



Global Report ▶▶

2025 Encryption Trends Report

Discover the latest from the industry!



Executive Summary

As predicted in the trends report of 2024, it had been a pivotal year for the cybersecurity industry, with notable advancements and ongoing evolution across key domains of Encryption spread across multiple sectors and industries in 2024. Similar trends, as predicted in 2024, are expected to continue for 2025 with greater momentum. Areas such as Artificial Intelligence (AI), Post-Quantum Cryptography (PQC), and reduced certificate lifespans remain at the forefront of industry transformation.

Significant regulations and standards are also expected to take shape in 2025 with the increasing usage and adoption of AI and PQC. Initiatives like eIDAS 2.0 and the European Digital Identity Wallets have continued to shape industry standards and drive discussions, with upcoming regulations likely to introduce significant changes in the near future. On the PQC front, the release of initial standards last year has brought the prospect of a post-quantum cryptographic future closer to reality, intensifying industry speculation and preparation.

According to the survey conducted by **Encryption Consulting** across multiple industries, the encryption software market alone is expected to grow by **USD 15.5 Billion** in 2025, with the overall global encryption industry growing at a compounded annual growth rate (CAGR) of **16.2%**. Projections for this decade (**2020 - 2030**) also indicate a substantial growth in encryption adoption across all industries, with the growing inclusion of **AI and PQC**.

Table of Content

Executive Summary	2
Global Encryption Adoption Trends - 2025	4
Cost of Data Breaches in 2024	15
Key Drivers for Implementing Encryption	19
Key Management Solution: Trends and Insights for 2025	25
Emerging Trends and Industry Highlights for 2025	30
Hardware Security Modules: Key Trends for 2025	32
Emerging Trends and Key Insights	38
Conclusion	44



Global Encryption Adoption Trends – 2025



The Encryption Consulting firm conducted an elaborate survey with thoroughly researched questions to understand the global encryption trends for 2025. Multiple geographies across the globe are covered as part of the survey, which includes the United States, the Middle East, Spain, Germany, Japan, Hong Kong, Mexico, the United Kingdom, South Korea, and Taiwan. The overall trend observed is the increased focus on encryption as a primary data protection strategy with the rapid adoption of new-age technologies such as AI, Quantum Computing, and more. The survey meticulously considered a mix of firms operating under different jurisdictions and geographical areas, seeking to grasp specific encryption trends.

Similar to every year, as a tradition, we are sharing the company's stand on implementing budget allocation for FY-2025.

Figure 1 highlights a steady growth from 64% in FY2021 to 79% in FY2024, an increase of 15 percent in the last 4 years. This upward trend suggests that adoption, usage, and the performance in the measured area has been improving each year.

Fig.1 Companies response to survey about encryption strategy

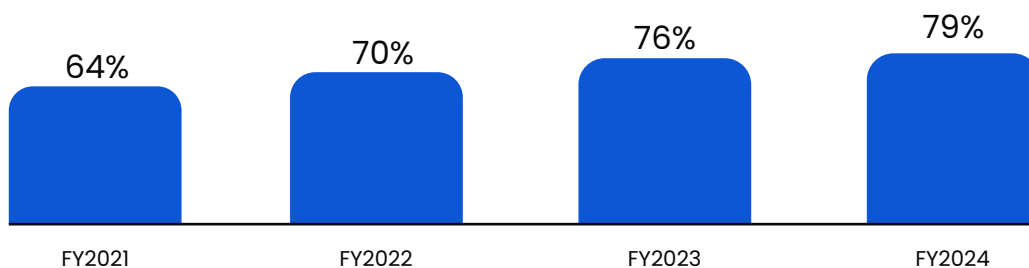
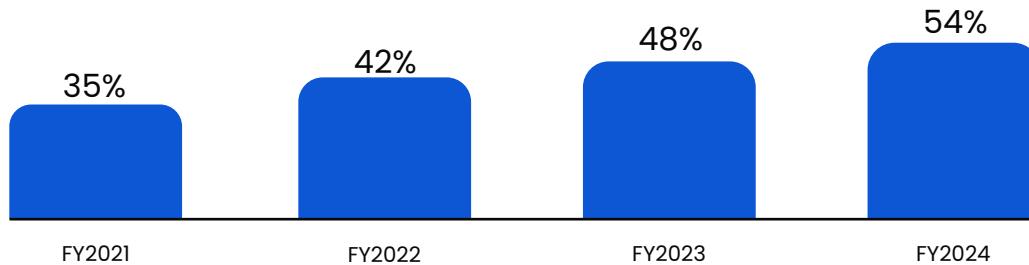


Fig.2 Companies planning to increase their annual budget for encryption



54% of the respondents are planning to increase their budget in the year 2025. The major driving force behind the trend is the change in the technological environment and the rise in digital threats. A major portion of the budget allocation is projected to be used to enhance the security infrastructure along with the handling of cloud encryption solutions.

Top Three Encryption Trends for 2025

Survey responses from professionals across various industries highlight three key encryption trends that will shape security strategies in 2025: PQC Readiness, AI-Driven Encryption Enhancements, and Cloud-Native Encryption Solutions. These priorities reflect the evolving security landscape and the need for organizations to adapt to emerging threats and technological advancements.

76%

PQC Readiness

74%AI-Driven Encryption
Enhancements**77%**Cloud-Native Encryption
Solutions

When asked about their primary encryption focus areas for 2025, respondents overwhelmingly prioritized cloud-native encryption solutions, underscoring the increasing reliance on cloud security for data protection. PQC readiness ranked high as organizations prepare for the long-term impact of quantum computing on cryptographic security. Meanwhile, AI-driven encryption enhancements are gaining momentum, reflecting a shift toward automation and intelligence-driven security measures to strengthen encryption frameworks.

PQC Readiness

The quantum shift is approaching fast. Since NIST launched the PQC project in 2016, multiple rounds of rigorous evaluation have taken place. After years of algorithm refinement, NIST finalized four algorithms in 2024 as part of the PQC Standardization Project, marking a major milestone in the transition to quantum-resistant cryptography.

CRYSTALS-Kyber: Key encapsulation mechanism (KEM) for secure key exchange

CRYSTALS-Dilithium: Digital signatures for authentication

FALCON: Digital signatures, particularly in applications requiring compact signatures

SPHINCS+: Stateless hash-based digital signatures

Fig. 3: NIST – PQC evolution over the years



The Gaps Observed in Enterprise Readiness

Security leaders across industries are increasingly recognizing the significant risks posed by advanced quantum computing. However, many organizations have yet to conduct comprehensive assessments of their cryptographic infrastructures, leaving them exposed to future quantum threats.



As the quantum era approaches, proactive preparation is essential to ensure long-term data security.

Sectors Impacted by Quantum Computing

Finance, defense, and healthcare are emerging as the leading adopters of quantum computing, according to survey responses from industry leaders. The financial sector remains at the forefront, with 70% of respondents highlighting strong use cases in areas such as fraud detection and cryptographic security. The defense sector is making significant investments in quantum computing, particularly for cybersecurity and process optimization. Meanwhile, 63% of respondents recognize the pharmaceutical industry's potential to leverage quantum computing for accelerating drug discovery and improving research efficiency.

While organizations see the advantages of quantum computing, they are also increasingly concerned about the security risks it introduces. A major challenge is its potential to break traditional encryption methods, particularly those based on RSA and other widely used cryptographic algorithms. As quantum capabilities advance, the urgency to develop quantum-resistant encryption is becoming a key focus across industries.

Fig.4: Sector-wise impact of quantum computing



70%
Finance/BKFS



68%
Defence



63%
Pharma



48%
Automobile



42%
Aerospace



37%
Media/Tech



18%
Others

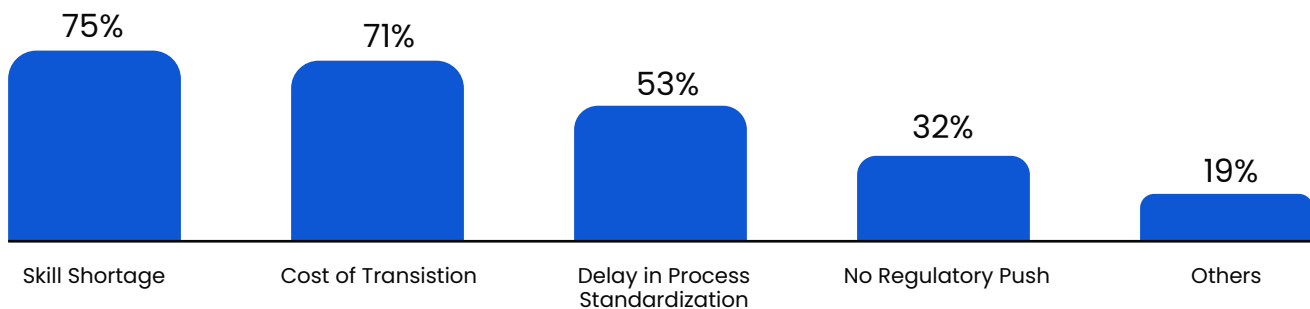
Challenges in PQC Implementation

PQC is termed as a one-stop solution to the risks arising from quantum computing. However, it is not a smooth transition from the existing cryptographic infrastructure. Organizations have reported several challenges they found while strategizing PQC deployment, and the top challenges are presented in the graph below. Skill shortage and cost of transition emerged as the top two challenges with PQC implementation as opted by 75% and 71% respectively.

73%

of the organizations prefer hiring a third-party consulting firm with expertise in PQC for assessment, strategy, and implementation to mitigate the risk of “Skill Shortage”

Fig.5: Challenges identified for PQC implementation



AI-Driven Encryption Enhancements

AI adoption is advancing rapidly, with continuous improvements reshaping encryption management and security operations. Organizations are leveraging AI to streamline processes, enhance efficiency, and strengthen cryptographic frameworks.

In 2025, AI's role in encryption management is expanding, enabling real-time threat detection, automated key lifecycle management, and adaptive encryption techniques. AI-driven solutions are addressing critical challenges such as scalability, compliance automation, and operational efficiency.



58% of critical organizations now use AI-powered tools for cryptographic key management and automated compliance checks, up from 45% in FY23.



AI integration in encryption processes is projected to grow at a 23% CAGR across industries through 2027.



AI-powered adaptive encryption has reduced response times to encryption-related breaches by 32% across major platforms.

With AI-driven encryption enhancements becoming more prevalent, businesses are focusing on optimizing encryption strategies, automating key processes, and improving overall security management.

\$2.5 million

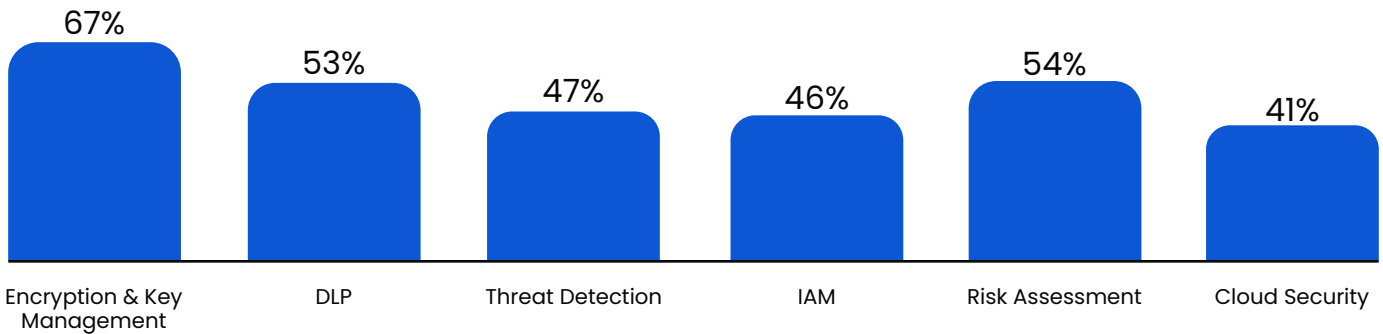
The average annual cost savings organizations achieve through AI-driven security and automation.

Top AI Use Cases in Cybersecurity

AI is transforming cybersecurity by enhancing threat detection, automating security operations, and strengthening encryption. While adoption is increasing, implementation rates vary across different use cases.

Security leaders recognize AI's potential across multiple security domains, but integration levels differ. The insights below highlight key AI applications and the percentage of organizations already leveraging them. Notably, encryption and key management have the highest adoption rate (67%), emphasizing AI's role in handling encryption and securing sensitive data. Risk assessment and threat detection also see significant adoption, underscoring AI's value in proactive threat mitigation. However, cloud security adoption remains the lowest (41%), indicating a slower pace of AI integration in this area.

Fig.6: Challenges identified for PQC implementation



Key Insights from Industry Security Leaders



AI-powered models detect 30% more threats than traditional rule-based systems by continuously learning and adapting to new attack patterns.

Manual encryption key management is prone to human errors, AI reduces these errors by 40%, improving both efficiency and security.

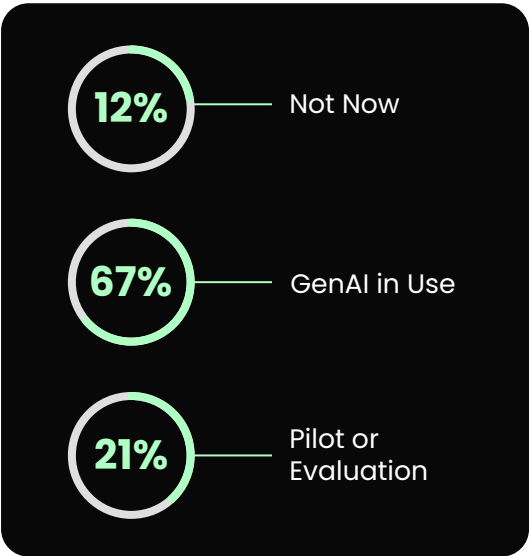
Organizations using AI-driven Identity and Access Management (IAM) systems have experienced a 60% decrease in unauthorized access attempts. These AI-based IAM solutions analyze user behavior, detect anomalies, and improve access controls while minimizing false positives through machine learning. This proactive approach enhances security and ensures compliance more effectively than traditional IAM methods.

GenAI in Cyber Security

Generative AI (GenAI) is rapidly transforming cybersecurity, driven by advancements in Large Language Models (LLMs). Organizations are increasingly leveraging GenAI for critical security functions such as threat detection, automated incident response, and real-time risk assessment.





Adoption of GenAI in Cybersecurity

Security leaders across industries are actively integrating GenAI into their operations. Currently, 67% of organizations have adopted GenAI-powered solutions, while 21% are in the pilot or evaluation phase. However, 12% remain hesitant due to concerns over regulatory challenges, accuracy issues, and AI hallucinations, where AI generates incorrect or misleading results, particularly when handling tasks beyond its training data.



Despite its potential, the implementation of AI-driven security presents several challenges. Many organizations struggle with data privacy concerns, regulatory uncertainties, and the reliability of AI in accurately interpreting threats. The lack of a clear legal framework further complicates deployment, while the demand for AI expertise continues to exceed the available skilled workforce. Additionally, high implementation costs create financial hurdles, forcing organizations to weigh AI’s benefits against the investment required.

While challenges persist, organizations recognize the transformative potential of GenAI in cybersecurity. With careful implementation and risk mitigation strategies, AI is set to play a crucial role in strengthening security defenses and enabling more proactive threat management.

Challenge		%	Description
	Data Privacy Concern	62%	AI models storing and using sensitive data
	AI Hallucinations	49%	Risk of GenAI misinterpreting security threats
	Regulatory Uncertainty	42%	Lack of clear legal framework governing AI
	Cost & Resource Skill	41%	High investment cost and limited AI-skillset workforce

Cloud-Native Encryption Solutions

Cloud migration is accelerating at an unprecedented rate, with adoption increasing year after year. As organizations transition to multi-cloud environments, securing data across these platforms has become a critical priority. Cloud-native encryption solutions offer robust protection for data in motion, at rest, and in use, addressing the unique security challenges posed by cloud environments.

In 2025, the adoption of advanced encryption techniques such as Bring Your Own Key (BYOK) and Keep Your Own Key (KYOK) is gaining momentum, allowing organizations to maintain greater control over their cryptographic keys and sensitive data. These techniques enhance security by ensuring that encryption keys remain exclusively under the organization's control, reducing reliance on third-party cloud providers.

Concerns over hosting sensitive data in the cloud are diminishing as organizations recognize the benefits outweigh the risks. Advances in cloud encryption technologies, including AES-256 for data at rest, TLS 1.3 and IPsec for data in transit, and End-to-End Encryption (E2EE), are reinforcing confidence in cloud security.

Survey responses highlight the growing reliance on cloud storage, with 67% of organizations having migrated more than 60% of their data to cloud environments. However, only 30% have surpassed the 80% threshold, indicating that complete cloud migration is not yet universal. Many organizations continue to adopt a hybrid approach, balancing cloud storage with on-premises infrastructure to meet security, compliance, and operational requirements.

As cloud adoption continues to rise, cloud-native encryption solutions will play a pivotal role in ensuring data security, regulatory compliance, and business continuity in an increasingly cloud-dependent world.

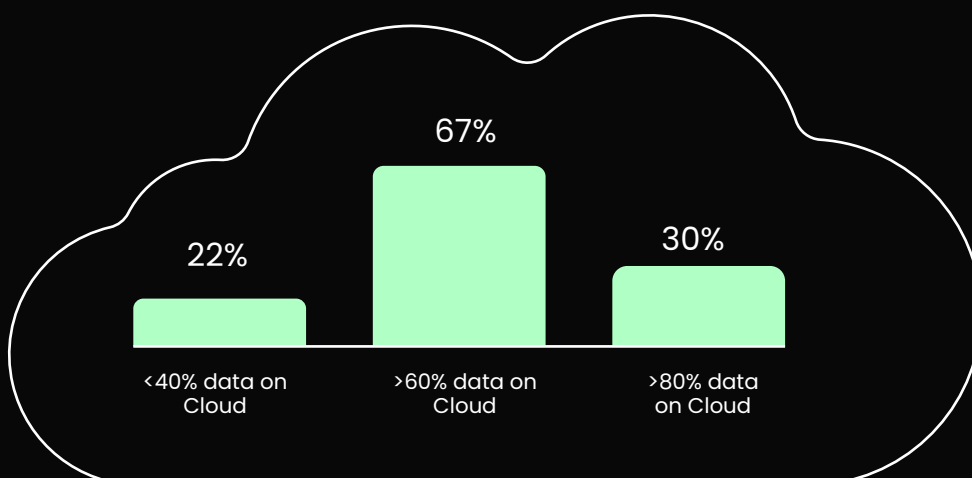
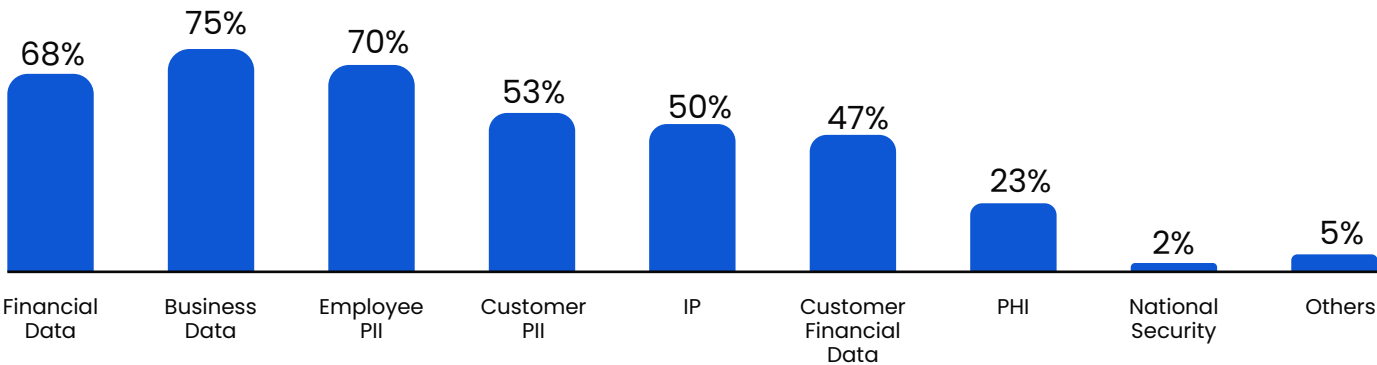


Fig. 7: Data stored in cloud

Sensitive Data Types Stored on Cloud

The volume of sensitive data stored in the cloud has increased compared to last year, reflecting a growing reliance on cloud infrastructure. However, defense and national security data remain the least migrated from on-premises environments due to the critical nature of this information and the severe consequences of potential security breaches.

Fig. 8: Type of data stored in the cloud



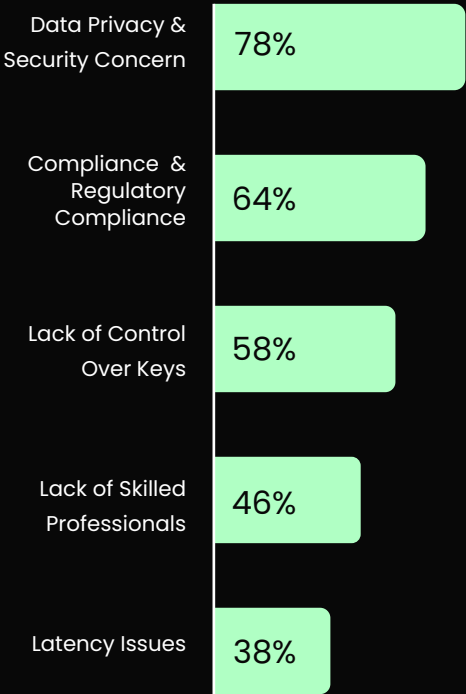
Organizations predominantly store business data, passwords, and personal information in the cloud, with business data being the most commonly migrated. In contrast, highly sensitive data such as protected health information (PHI) and biometric data are stored in the cloud far less frequently. This cautious approach is largely driven by regulatory requirements and security concerns, as organizations strive to balance the benefits of cloud adoption with the need to protect their most sensitive assets. While cloud storage continues to expand, organizations remain selective about which types of data they entrust to cloud environments, prioritizing security and compliance in their migration strategies.

Challenges in Full Cloud Migration

Despite the increasing adoption of cloud platforms, many organizations continue to face significant barriers to fully migrating their data and workloads. Security risks, regulatory compliance, data sovereignty, and operational complexities remain among the top concerns. Organizations dealing with highly sensitive data, such as financial institutions and government agencies, are particularly cautious due to the risks of unauthorized access, data breaches, and vendor lock-in.

Survey respondents highlighted key obstacles to full cloud adoption, with the most common challenges represented in the graph below. While organizations increasingly store business data, passwords, and personal information in the cloud, more sensitive data such as protected health information and biometric data is migrated far less frequently. This trend is largely driven by regulatory requirements and the need for enhanced security measures. As a result, organizations are adopting a strategic approach to cloud migration, leveraging the cloud for operational efficiency while ensuring that highly sensitive information remains under stricter protection.

Fig. 9: Barriers in the full cloud adoption

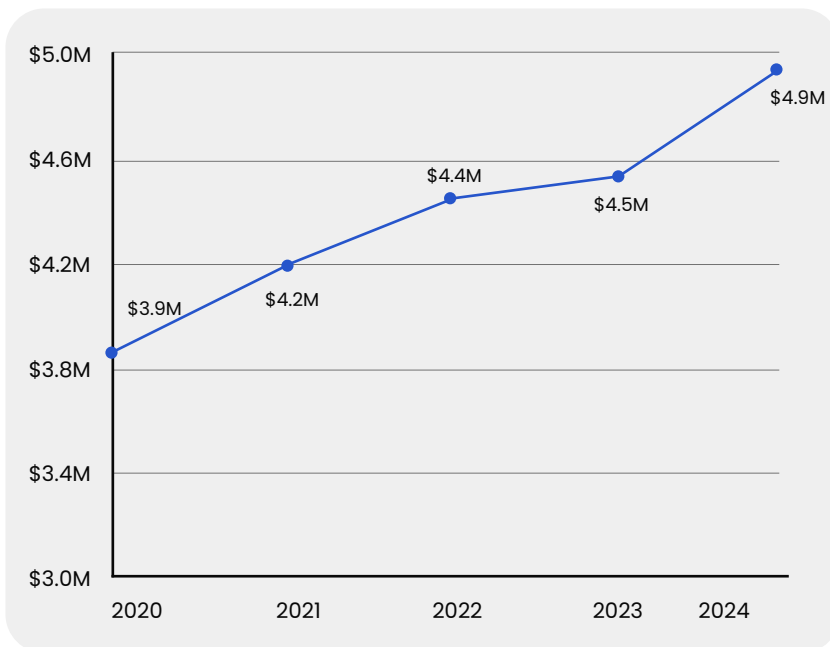


Cost of Data Breaches in 2024



Based on survey responses and insights from leading research firms, data breaches continue to impose significant financial burdens on organizations. The cost of breaches has risen by approximately 10% compared to last year, highlighting the escalating impact of cyber threats. Additionally, our 2025 survey reveals a widening skills gap, with 39% of organizations reporting a shortage of qualified professionals to manage security incidents effectively. This shortage further amplifies the risks, making it increasingly challenging for organizations to detect, respond to, and mitigate breaches in a timely manner.

Fig. 10: Cost of data breach over the years



Key Findings



Average cost of data breach is estimated to be **\$4.9 M** in 2024. Increase in cost can be attributed to lost customers, fines, and breach response



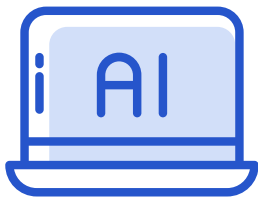
Healthcare is the most impacted sector due to data breaches & **United States** leads the world in average breach cost



39% of companies attribute low skilled employees or staff shortage to be main roadblock for tackling breaches.

AI in Security: Impact on Data Breach Loss

Detecting and responding to security breaches has long been a challenge for data security teams. However, the integration of AI in cybersecurity has made it significantly harder for bad actors to exploit vulnerabilities and cause damage. This year's survey introduces a new section analyzing AI's impact on breach mitigation, and the results are clear, AI is helping organizations detect breaches faster and reduce associated costs.

**31%**

Full Usage

37%

Limited Usage

32%

No Usage

AI Usage in Data Security

According to survey responses, 68% of organizations are leveraging AI for security, either fully or to some extent, to manage security incidents more effectively. Organizations utilizing AI-driven security measures report significantly lower breach costs compared to those without AI. The average cost of a data breach for organizations not using AI stands at \$6.12 million, whereas those leveraging AI experience a reduced average breach cost of \$3.92 million, a 36% decrease in financial impact.

**\$ 3.92M**

With AI Security

**\$ 6.12M**

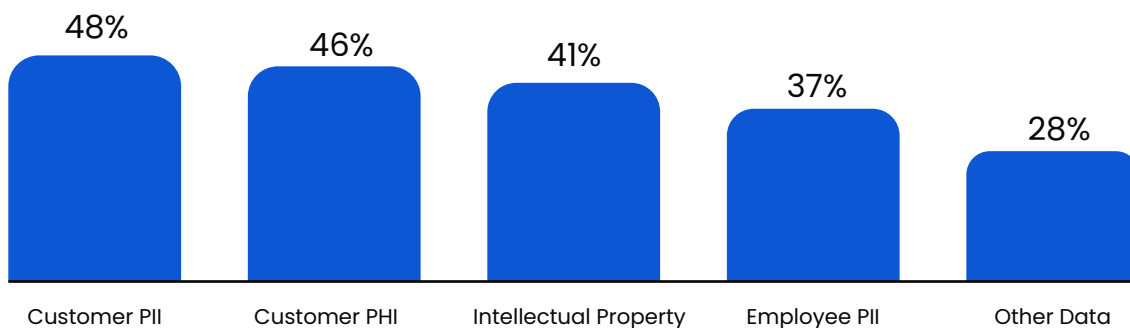
Without AI

Top Categories of Data Compromised in Security Breaches

In 2024, Customer's Personally Identifiable Information (PII) and Protected Health Information (PHI) emerged as the most frequently compromised data types, reported by 48% and 46% of respondents, respectively. Intellectual property also remained a prime target, with 41% of security leaders confirming data loss in this category during breaches.

The graph below presents insights from CISOs and security heads on the types of data most affected by security incidents. Respondents were allowed to select multiple categories, reflecting the widespread impact of breaches across various data types.

Fig. 11: Categories of data stolen during breach/attack



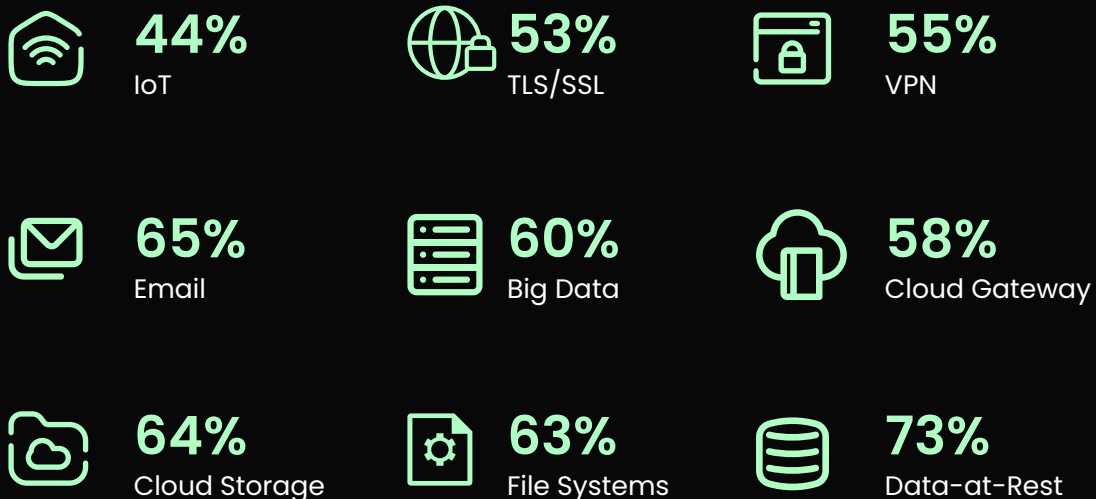
Preferred Encryption Deployment Options

Encryption deployment trends in 2025 remain consistent with those observed in 2024, with no overwhelming preference for a single approach. Data-at-rest encryption continues to lead, with 73% of organizations prioritizing its implementation, followed closely by cloud encryption at 64%.

A positive development is the growing focus on future-ready encryption strategies, particularly those leveraging AI and preparing for emerging threats from quantum computing. This shift highlights organizations' proactive approach as cybercriminals continue to refine their attack methods. Additionally, there has been a notable increase in organizations securing email communications to prevent data-in-motion breaches.

The figure below illustrates the adoption rates of various encryption deployment options. Data-at-rest remain the most widely secured, with 73% adoption, while IoT security lags at 44%. Other key areas, such as cloud storage (64%) and email encryption (65%), also demonstrate significant uptake, reflecting changing enterprise security priorities.

Fig. 12: Preferred domains for encryption deployment



Key Drivers for Implementing Encryption



As organizations deepen their reliance on digital infrastructure, securing sensitive data has become a critical business imperative. Encryption is no longer just a regulatory requirement, it is a strategic necessity for securing customer trust, ensuring compliance, and mitigating financial risks. The 2025 Global Encryption Trends Survey identifies the primary factors driving encryption adoption.

Rising Cybersecurity Threats and Escalating Attack Costs

The frequency and sophistication of cyberattacks have surged, causing significant financial and operational disruptions. Data breaches, ransomware incidents, and insider threats continue to challenge organizations, making encryption a fundamental defense against unauthorized access.



In 2024, 71% of organizations experienced at least one cybersecurity incident, underscoring the pervasive nature of digital threats.



Data breaches involving unencrypted data resulted in 29% higher financial losses compared to those where encryption was in place, demonstrating its tangible cost-saving benefits



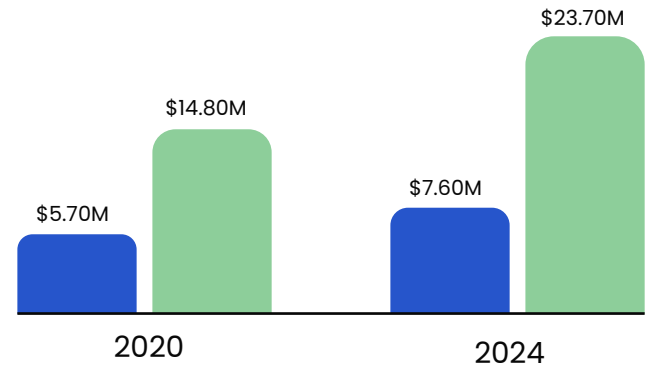
Phishing and malware attacks targeting employees rose by 22% year-over-year, reflecting an increasing reliance on social engineering tactics to compromise sensitive information.

As cybercriminals refine their attack methods, encryption remains a vital tool for ensuring data confidentiality, preventing unauthorized access, and minimizing the financial and reputational fallout of security incidents.

Regulatory Compliance and Data Privacy Mandates

Organizations increasingly recognize that the cost of compliance is significantly lower than the cost of non-compliance. Survey data reveals that non-compliance expenses are nearly three times higher than compliance costs, making regulatory adherence a key driver for encryption adoption. Rather than facing hefty fines and legal consequences, industries are prioritizing compliance as a proactive security measure.

Fig. 13: Cost of compliance vs cost of non-compliance



As illustrated in Figure 13, the financial disparity between compliance and non-compliance has widened over the years. In 2020, organizations spent an average of \$5.7M on compliance, compared to \$14.8M in non-compliance penalties. By 2024, compliance costs had risen to \$7.6M, while non-compliance expenses skyrocketed to \$23.7M, emphasizing the escalating financial risks of regulatory violations.

Fig. 14: Industry-specific compliance costs



Finance (\$30.9M) and Healthcare (\$28.3M) face the highest compliance expenses due to stringent regulatory mandates.



Manufacturing (\$24M) and Energy & Utilities (\$19.5M) also invest heavily in compliance to protect critical infrastructure.



In contrast, Retail (\$9.7M) and Media (\$7.4M) incur lower compliance costs due to fewer regulatory obligations.

Compliance expenditures encompass a range of activities, including regulatory audits, vendor selection, security upgrades, staff training, and continuous monitoring to ensure adherence to industry standards. While compliance costs vary by sector, they remain an important investment for preventing financial risks, strengthening data security, and maintaining customer trust.

Fig. 15: Cost of compliance as per sector



\$ 30.90M

Finance



\$ 30.90M

Healthcare



\$ 30.90M

Manufacturing



\$ 30.90M

Energy & Utilities



\$ 30.90M

Consumer Products



\$ 30.90M

Retail

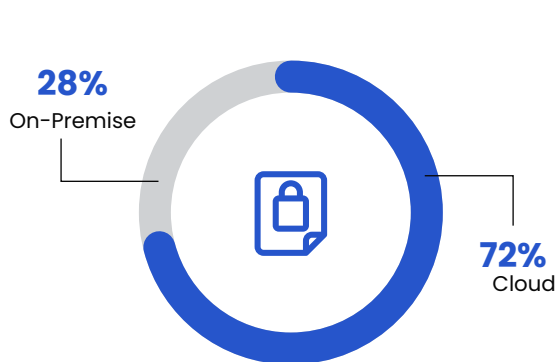


\$ 30.90M

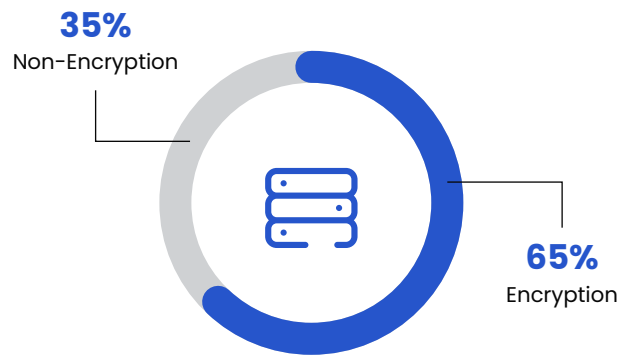
Media

Rapid Growth in Cloud Adoption

Organizations are increasingly shifting from on-premise infrastructure to cloud services, a trend reflected in survey responses from CISOs. In 2025, 92% of organizations are expected to adopt hybrid cloud strategies, driving the demand for robust cloud security solutions.



Sensitive data stored in cloud vs on-premise



Organizations preferring encryption as a security solution to protect data hosted on cloud

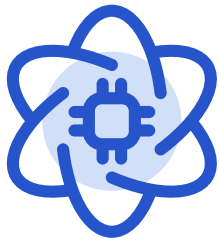
As the volume of sensitive data stored in the cloud continues to grow, the need for encryption as a primary protection mechanism has become more critical than ever. 65% of organizations identify encryption as their top choice for securing cloud data, emphasizing its importance in mitigating security risks and ensuring regulatory compliance.



Threat of Quantum Computing

Advancements in quantum computing algorithms pose a significant threat to widely used encryption methods such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). As quantum capabilities progress, organizations are increasingly adopting PQC to secure their data against future threats.

A majority of organizations (67%) recognize quantum computing as a serious security risk, primarily due to its potential to break existing encryption methods. While some remain unconcerned, the high awareness levels indicate that many are already evaluating mitigation strategies. The small percentage of uncertainty suggests that most organizations have a well-defined stance on the issue, highlighting the growing urgency for quantum-resistant security measures.

**5%**

Not Sure

28%

No

67%

Yes

Organizations Considering Quantum Threats as a Serious Risk

- In 2024, NIST finalized its quantum-resistant encryption standards, accelerating adoption, with 15% of enterprises launching quantum-safe pilot programs.
- Analysts project that unmitigated quantum attacks could lead to global economic losses exceeding \$3 trillion annually by 2035.

Customer Trust and Brand Reputation

A data breach can cause irreparable damage to an organization's reputation and customer trust. In an era where data security and transparency are top priorities for consumers, businesses must implement strong encryption to protect sensitive information and maintain credibility.

Key factors driving encryption adoption include:



81% of respondents prefer vendors that prioritize data security and privacy.

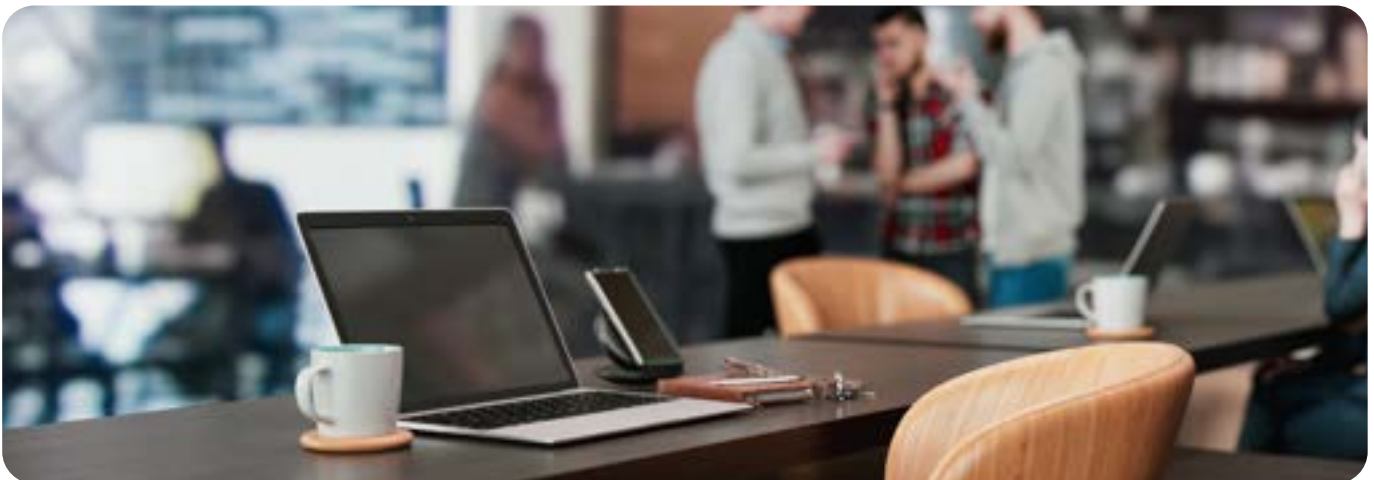


Organizations with unencrypted data experienced a 27% higher customer churn rate.



78% of surveyed companies reported that publicizing encryption practices led to increased customer trust.

As customers become more aware of data privacy risks, businesses that demonstrate a commitment to encryption gain a competitive edge and strengthen long-term customer relationships.



Key Management Solution: Trends and Insights for 2025



Study Background

Key management is a critical component for industries that rely on encryption for data protection. Securing encryption keys is a top priority, as any compromise can lead to severe financial and reputational damage.

Survey data highlights a significant rise in key management adoption:

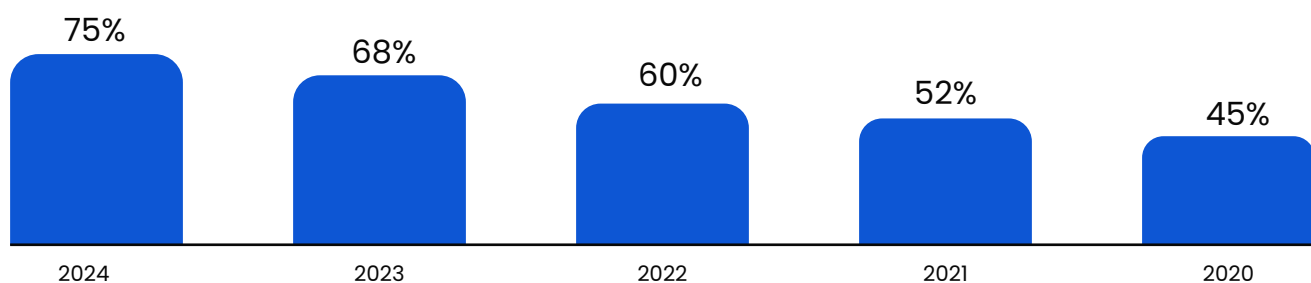


Adoption rates have surged from 45% in 2020 to 75% in 2024, reflecting a 30% increase post-pandemic.

This trend underscores the growing demand for robust key management solutions across industries worldwide.

Looking ahead, projections suggest key management adoption will reach 82% by 2025, as more organizations recognize it as a critical requirement for encryption security. The graph below illustrates the steady increase in implementation over the past five years.

Fig.16: Implementation rate of key management solutions across sectors



Key Management Trends 2025: Sector-Wise Analysis

Our survey provides a detailed industry breakdown of key management adoption, emerging trends, and rising challenges across major sectors in 2025.



Finance

The financial sector leads in adopting advanced key management solutions, driven by strict compliance regulations and high data sensitivity.

- 88% of financial institutions now use Centralized Key Management Systems (CKMS) to streamline operations and comply with PCI DSS, GLBA, and SOX.
- 25% rely on Hardware Security Modules (HSMs) to protect high-value transaction logs and encryption keys for authentication systems.
- 20% have adopted hybrid models, combining on-premise and cloud-based solutions for operational flexibility and robust security.



Healthcare

The healthcare industry has witnessed a surge in decentralized and scalable key management solutions to meet HIPAA requirements and safeguard patient data.

- 75% of providers use decentralized key management with fine-grained access controls to protect Electronic Health Records (EHRs).
- 35% have adopted cloud-based CKMS for administrative data management and cost-effective operations.
- 45% integrate Data Loss Prevention (DLP) solutions with encryption to minimize unauthorized data exfiltration and breaches.



Retail

Retailers prioritize securing payment card data and customer information while handling large-scale transactional data.

- 70% have implemented cloud-based CKMS for seamless scalability and enhanced security.
- 40% have increased investments in HSMs to protect high-value assets, including loyalty programs and proprietary recommendation algorithms.
- 85% now enforce regular key rotation, refreshing encryption keys at least quarterly to reduce the risk of compromise.



IoT (Internet of Things)

The rapid expansion of IoT networks has made encryption key management for billions of connected devices a critical challenge.

- 60% of organizations report difficulties in provisioning and managing encryption keys for globally distributed IoT devices.
- 45% have adopted hybrid key management, using cloud-based CKMS for key provisioning and on-premise solutions for secure storage.
- 20% are exploring blockchain-based solutions to enhance key traceability and reduce security vulnerabilities.



Telecommunications

With the expansion of 5G networks and connected devices, the telecom sector faces increased cybersecurity threats.

- 82% have integrated CKMS to secure customer metadata, call records, and 5G infrastructure.
- 30% leverage AI-powered encryption to detect and mitigate threats in real time.
- 50% have adopted hybrid key management models, balancing on-premise and cloud-based security solutions.



Defense and Security

The defense sector relies on high-grade encryption and stringent key management protocols to protect classified information.

- 95% of defense agencies use HSMs to safeguard military communications and intelligence data.
- 70% are transitioning to quantum-resistant encryption to counter future cybersecurity threats.
- 45% invest in AI-enhanced encryption for anomaly detection and cyber espionage prevention.



Transportation

With the rise of autonomous vehicles and connected transportation systems, encryption is vital for cybersecurity and passenger safety.

- 65% of transportation networks now use centralized key management for securing GPS, ticketing systems, and vehicle communications.
- 35% of aviation and maritime companies leverage blockchain-based encryption key management.
- 50% have implemented real-time key rotation to protect autonomous vehicle networks from cyber threats.



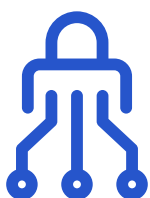
Energy

The energy sector faces increasing cyber threats, necessitating robust encryption strategies for securing power grids, smart meters, and operational technology (OT).

- 75% have deployed HSMs to protect critical infrastructure from cyberattacks.
- 40% utilize AI-powered key management for predictive threat detection and real-time incident prevention.
- 55% have adopted hybrid cloud encryption models to secure multi-region energy networks.

This sector-wise analysis highlights the growing adoption of key management solutions across industries, emphasizing their critical role in securing sensitive data and ensuring regulatory compliance in 2025.

Emerging Trends and Industry Highlights for 2025



Quantum-Resistant Cryptography

30% of organizations in finance, healthcare, and defense have begun transitioning to quantum-resistant cryptographic algorithms, preparing for the impact of quantum computing.

These sectors are leading the charge, recognizing the urgency of staying ahead of emerging quantum threats as the environment changes.



AI-Powered Key Management

15% of early adopters across industries are utilizing AI-driven tools to automate key lifecycle management, detect anomalies, and enhance threat response.

According to CISOs, AI-powered key management, when combined with human oversight, is proving to be both highly efficient and cost-effective.



Managed Security Services (MSS)

With rising costs and a shortage of in-house expertise, 35% of small and medium-sized enterprises (SMEs) are turning to MSS providers for comprehensive, cost-effective key management solutions.

Key Takeaways from the 2025 Survey

Industry-Specific Drivers: Regulatory compliance and data sensitivity remain the primary forces shaping key management strategies across industries.

Hybrid Models: Adoption of hybrid key management solutions continues to grow, balancing security, scalability, and operational efficiency.

Emerging Technologies: AI-powered automation and quantum-resistant cryptography are becoming essential components of secure key management.

Regulatory Compliance: Effective key management remains a critical factor in meeting global compliance standards such as GDPR and CCPA.

This industry-wide analysis underscores the growing importance of key management across all sectors. Organizations are increasing their budgets not only to meet compliance mandates but also to strengthen operational security.

A closer look at budget trends reveals:

- 58% of organizations plan to increase spending on key management solutions, demonstrating a strong commitment to cybersecurity investments.
- 33% will maintain their current budget, indicating a steady approach to security.
- Only 9% anticipate budget reductions, highlighting the consensus that robust key management is vital in addressing evolving security challenges.



33%

No Change

9%

Reduced Budget

58%

Increased Budget

Expenditure on Key Management

Hardware Security Modules: Key trends for 2025



Study Background

HSMs remain the preferred choice for CISOs when it comes to critical key management. A vast 78% of CISOs cite physical security as the primary reason for choosing HSMs over other key management solutions, while 72% express confidence in HSMs' ability to withstand tampering attempts and protect stored encryption keys with high efficiency.



Highly regulated and security-driven industries, in particular, continue to favor HSMs for their ability to safeguard cryptographic keys, ensuring compliance with stringent regulatory requirements.



As the cybersecurity environment is transforming around us, organizations are scaling their operations, and HSMs are serving as the backbone of secure encryption practices, reinforcing data integrity and enhancing overall cybersecurity resilience.



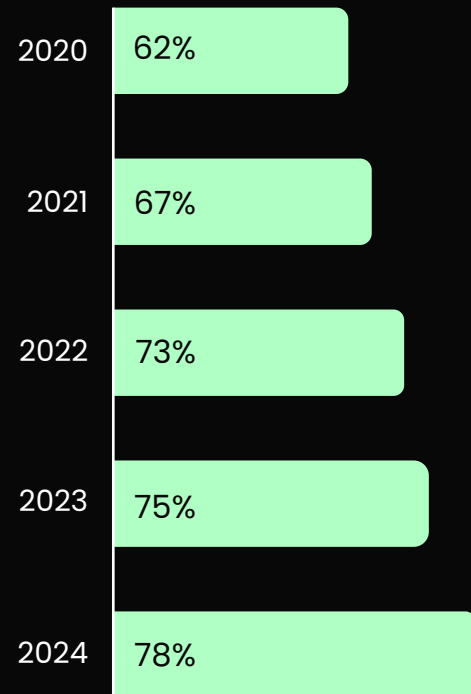
This study explores HSM adoption trends across industries, along with key takeaways and global insights on HSM usage.

Rising Adoption of HSMs Over the Years

A key trend observed in this survey is the consistent rise in HSM adoption across industries from 2020 to 2024, with a 16% growth rate over the past five years. This increase is largely driven by the heightened risk of encryption key loss and stricter regulatory requirements worldwide.

Figure 17 illustrates this steady progression, with adoption rising from 62% in 2020 to 78% in 2024. The most significant jump, 5 percentage points between 2021 and 2022 suggests a critical turning point, likely influenced by major security incidents, regulatory changes, or the acceleration of digital initiatives post-pandemic. While growth has stabilized in recent years, the sustained upward trend reflects continued industry commitment to robust encryption key protection and compliance readiness.

Fig.17: Organizations willing to spend on HSMs



HSM vs. Cryptographic Key Management Systems (CKMS)

The survey also examined organizations' preferences for key management solutions. A hybrid approach combining HSMs and CKMS emerged as the most popular choice, adopted by 46% of respondents.

The accompanying figure provides a high-level breakdown of HSM, CKMS, and hybrid solution usage, offering insight into how organizations balance security, flexibility, and compliance needs.



46%

Hybrid Solution



26%

HSM



28%

CKMS

Industry-Wise HSM Adoption Trends – 2025

HSM adoption varies significantly across industries, driven by factors such as data sensitivity, regulatory mandates, and organizational scale. This survey provides an industry-specific breakdown of HSM usage, with finance (55%) and healthcare (34%) leading adoption, followed by IoT deployments.



Finance

As one of the most heavily regulated sectors, financial institutions rely on HSMs to ensure compliance and protect critical assets.

- 55% of financial institutions use HSMs for securing transaction logs, customer authentication keys, and digital certificates.
- Compliance with PCI DSS and GLBA drives adoption, as HSMs provide a tamper-proof environment with advanced cryptographic capabilities.
- 30% are implementing a hybrid model, combining HSMs with CKMS for enhanced scalability without compromising security.



Healthcare

With HIPAA and other regulations requiring strict data security, healthcare organizations integrate HSMs to protect patient health information (PHI).

- 34% of healthcare providers deploy HSMs to secure medical images, genetic data, and electronic health records (EHRs).
- HSMs act as secure enclaves for cryptographic operations, reducing risks associated with cloud-based storage.
- 18% of healthcare organizations now use multi-party HSMs, up from 15% last year, to enhance security across research networks and healthcare systems.



Retail

Retailers leverage HSMs to protect customer data, secure transactions, and ensure compliance with PCI DSS.

- 12% of retailers use HSMs to secure sensitive customer data and intellectual property.
- Large retailers handling high transaction volumes rely on HSMs for payment card encryption.
- 7% are testing HSM-based secure enclaves to process customer data within hybrid cloud environments.



IoT (Internet of Things)

IoT networks require strong security measures to protect devices from cyber threats, making HSMs essential.

- 20% of organizations with critical IoT deployments use HSMs for firmware updates, device provisioning, and secure communication.
- HSMs serve as dedicated cryptographic processors, offloading security workloads from resource-constrained IoT devices.
- 12% implement HSM-based key vaults for managing encryption keys at scale.



Telecommunications

Telecom providers rely on HSMs to secure vast volumes of voice, messaging, and data transmissions.

- 30% of telecom firms use HSMs for encrypting network communications.
- HSMs play a critical role in 5G security, safeguarding SIM card encryption keys and network authentication mechanisms.
- 18% of telecom providers use HSMs to support PKI for secure communications.



Defense and Security

Government and defense agencies deploy HSMs to protect classified information and national security infrastructure.

- 45% of defense organizations rely on HSMs for encrypting classified intelligence data and government networks.
- Military-grade HSMs provide secure authentication and data integrity for critical communications.
- 20% of national security agencies are investing in quantum-resistant HSMs to counter future encryption threats.



Transportation & Aviation

Encryption is crucial in securing autonomous vehicles, aircraft networks, and logistics infrastructure.

- 22% of transportation firms use HSMs for secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) encryption.
 - Airlines integrate HSMs to encrypt passenger data and secure aircraft communication networks.
 - 15% of logistics firms use HSMs to protect digital tracking systems and maintain supply chain security.
-



Energy

As a frequent target of cyberattacks, the energy sector prioritizes HSM adoption to secure power grids and industrial control systems.

- 35% of energy companies deploy HSMs to protect SCADA systems and prevent unauthorized access.
- HSMs help secure renewable energy networks, encrypting distributed solar and wind power data.
- 18% of oil & gas firms use HSMs to encrypt SCADA pipelines for real-time monitoring and cyber threat protection.

Emerging Trends and Key Insights



Cloud-Integrated Security: By 2026, over 50% of organizations will adopt hybrid models, combining HSMs with CKMS to achieve both on-premises security and cloud scalability.



Quantum-Resistant HSMs: As quantum computing advances, 15% of enterprises are transitioning to quantum-resistant HSMs to safeguard encryption from future threats.



Cost-Effective Security: Managed HSM services are gaining traction, with 20% of small and medium-sized businesses (SMBs) opting for subscription-based models to reduce upfront costs while maintaining strong security.



Blockchain Security: 10% of organizations are leveraging HSMs to secure private keys in blockchain environments, particularly in industries like finance and supply chain management.

Key Takeaways

- HSMs continue to be essential for industries that require high-assurance encryption for sensitive data.
- Adoption rates vary, with financial services and healthcare leading due to stringent compliance requirements.
- Trends such as quantum-resistant cryptography, cloud integration, and managed services are shaping the future of HSM deployment.

Code Signing Trends of 2025

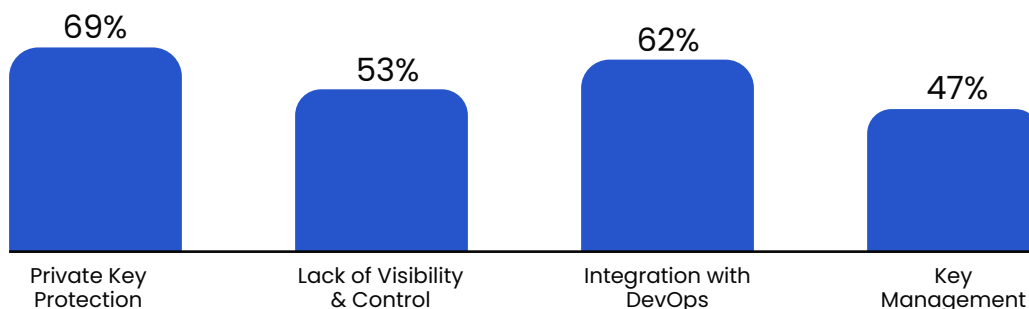
As software security threats are becoming more advanced, code signing remains an important practice for ensuring authenticity and integrity. Organizations increasingly recognize the need to attach digital signatures to software, verifying that it originates from trusted sources. Industry data highlights strong growth in adoption, with the code signing adoption rate at 54% in 2024. Looking ahead, 87% of respondents express confidence that adoption will continue to rise in 2025, reflecting a growing consensus on its importance for secure software distribution and authentication.



Code-Signing Challenges

Despite this upward trend, organizations face key challenges in implementing effective code signing protocols. Protecting private keys remains the most pressing concern, with 69% of respondents identifying it as a top challenge. Integration with DevOps environments is another significant hurdle, cited by 62% of respondents. The decentralized nature of modern software development further complicates deployment, requiring organizations to balance security with operational efficiency. As code signing adoption accelerates, addressing these challenges will be critical in ensuring a seamless and secure implementation across industries.

Fig.18: Organizations willing to spend on key management



Supply Chain Security Trends of 2025

In 2025, businesses across industries are prioritizing encryption to secure sensitive supply chain data, ensuring protection against cyber threats and regulatory non-compliance. Insights from the 2025 Global Encryption Trends Survey reveal how organizations are strengthening their security strategies to mitigate risks and enhance supply chain resilience.

Key Findings from Survey

Escalating Concerns Over Supply Chain Vulnerabilities

Supply chain security has become a top priority, with 78% of organizations placing greater emphasis on securing their supply chains, a 12% increase from 2024. This shift highlights growing concerns over third-party risks, as 62% of respondents identified vendor security gaps as the leading cause of supply chain breaches. The urgency is further underscored by the fact that 40% of enterprises experienced at least one supply chain-related cyber incident in the past year, with an average financial impact of \$4.2 million per breach. As cyber threats grow more sophisticated, organizations are under increasing pressure to bolster their defenses.

Encryption Adoption for Supply Chain Security

Encryption remains the cornerstone of supply chain security, with 81% of organizations implementing end-to-end encryption to safeguard supplier communications and data. Additionally, 57% encrypt data exchanges between supply chain partners, reflecting a strong but slightly lower emphasis on securing data in transit. However, adoption of quantum-resistant encryption remains limited at 32%, indicating that while awareness of future threats is rising, most businesses still rely on traditional encryption methods. This gap highlights the need for proactive planning as quantum computing advances.



End to end encryption for securing suppliers



Encrypted data exchanges between supply chain partners



Quantum resistant encryption for supply chain

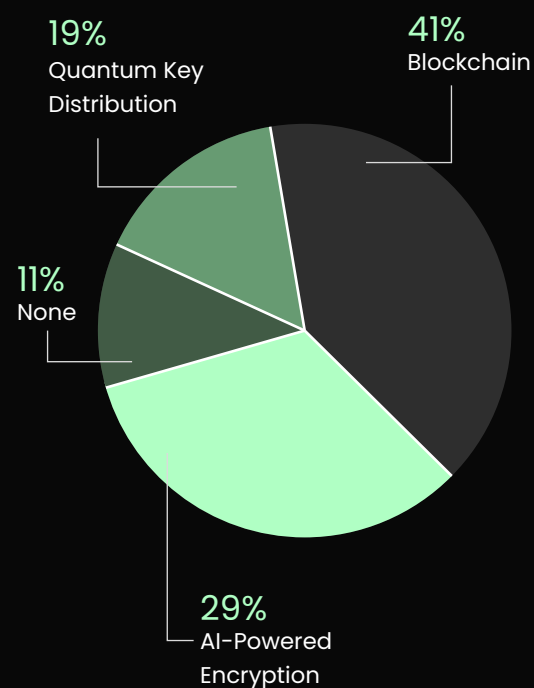
Regulatory Compliance Driving Encryption Strategies

Compliance with global regulations continues to drive encryption adoption, with 73% of organizations citing adherence to NIST, GDPR, and CISA guidelines as a key factor in securing supply chain data. The introduction of stricter cybersecurity regulations in 2025 has prompted 66% of companies to enforce tighter encryption requirements for suppliers, ensuring third-party security aligns with internal policies. Additionally, 48% of enterprises now conduct mandatory encryption audits for vendors, signaling a shift toward proactive risk management.

Adoption of Emerging Encryption Technologies

Organizations are increasingly turning to advanced encryption technologies to strengthen supply chain security. 41% have adopted blockchain, making it the most widely implemented solution due to its ability to ensure tamper-proof and transparent transactions. 29% are leveraging AI-powered encryption, demonstrating a growing reliance on artificial intelligence for detecting vulnerabilities and enhancing security. Meanwhile, 19% have implemented Quantum Key Distribution (QKD) as an early measure to counter future quantum threats. Notably, only 11% of organizations have yet to adopt any of these emerging encryption technologies, indicating that the vast majority, 89% of respondents recognize the importance of strengthening their encryption strategies.

Fig.19 Emerging encryption adoption



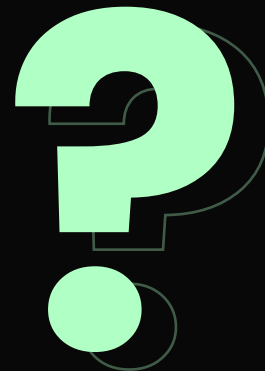
These trends indicate that while organizations recognize the urgent need for stronger supply chain security, challenges remain in fully adopting next-generation encryption. The disparity between traditional encryption methods and emerging technologies suggests that businesses must accelerate efforts to protect their security architectures against the rising security threats.

Regulatory Compliance for Encryption

Encryption adoption is increasingly driven by regulatory requirements, with 78% of organizations in 2025 prioritizing compliance with frameworks such as NIS2, DORA, the EU AI Act, PCI DSS 4.0, and the UK Cyber Resilience Act. This reflects a broader industry shift toward standardized encryption practices to meet evolving security mandates. Meanwhile, NIST's efforts in developing quantum-resistant encryption highlight the growing urgency of preparing for future cryptographic threats.

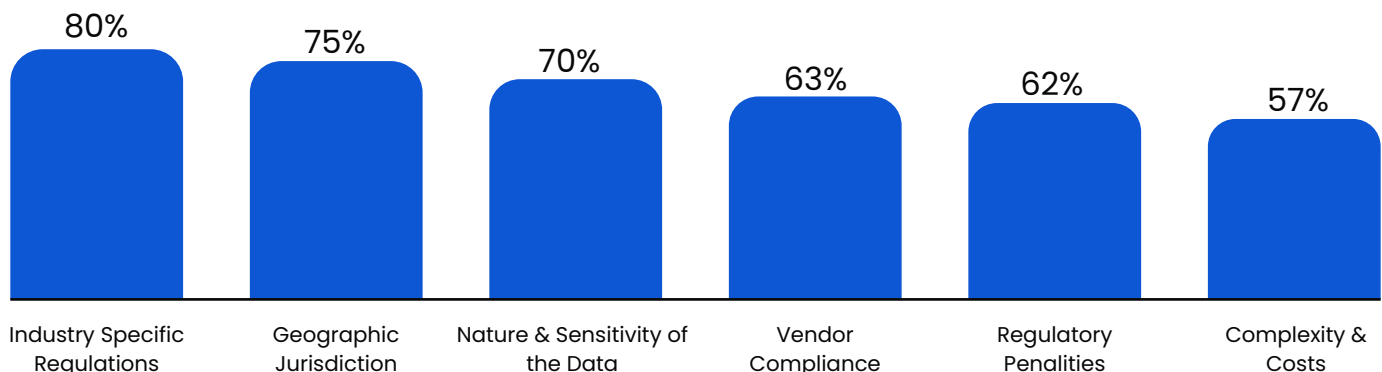
What Determines Compliance Priorities?

When determining compliance priorities, 80% of organizations emphasize industry-specific regulations, demonstrating that encryption requirements are often dictated by sector-specific security needs. Geographic jurisdiction follows closely, with 75% highlighting the necessity of adapting encryption strategies to regional laws and cross-border compliance challenges.



Data sensitivity remains a major consideration at 70%, reinforcing the need for strong encryption measures to protect high-value information. Vendor compliance (63%) and regulatory penalties (62%) also shape encryption strategies, as organizations navigate third-party security requirements and financial risks associated with non-compliance. While complexity and cost are factors for 57% of businesses, the focus remains on meeting regulatory standards to maintain security and compliance.

Fig. 20: Key Factors Influencing Regulatory Compliance Prioritization



Key Challenges in Regulatory Compliance

As organizations work to comply with regulations such as GDPR, PCI DSS, HIPAA, FIPS, NIS2, and DORA, they face significant challenges in implementing and managing encryption effectively. The 2025 Global Encryption Trends Survey highlights two primary concerns reported by CISOs and CEOs: managing encryption across multiple platforms and maintaining effective encryption key management.



The survey findings indicate that inconsistent encryption practices across cloud and on-premise environments increase compliance risks, leading to potential data exposure, security incidents, and financial penalties. As regulatory requirements continue to expand, organizations are adapting their encryption strategies to address these challenges.

Key Highlights

67%

face challenges in ensuring consistent encryption policies across multi-cloud environments.

62%

believe encryption key management and governance to be their primary concern.

58%

consider the high cost of implementation to comply with global regulatory standards to be their core challenge.

54%

face the challenge of a lack of skilled personnel and expertise to ensure smooth & effective compliance.

50%

consider frequent updates to encryption policies in regard to regulations like NIS2, GDPR, DORA, and more to be the biggest challenge.

Conclusion

This report highlights critical trends shaping cybersecurity strategies, emphasizing the need for automation, quantum readiness, and regulatory alignment. To maximize the insights provided, organizations should focus on:

Prioritizing Certificate Management Automation

Reduce operational risks and compliance challenges by implementing automated certificate lifecycle management solutions to prevent outages and security lapses.

Enhancing Key Management and Software Integrity

Secure cryptographic keys with HSMs and enforce strict code-signing policies to mitigate supply chain attacks.

Building a Scalable Cloud Security Strategy

Implement consistent encryption, access control, and policy enforcement across hybrid and multi-cloud environments.

Preparing for the Post-Quantum Era

Start assessing cryptographic assets and planning migration to quantum-resistant algorithms to ensure long-term data security.

Strengthening Compliance Frameworks

Align security strategies with evolving regulations such as NIS2, DORA, and the Cyber Resilience Act to avoid penalties and enhance resilience.

Making the Most of This Report

- Use these insights to assess your current security posture, identify gaps, and prioritize areas for improvement. Leverage automation, proactive risk mitigation, and expert guidance to stay ahead of evolving threats.
- Encryption Consulting provides tailored products and services in domains like PKI, certificate lifecycle management, PQC, code-signing, encryption, and more. Contact our experts to get end-to-end security strategies and a roadmap that align with your business objectives.





Building a cyber-secure future together!

Encryption Consulting is a trusted leader in data protection, offering expert solutions in applied cryptography. Trusted by Fortune 500 companies, we secure organizations with our advisory services, products, and training to ensure compliance, efficiency, and resilience.

[Connect with an Expert](#)



Global Headquarters - 130 N Preston
Rd, Prosper, TX 75078, USA

Contact Us

- info@encryptionconsulting.com
- +1- 469-815-4136