Ponemon INSTITUTE

ENTRUST

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

2021 GLOBAL ENCRYPTION TRENDS STUDY

Executive Summary

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

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

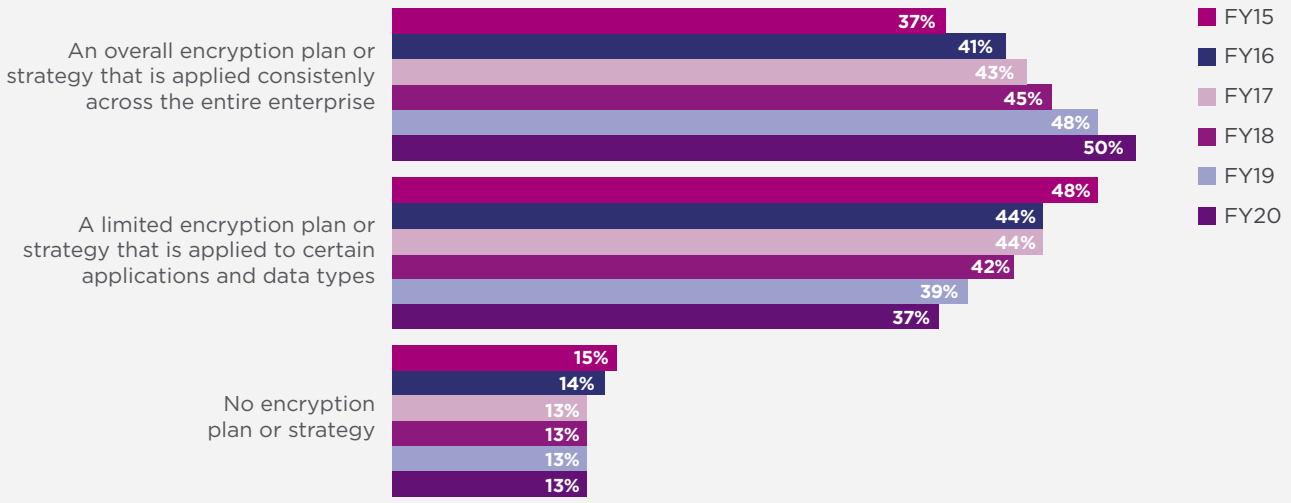
The purpose of this research is to examine how the use of encryption has evolved over the past 16 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a U.S. sample of respondents.[3]

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

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

Following are the findings from this year's research.

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



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

[2] Country-level results are abbreviated as follows: Australia (AU), Brazil (BZ), France (FR), Germany (DE), Hong Kong (HK), Japan (JP), Korea (KO), Mexico (MX), Middle East (AB), Netherlands (NL), Russia (RF), Spain (SP), Southeast Asia (SA), Sweden (SW), Taiwan (TW), United Kingdom (UK), and United States (US).

[3] The trend analysis shown in this study was performed on combined country samples spanning 16 years (since 2005).

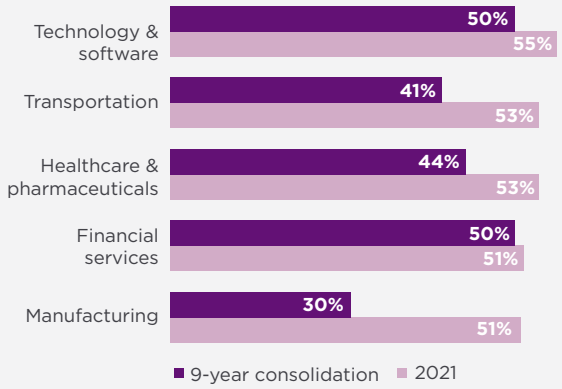
STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since conducting this study 16 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having an encryption plan or strategy. The results have essentially reversed over the years of the study.

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

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

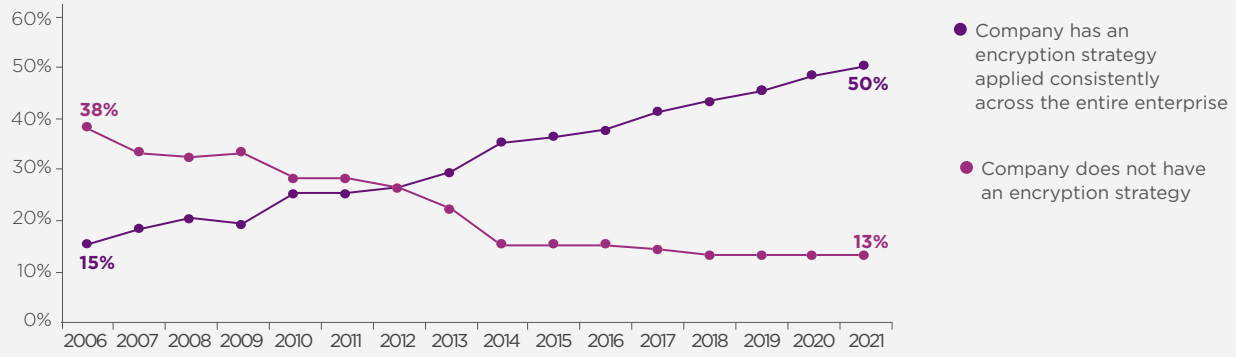
On the rise: The growing use of encryption – top 5 industries



TRENDS IN ADOPTION OF ENCRYPTION

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

Your data is in the clouds. Is your encryption strategy up in the air?
Trends in encryption strategy



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

THREATS, MAIN DRIVERS AND PRIORITIES

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

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

Mistake or malice: The results are the same
Top 6 threats to sensitive data

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

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

Who will be first to find your unencrypted data?

65% of respondents say discovering where sensitive data resides is the top challenge to an encryption strategy

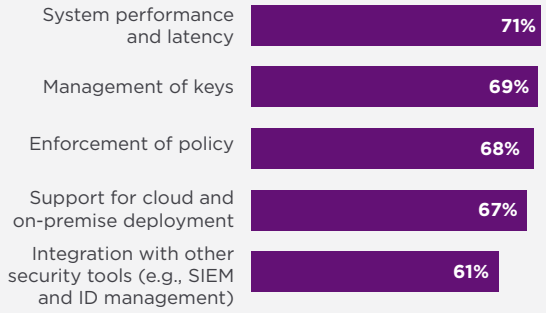
DEPLOYMENT CHOICES

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

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.

Must-haves for data protection
Top 5 most important feature of encryption solutions



Which data types are most often encrypted? Payment-related data and financial records are most likely to be encrypted as a result of high-profile data breaches in financial services. The least likely data type to be encrypted is health-related information and non-financial information, which is a surprising result given the sensitivity of health information.

ATTITUDES ABOUT KEY MANAGEMENT

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

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

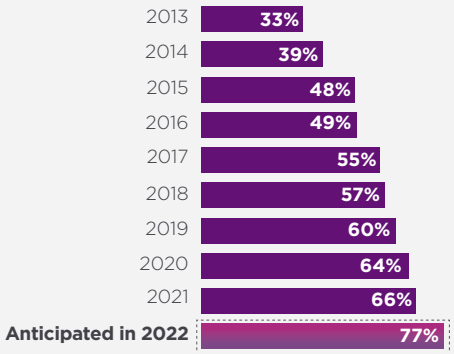
IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

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

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

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

The keys to success
Ratings of the importance of HSMs to an organization's encryption and key management strategy



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

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

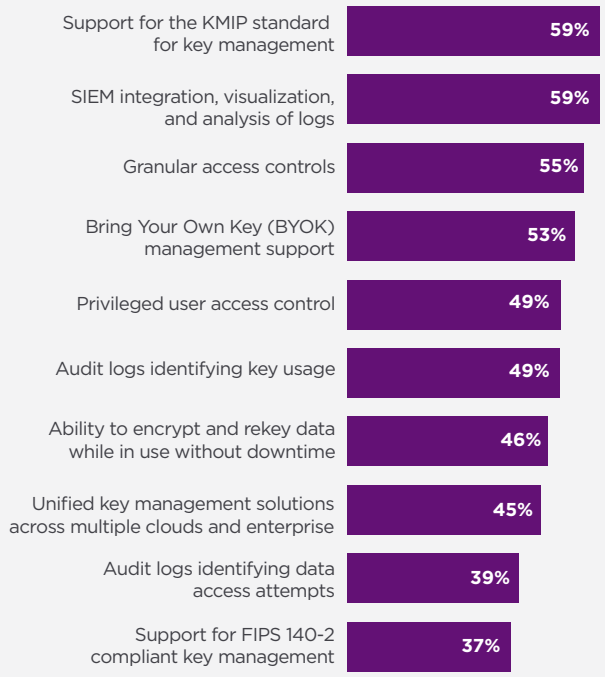
CLOUD ENCRYPTION

Sixty percent of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking. Another 24 percent of respondents expect to do so in the next one to two years. These findings indicate the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

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

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

Solving multi-cloud data protection challenges
Top 10 most important cloud encryption features



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/GO/2021-GETS

ENTRUST

SECURING A WORLD IN MOTION

Learn more at entrust.com