ENTRUST | Ponemon INSTITUTE

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

2022 GLOBAL ENCRYPTION TRENDS STUDY

Executive Summary

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

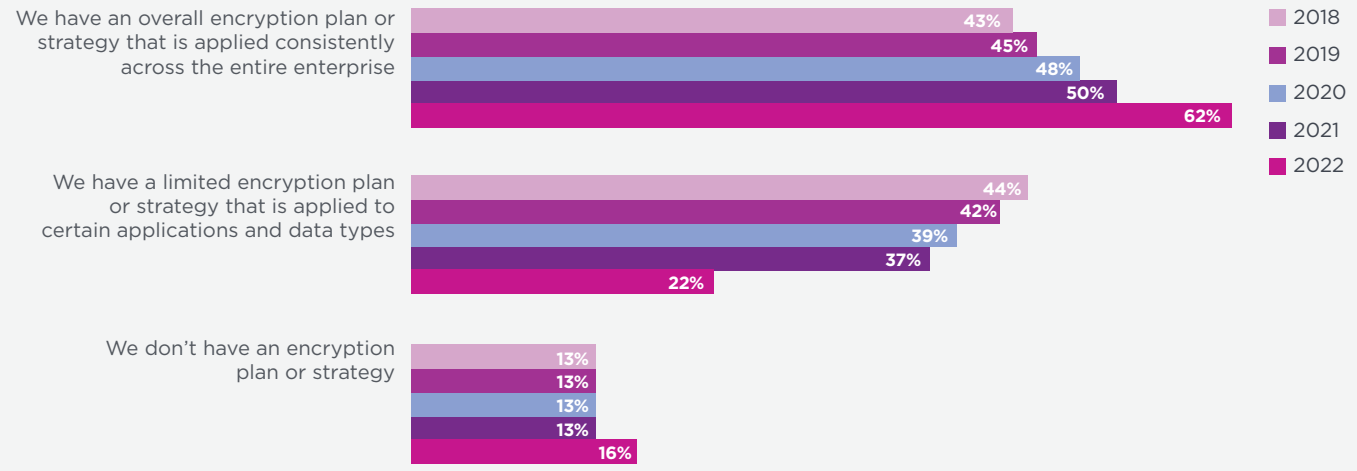
We surveyed 6,264 individuals across multiple industry sectors in 17 countries/regions – Australia, Brazil, France, Germany, Hong Kong, Japan, Mexico, the Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), Netherlands, the Russian Federation, Spain,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

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

Organizations with an overall encryption strategy increased significantly since last year. As shown in Figure 1, since 2018, the deployment of an overall encryption has steadily increased. This year, 62 percent of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise, a significant increase from last year. Only 22 percent of respondents say they have a limited encryption plan or strategy that is applied to certain applications and data types, a significant decrease from last year. The average annual global budget for IT security is $24 million per organization. The countries with the highest average annual budgets are the U.S. ($41 million) and Germany ($28 million).

Below are the findings from this year's research.

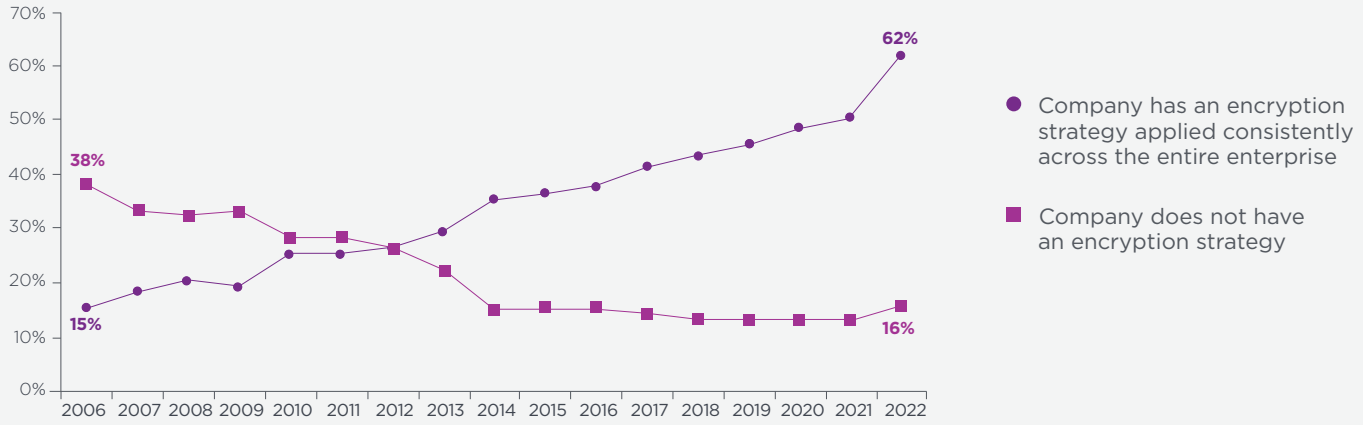
Figure 1. **Does your company have an encryption strategy?**
Country samples are consolidated.



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

Multi-cloud security. Are you in control or in the dark?

Trends in encryption strategy

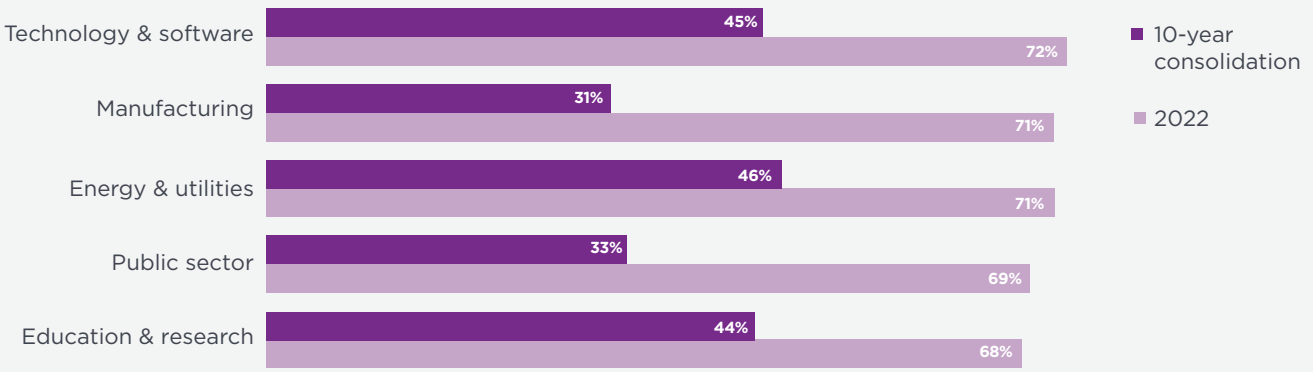


Enterprise-wide encryption strategies have continued to increase. Since conducting this study 17 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having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

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

Key industries prioritize data control.

Top 5 industries that use encryption.



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

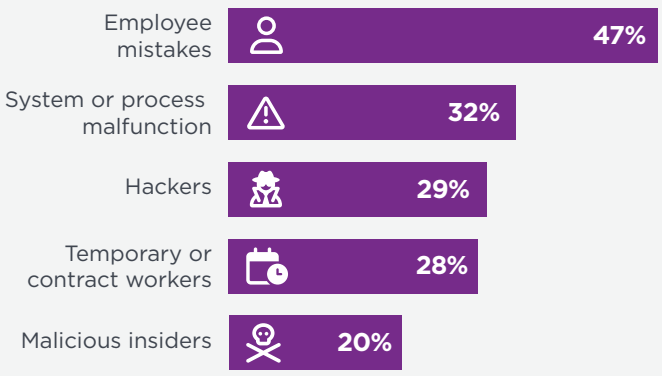
The use of encryption has increased in most industries. Results suggest a steady increase in most of the 13 industry sectors represented in this research. The most significant increases in extensive encryption usage occur in manufacturing, energy & utilities, and the public sector.

THREATS, MAIN DRIVERS, AND PRIORITIES

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

What (or who) puts your data security at risk?

Top 5 threats to sensitive data



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

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

The search continues:

Where does the data reside?

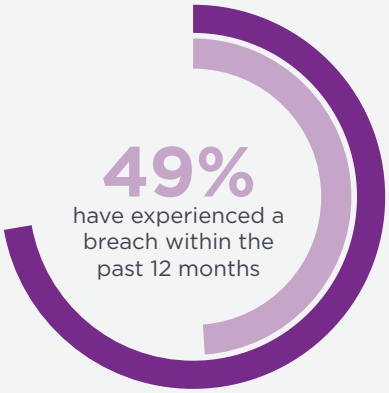
55% of respondents say discovering where data resides is the top challenge in an encryption strategy.

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

DEPLOYMENT CHOICES

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

Threats are on the rise.
It's not a matter of if. It's when. Are you prepared?



ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

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

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

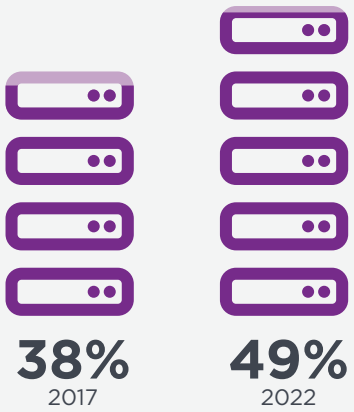
ATTITUDES ABOUT KEY MANAGEMENT

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

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

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

Does your organization use HSMs?



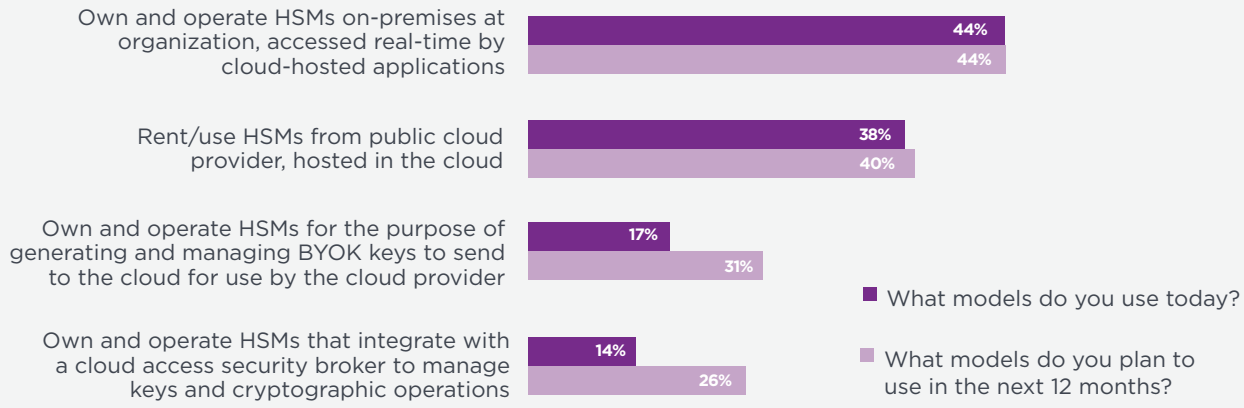
How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. Forty-four percent of respondents say their organizations own and operate HSMs on-premises, accessed real-time by cloud-hosted applications and 40 percent of respondents rent/use HSMs,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

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

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

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

Growing use of customer-controlled HSMs to support cloud use cases



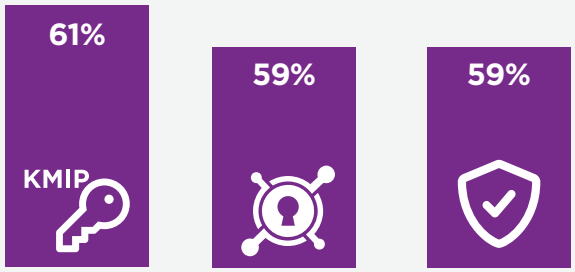
CLOUD ENCRYPTION

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

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

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

Most important cloud encryption features



Support for the KMIP standard

Granular access controls

SIEM integration, visualization, and analysis of logs

ABOUT PONEMON INSTITUTE

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries.

ABOUT ENTRUST

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

TO READ THE FULL REPORT VISIT:
ENTRUST.COM/C/GLOBAL-ENCRYPTION-TRENDS-STUDY

SECURING A WORLD IN MOTION

Learn more at entrust.com