Entrust Datacard®

nCIPHER
AN ENTRUST DATACARD COMPANY

2020 GLOBAL ENCRYPTION TRENDS STUDY

Executive Summary

Ponemon INSTITUTE

PONEMON INSTITUTE PRESENTS THE FINDINGS OF THE 2020 GLOBAL ENCRYPTION TRENDS STUDY[1]

We surveyed 6,457 individuals across multiple industry sectors in 17 countries - Australia, Brazil, France, Germany, Hong Kong, India, Japan, Mexico, the Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), Netherlands, the Russian Federation, Southeast Asia, South Korea, Sweden, Taiwan, the United Kingdom, and the United States.[2]

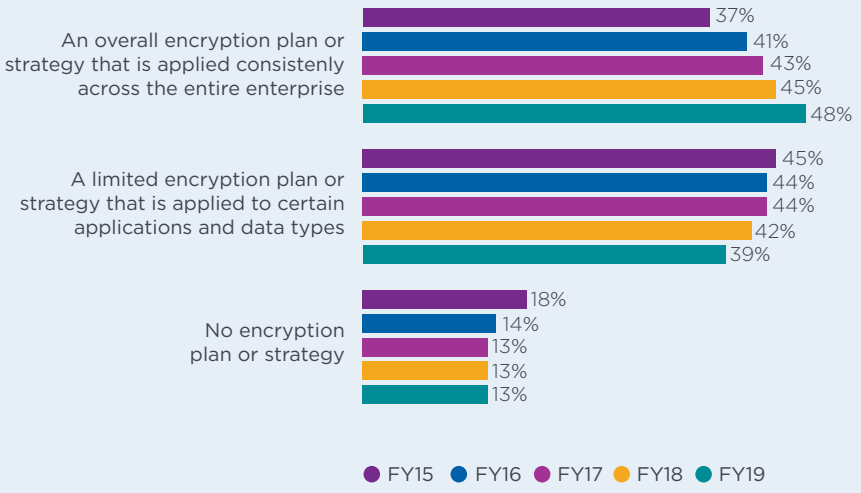
The purpose of this research is to examine how the use of encryption has evolved over the past 15 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a US sample of respondents.[3]

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, 48 percent of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise and 39 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 2019 and completed in January 2020. 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 2019.

[2] Country-level results are abbreviated as follows: Australia (AU), Brazil (BZ), France (FR), Germany (DE), Hong Kong (HK), India (IN), Japan (JP), Korea (KO), Mexico (MX), Middle East (AB), Netherlands (NL), Russia (RF), 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 15 years (since 2005).

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since conducting this study 15 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, Sweden and Hong Kong. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 48 percent.

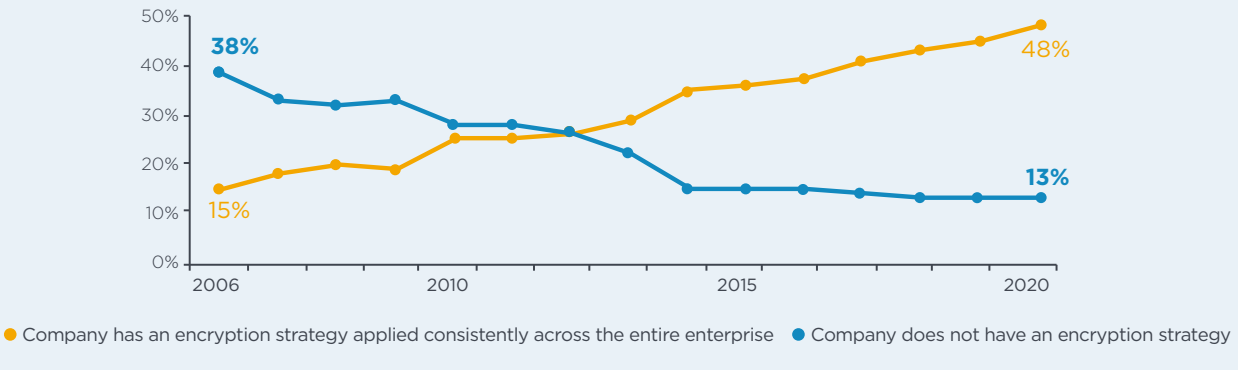
The IT operations function is the most influential in framing the organization's encryption strategy over the past 14 years. However, in the United States, lines of business are more influential (30 percent of respondents). IT operations and IT security have a similar level of influence in the United States and Mexico.

TRENDS IN ADOPTION OF ENCRYPTION

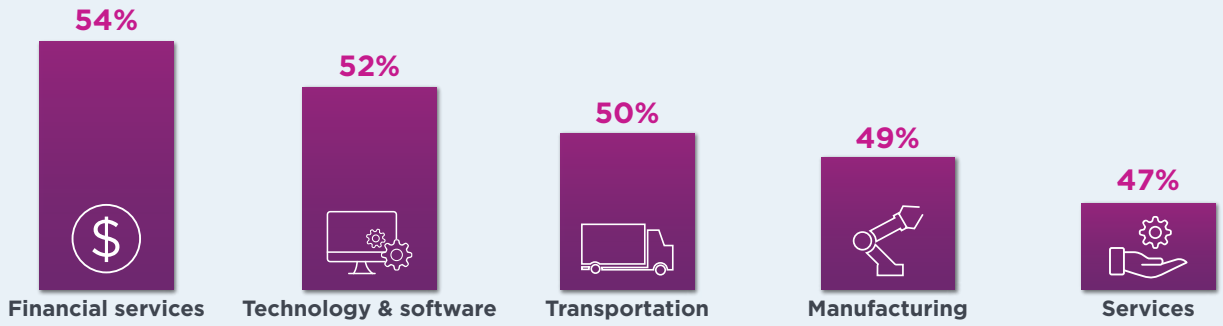
The use of encryption increases in all industries. Results suggest a steady increase in all industry sectors, with the exception of healthcare and pharmaceutical. The most significant increases in extensive encryption usage occur in manufacturing, hospitality and consumer products.

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.

Trends in encryption strategy over the past 15 years



Top 5 industries that use encryption



THREATS, MAIN DRIVERS AND PRIORITIES

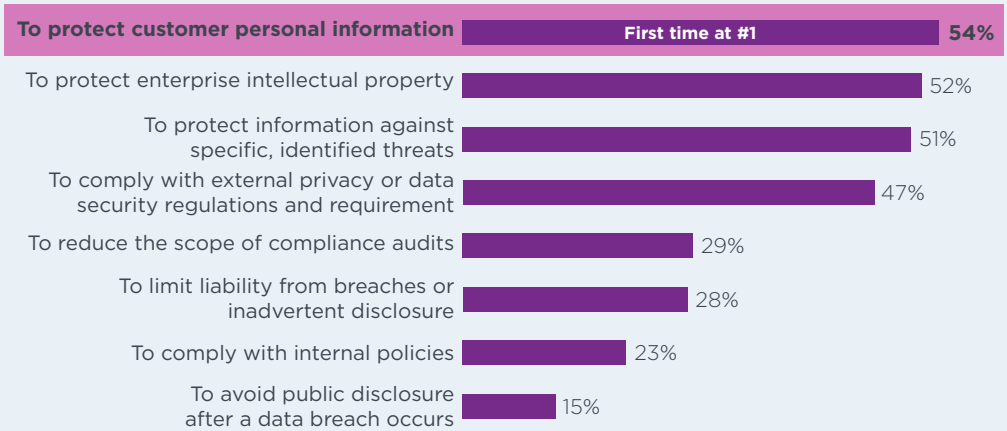
Employee mistakes continue to be the most significant threats to sensitive data. The most significant threats to the exposure of sensitive or confidential data are employee mistakes. In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping 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.

The main driver for encryption is the protection of customer's personal information. Organizations are using encryption for protection of customers' personal information (54 percent of respondents), the protection of enterprise intellectual property (52 percent of respondents) and protection against specific, identified threats (51 percent of respondents).

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

Top threats to sensitive data

Main drivers for using encryption technology



DEPLOYMENT CHOICES

No single encryption technology dominates in organizations. Organizations have very diverse needs. Internet communications, databases and laptop hard drives are the most likely to be deployed and correspond to mature use cases. For the third year, the study tracked the deployment of encryption of IoT devices and platforms/data repositories. Sixty percent of respondents say encryption is at least partially deployed for IoT devices, and 61 percent of respondents say encryption of IoT platforms/data repositories is at least partially deployed.

ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

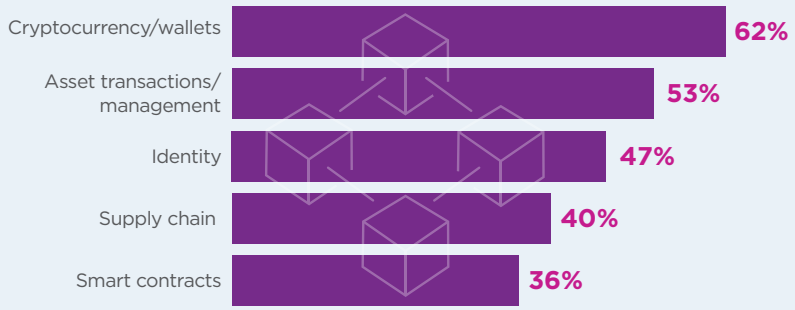
Certain encryption features are considered more critical than others. According to the consolidated findings, system performance and latency, enforcement of policy and support for both cloud and on-premise deployment are the three most important encryption features.

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 types to be encrypted are non-financial business information and health-related information, which is a surprising result given the sensitivity of health information.

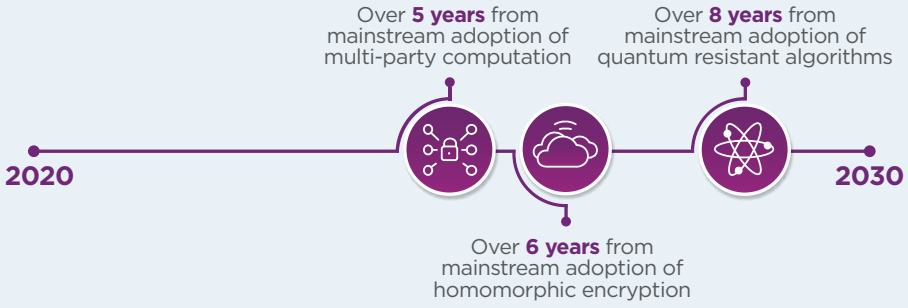
Most companies plan to use blockchain. Sixty percent of respondents say their organizations will use blockchain. The two primary use cases are for cryptocurrency/wallets and asset transactions/management.

Newer encryption technologies are at least 5 years from mainstream adoption. Respondents were asked when they believe homomorphic encryption, multi-party computation, and quantum algorithms will achieve mainstream enterprise adoption. The solution expected to achieve adoption the soonest is multi-party computation.

60% of organizations plan to use blockchain. The top 5 use cases are:



When will we see mainstream adoption of new encryption technology?
Enterprises project that we are:



ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management? Sixty 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 67 percent occurs in Germany. At 38 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.

Companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) formal key management infrastructure (KMI), (2) formal key management policy (KMP), and (3) manual processes.

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMS)

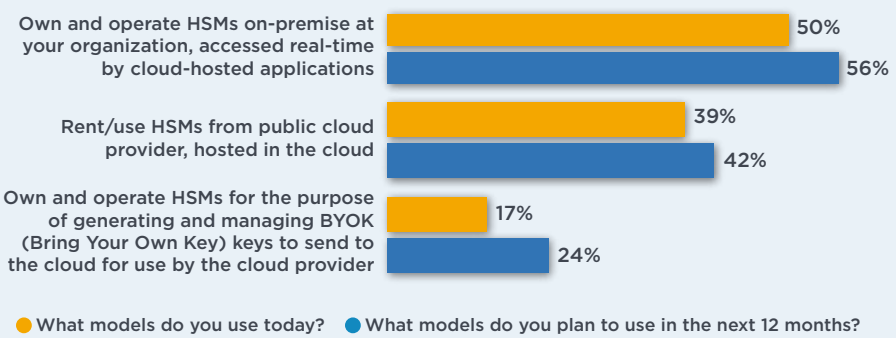
Germany, the United States and Middle East organizations are more likely to deploy HSMs. Germany, the United States and the Middle East are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 48 percent.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. Fifty 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. In the next 12 months, both figures will increase. The use of HSMs with Cloud Access Security Brokers and the ownership and operation of HSMs for the purpose of generating and managing keys to send to the cloud for use by the cloud provider 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 64 percent. The pattern of responses suggests Australia, Germany and the United States are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

What best describes an organization's use of HSMs? Fifty-nine 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-one 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's the role of Hardware Security Modules (HSMs) with cloud applications?



What are the primary purposes or uses for HSMs? The two top uses are application-level encryption and TLS/SSL, followed by public cloud encryption, including for BYOK (Bring Your Own Key). There is a significant increase forecast in the use of database encryption 12 months from now. It is significant to note that HSM use for application-level encryption will soon be deployed in 51 percent of the organizations represented in this study.

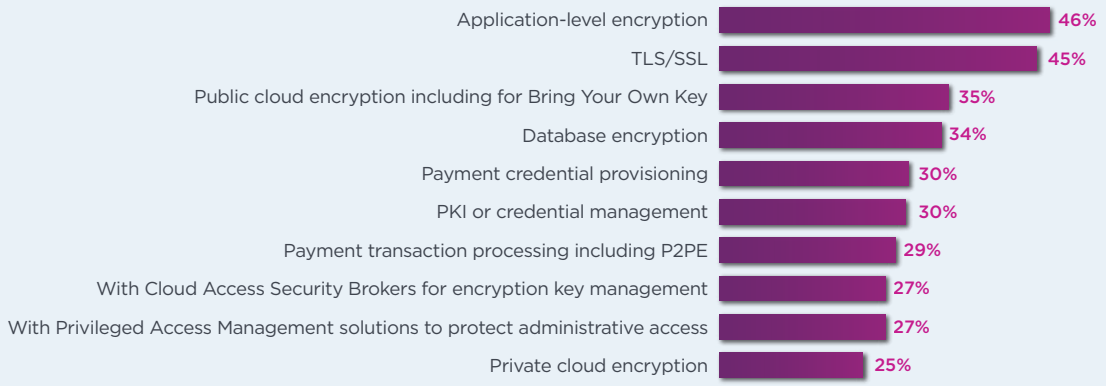
CLOUD ENCRYPTION

Fifty-eight 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 25 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.

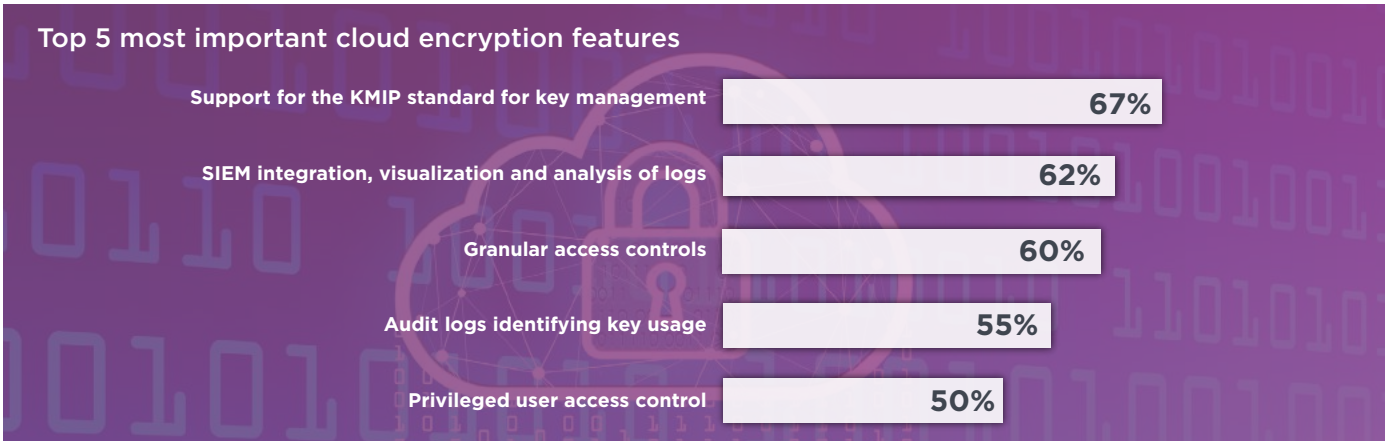
How do organizations protect data at rest in the cloud? Forty-five percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 36 percent of respondents perform encryption in the cloud, with cloud provider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

What are the top three cloud encryption features? The top three features are support for the KMIP standard for key management (67 percent of respondents), SIEM integration, visualization and analysis of logs (62 percent of respondents) and granular access controls (60 percent of respondents).

The top 10 use cases for Hardware Security Modules (HSMs) in 2020



Top 5 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 NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. **www.ncipher.com**

ABOUT ENTRUST DATACARD

Employees, citizens and consumers increasingly expect anywhere-anytime experiences — whether they are logging on to corporate networks, crossing borders, accessing e-gov services or making purchases. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible. Our 45+ years of industry-leading expertise and experience spans the globe, with more than 2,000 employees serving customers in 150 countries worldwide. For more information, visit **www.entrustdatacard.com**

CLICK TO DOWNLOAD FULL REPORT