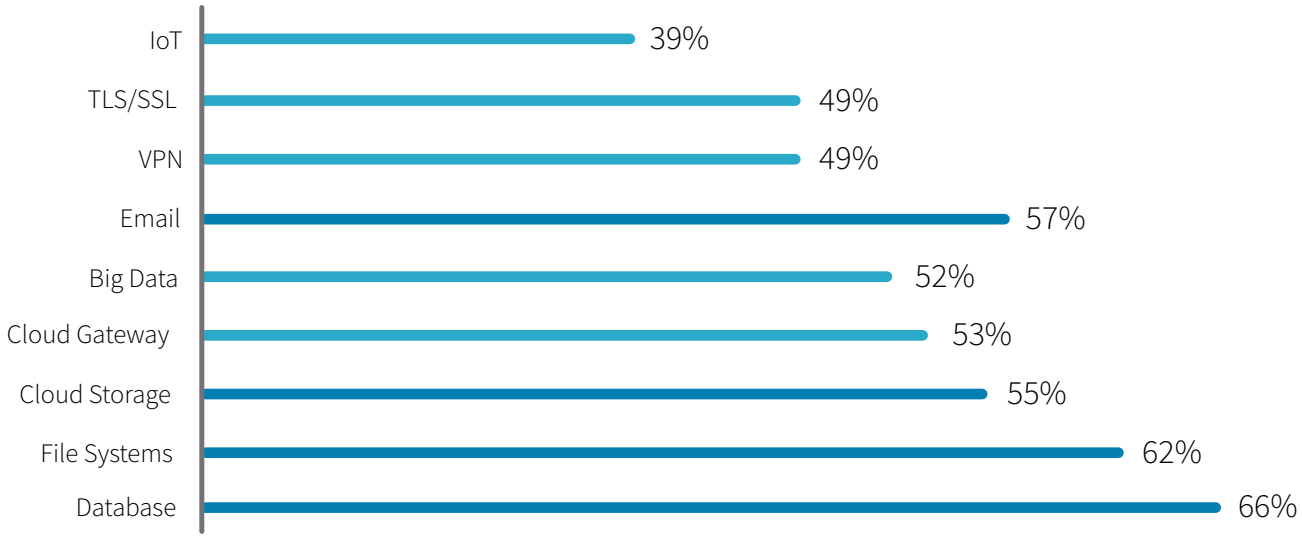


Deployment Options

There are several deployment options in Encryption. 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/Database encryption and Cloud encryption. Focus on IoT comes as a surprise as this is the emerging tech.

As shown in Figure 8, about 70% of respondents say encryption of IoT platforms has been partially deployed and 39% 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.

Fig. 8 - Holistic view on Encryption usage across domains FY22



Key Drivers for Encryption

Protection of the customer's PII still stands as a top key driver for implementing encryption for about 65% of the respondents. This can be attributed to the reputational damage of the firm if they lose PII to a breach. Next in the list is the protection of IP which was opted by 53% of the respondents. About 52% of the respondents mentioned that compliance with the local laws and regulations is the key driver as any violation can cause severe financial damage through penalty. Similar percentage of respondents mentioned that protection against the rising threats is a key driver for encryption adoption.

Barriers for Encryption

Data discovery is a key barrier identified during survey for about 64% of the respondents for implementing encryption. About 53% of the respondents mentioned that lack of technical skill for implementing and managing encryption is a barrier. About 45% felt that cost of in house implementation as a barrier. Along with these, data classification was seen as barrier. 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.

Fig. 9 - Key Drivers for encryption solution implementation FY22

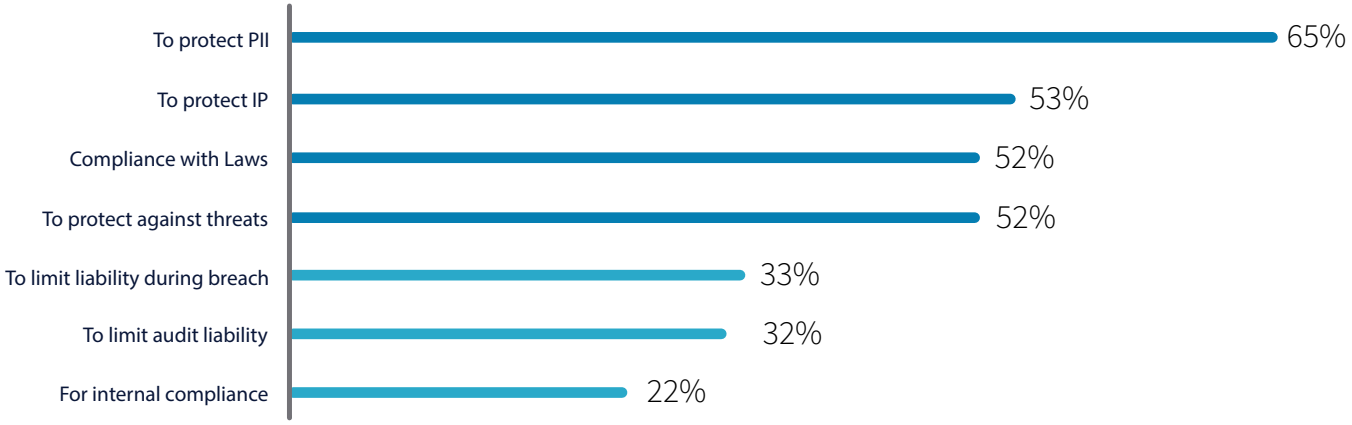
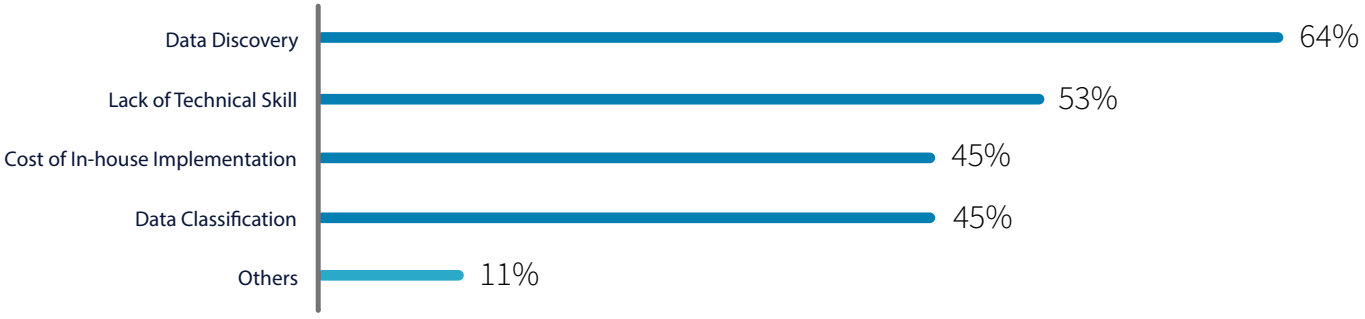


Fig. 10 - Entry barriers for planning encryption strategy FY22

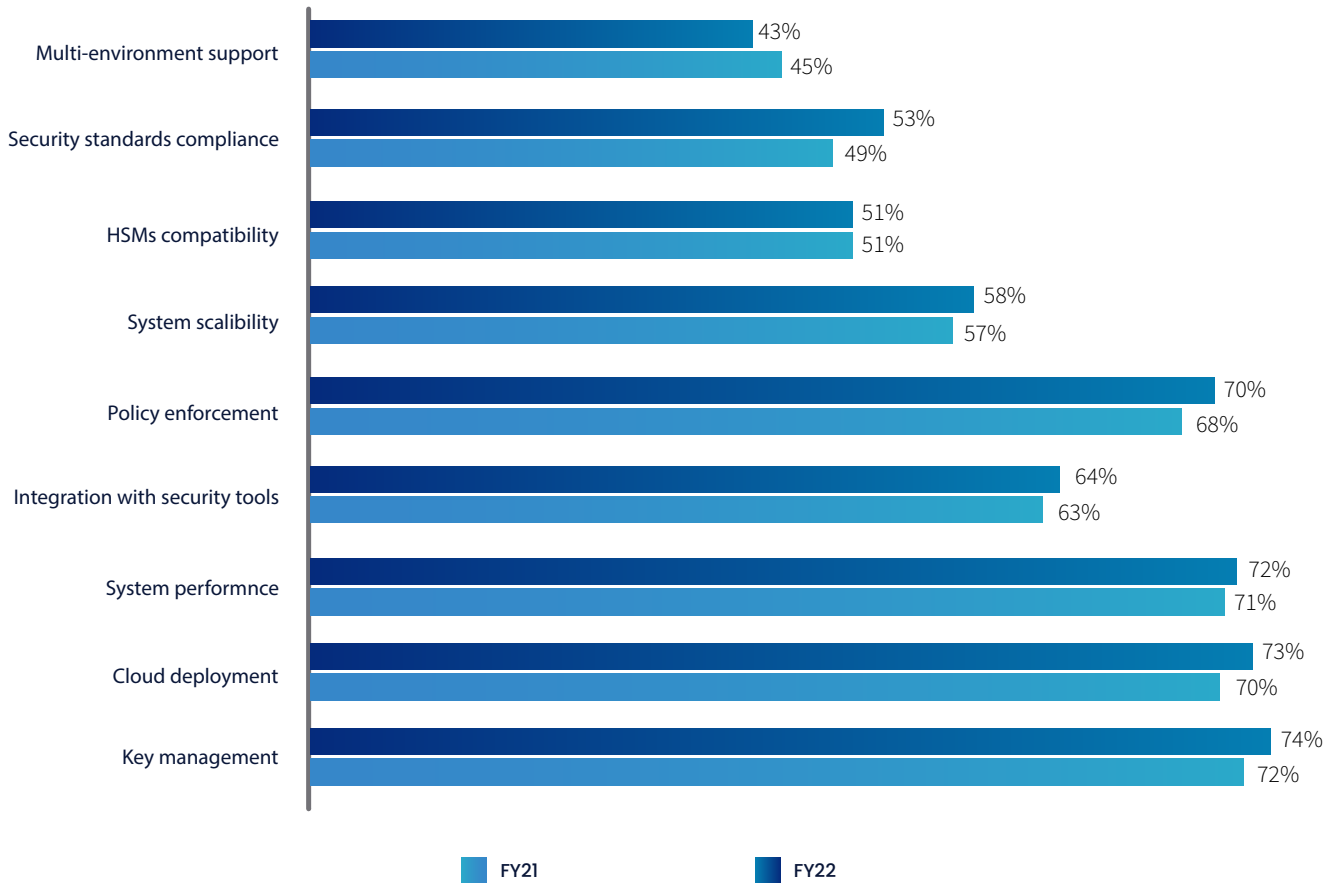


Encryption Features and Data Types

Encryption Consulting identified nine critical encryption features to mark the level of criticality. Fig 11 shows the response on how the organizations prioritize these identified features. 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 FY21 to FY22.

Fig. 11 - Critical features in encryption technology solutions

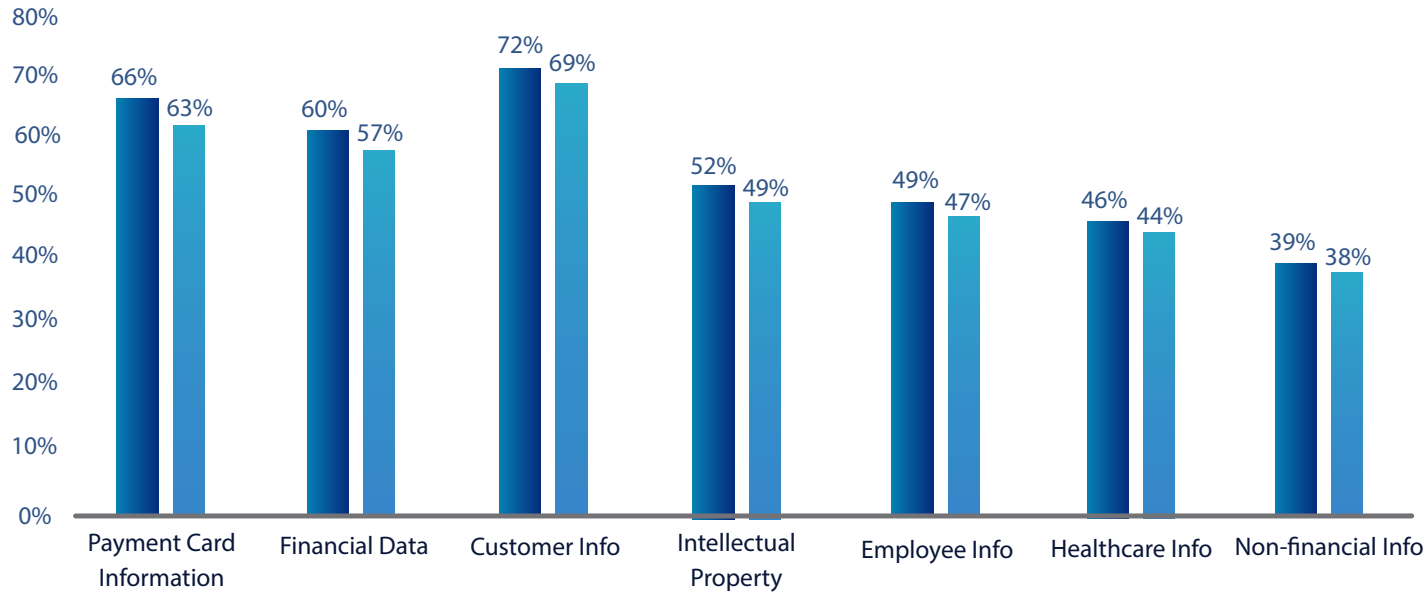


Most frequently encrypted data types:

There are seven frequently encrypted data types which is same as the last year's survey. Organizations responded with the seven data types. 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.

Non-financial data is the least preferred data type for encryption which can be understood due to its non-sensitive nature. Suprisingly, healthcare data is the second least encrypted data type. This might be attributed to lack of strict healthcare laws in many demographics. Figure 12, represents data comparison between FY21 and FY22.

Fig. 12 - Preferred data types for encryption



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.

Fig. 13 - Primary use cases for Kubernetes

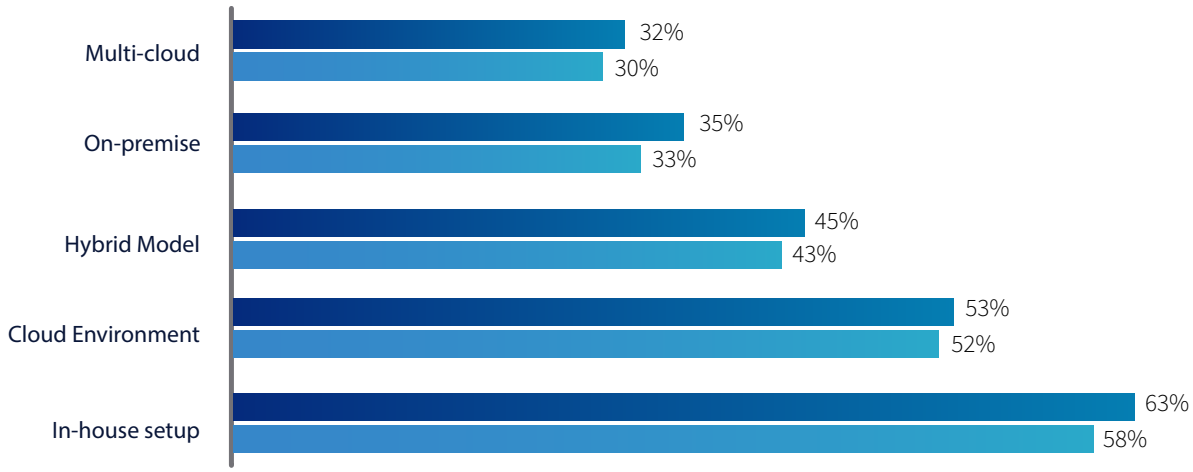
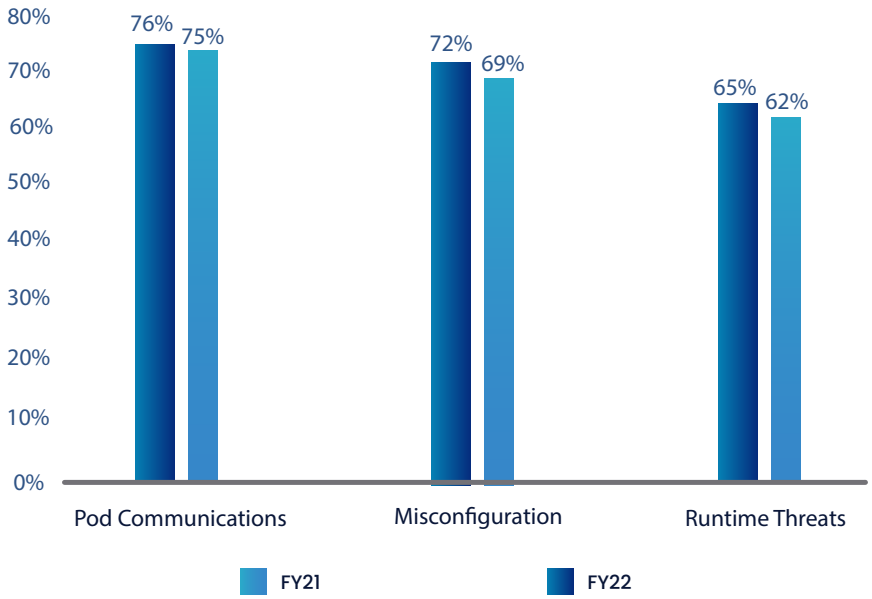


Fig. 14 - Companies response for major security threats for Kubernetes



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.

Fig. 15 - Main average rating on the challenges faced for Key Management

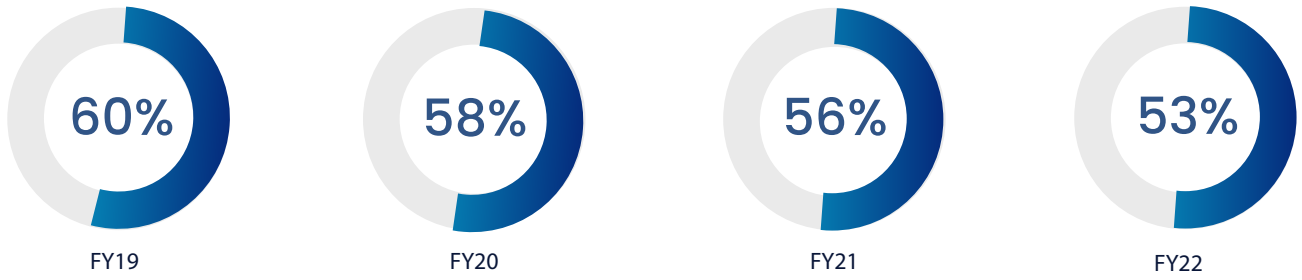
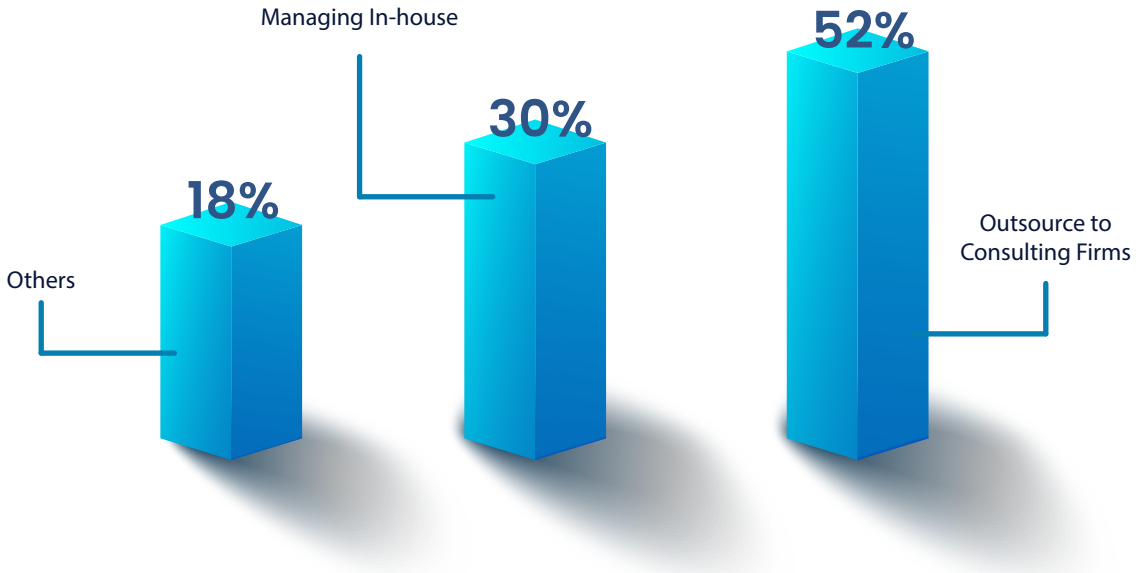


Fig. 16 - Organizations inclining towards consulting firms for technical expertise



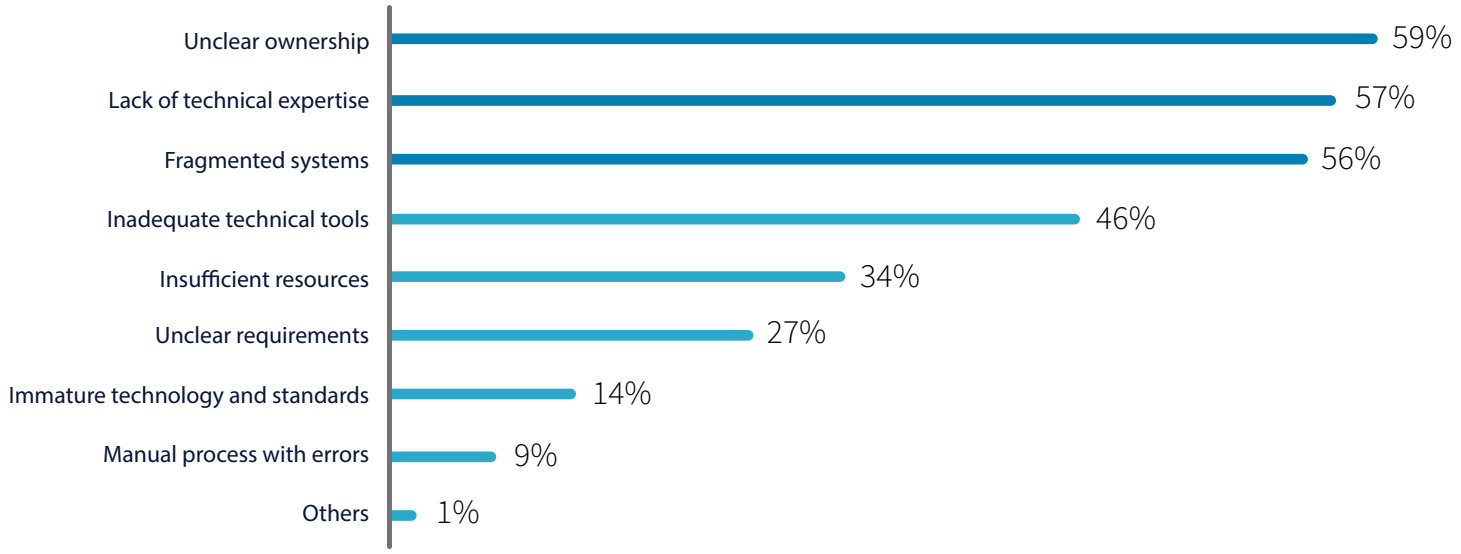
The highest percentage of responding companies (52%) preferred to outsource the Key management to expert consulting firms and 30% of companies wants to manage in-house, 18% companies can go either way.

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.

Fig. 17 - Major challenges in Key Management



The top three reasons why key management is painful :

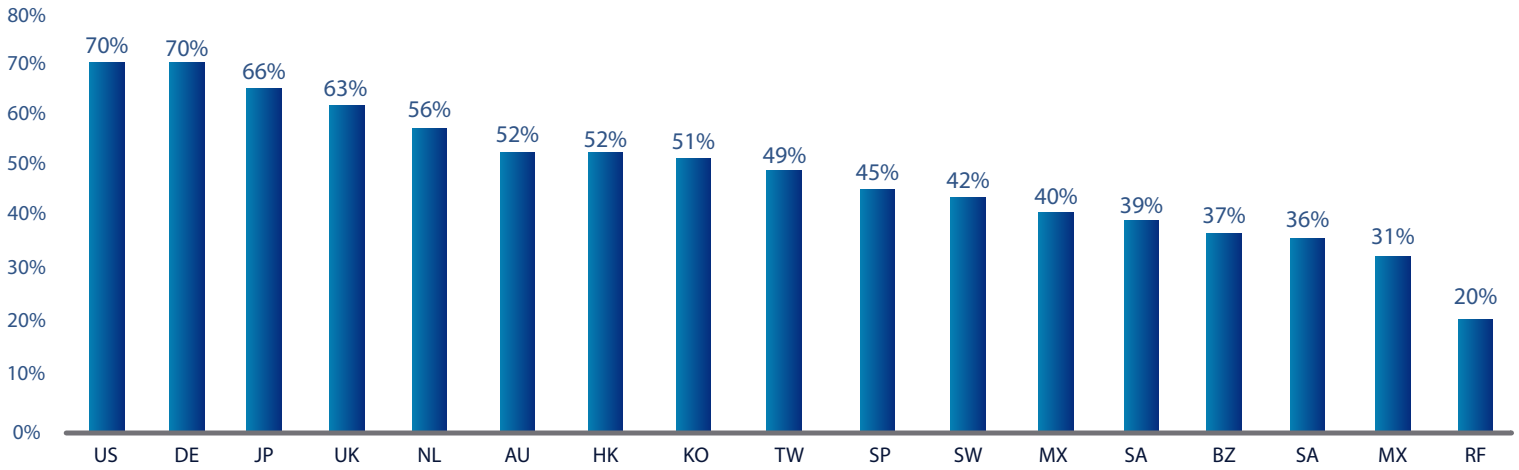
1. Unclear ownership of the key management function
2. Lack of technical expertise and skilled resources
3. Isolated or fragmented key management systems

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 **47% in 2019 to 57% in 2022** 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 19 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 19 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.

Fig. 18 - Willingness of Countries to deploy HSMs



*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.

The deployment of HSMs has increased steadily. Figure 19 shows a four year trend for HSMs. As can be seen, the rate of HSM deployment has constantly increased across the globe from 47% in FY19 to 57% in FY22.

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, 55 percent of respondents own and operate HSMs on premise for cloud-based applications, and 50 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.

Fig. 19 - HSM deployment rates over four years consolidated across countries

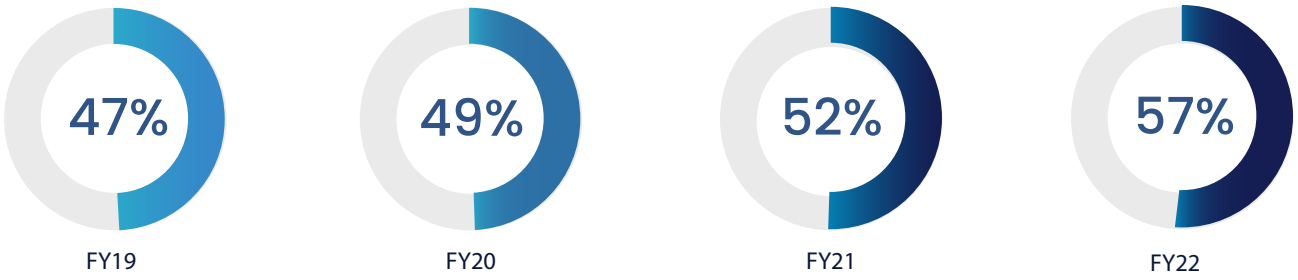
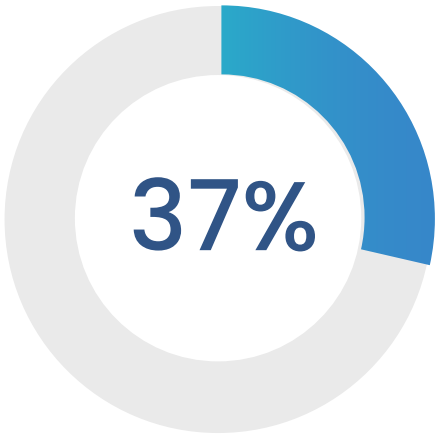


Fig. 20 - HSM usage trend with Cloud applications

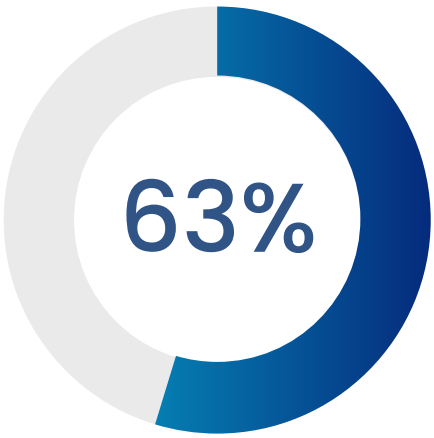
Figure 21 depicts the HSMs usage scenario by the responding organizations. 63% of the organization have a centralized team for managing HSMs & cryptography with in their firm. 37% of the respondents have a siloed approach.

In the siloed approach, individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional individual application-specific approach.

Fig. 21 - Organizational usage of Hardware Security Modules



Traditonal siloed application specific approach

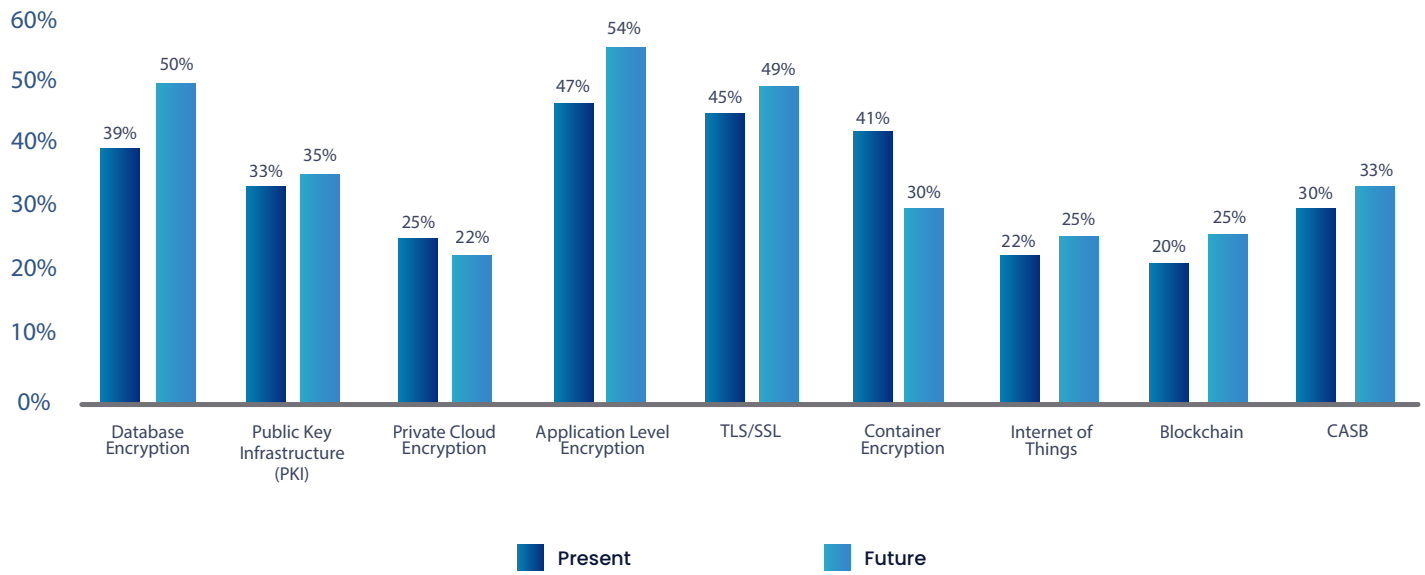


Centralized team managing all encryption (including HSMs)

Fig. 22, indicates the use cases of HSMs by different organizations participated in the survey. Present use cases of HSM versus future use cases. As per the survey outcome, data base 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 54 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 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.

Fig. 22 - HSMs - Current deployment vs Future deployment



Cloud Encryption

According to Figure 23, 47 percent of respondents say that more than 40% of their organization's data is on cloud. Another 47 percent of respondents confirmed that 60% of sensitive data is on cloud. Interesting fact is that only 23% reported that more than 50% of their data on cloud is encrypted. Organizations have 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 24 depicts sensitive data types stored on cloud by various organizations. Financial records, Employee records and business data are the top three data types that are stored on cloud and as expected, national security data is the least preferred.

Fig. 23 - Analysis on data stored on cloud by the respondents

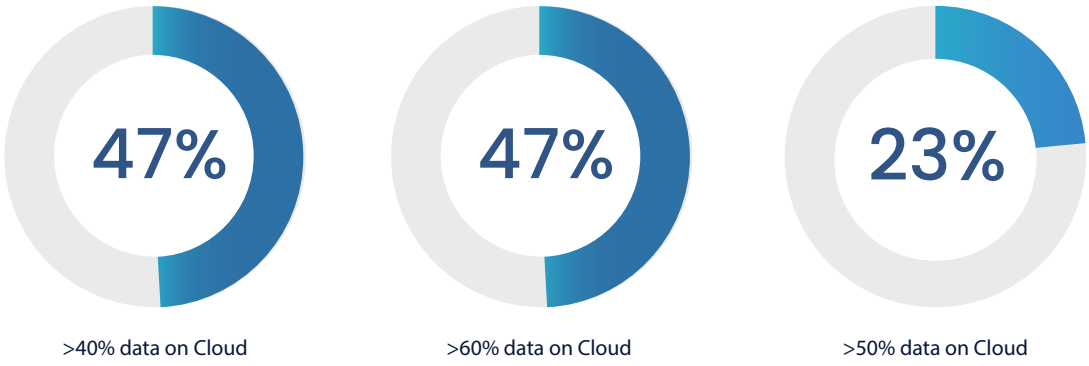
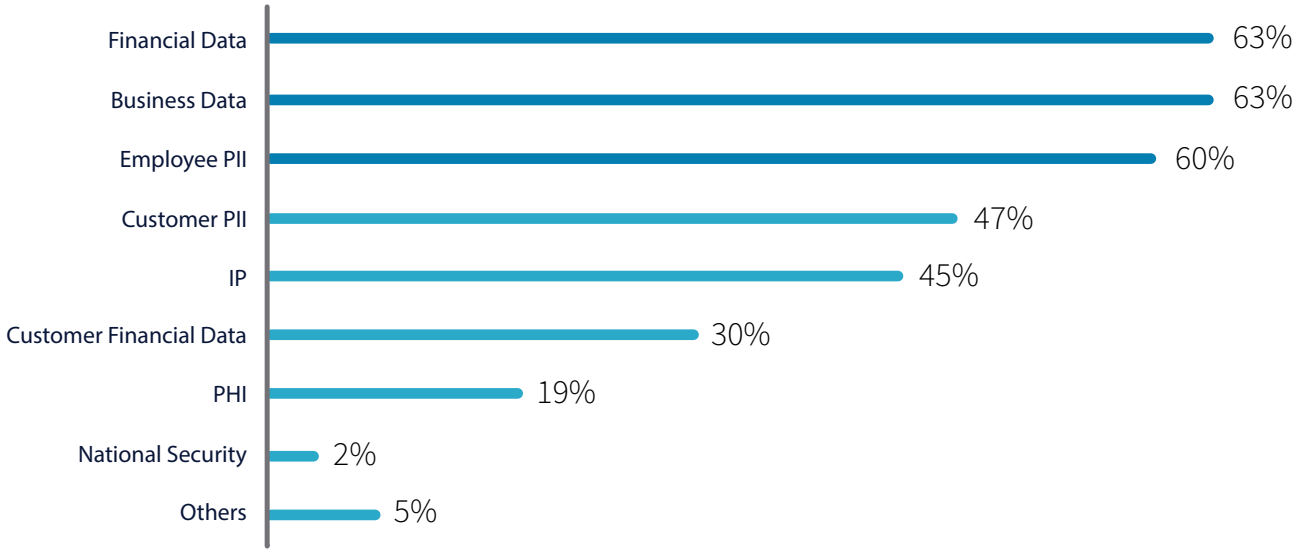


Fig. 24 - Analysis on sensitive data types stored on cloud FY22



We have more analysis from you from a different survey on cloud encryption by Entrust & Ponemon: As shown in Figure 25, 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 26.

Fig. 25 - How does your organization protect data at rest in the cloud

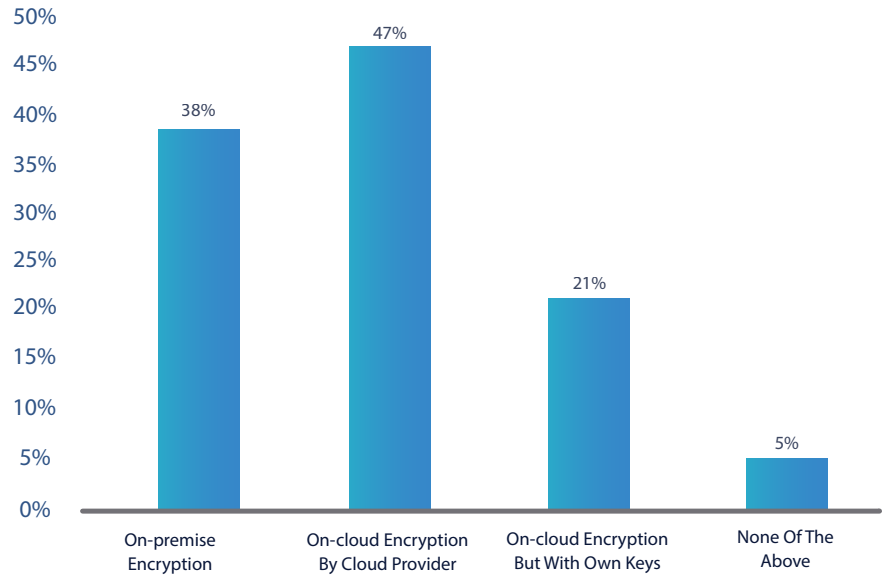
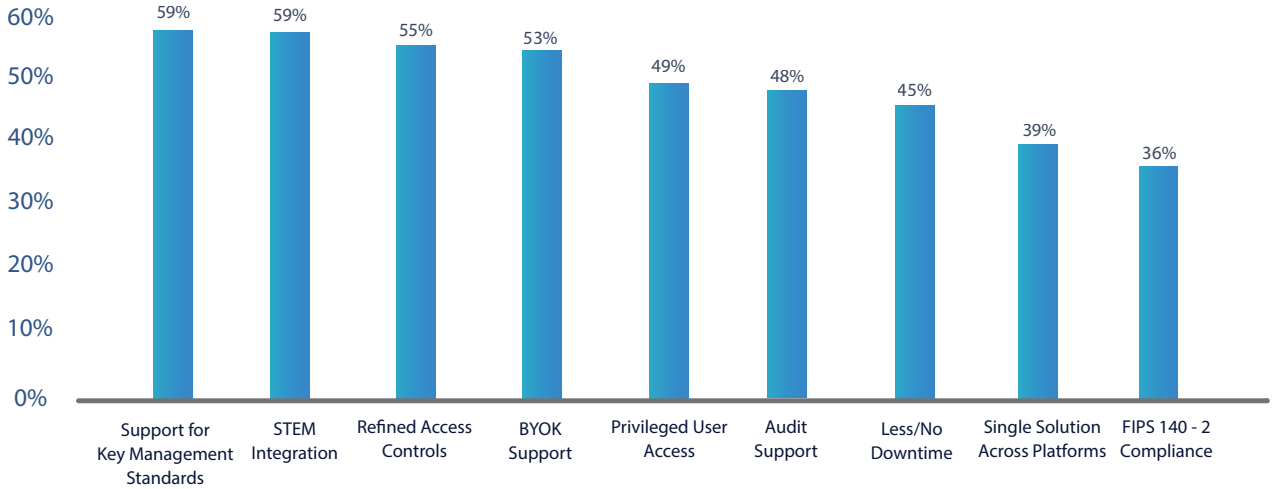


Fig. 26 - Critical features associated with cloud encryption



About Encryption Consulting

Encryption Consulting is an established data protection consulting market leader. Since its inception, this company has observed exponential growth in terms of customer base and the services it offers. It provides comprehensive consultancy services with the utmost security measures for individuals and businesses alike to protect their confidential information from malicious individuals or organizations.

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and integrating our 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.

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

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

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

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

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

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

Fornetix Key Orchestration TM is a scalable and Aexible solution designed to simpligy key management. Granular ploicy 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 is revolutionizing the manner in which NetOps and SecOps team.

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

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

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

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 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.

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.

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

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized accees. 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 that 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 environment? 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

encryptionconsulting.com

linkedin.com/company/encryptionconsulting

facebook.com/encryptionconsulting

twitter.com/encryptioncons