THALES

Ponemon INSTITUTE

GLOBAL ENCRYPTION TRENDS STUDY

April 2018

EXECUTIVE SUMMARY

Ponemon Institute is pleased to present the findings of the *2018 Global Encryption Trends Study*,[1] sponsored by Thales eSecurity. We surveyed 5,252 individuals across multiple industry sectors in 12 countries: Arabia (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates)[2], Australia, Brazil, France, Germany, India, Japan, Mexico, the Russian Federation, the United Kingdom, the United States and, for the first time, South Korea (hereafter referred to as Korea).

The purpose of this research is to examine how the use of encryption has evolved over the past 13 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.

43%

of organizations now have a consistent, enterprise-wide **encryption strategy**

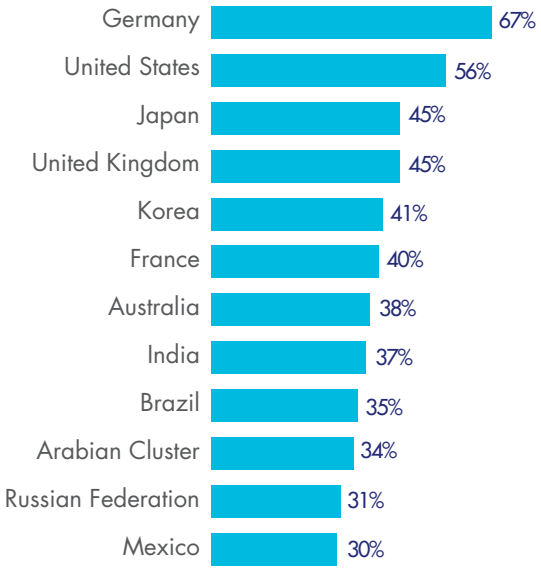
More organizations represented in this research continue to recognize the importance of having an encryption strategy, either an enterprise-wide (43 percent of respondents) strategy or a limited plan that targets certain applications and data types (44 percent of respondents).

Strategy and adoption of encryption

Enterprise-wide encryption strategies increase. Since conducting this study 13 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 highest prevalence of an enterprise encryption strategy is reported in Germany followed by the U.S. and Japan. Respondents in Mexico, Russian Federation, Arabia, Brazil and Australia report the lowest adoption of an enterprise encryption strategy.

Countries with the most/least mature encryption strategies



[1] This year's data collection was completed in January 2018. Throughout the report we present trend data based on the fiscal year (FY) the survey commenced rather than the year the report is finalized. Hence, our most current findings are presented as FY17. The same dating convention is used in prior years.

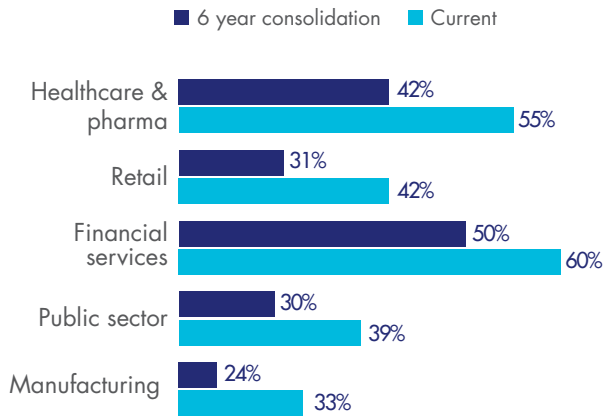
[2] Country-level results are abbreviated as follows: Arabian cluster (AB), Australia (AU), Brazil (BZ), France (FR), Germany (DE), India (IN), Japan (JP), Korea (KO), Mexico (MX), Russia (RF), United Kingdom (UK), and United States (U.S.).

[3] The trend analysis shown in this study was performed on combined country samples spanning 13 years (since 2005).

IT operations function is the most influential in framing an organization's encryption strategy. However, in some countries lines of business are more influential. These are the United States, Australia and Mexico. IT security and IT operations have a similar level of influence in the United States, Australia and Mexico.

The use of encryption increases in all industries. We looked at the extensive usage of encryption solutions for 10 industry sectors over seven years. Results suggest a steady increase in all industry sectors. The most significant increases in extensive encryption usage occur in healthcare & pharmaceutical, retail and financial services.

The top 5 growing industries



Threats, main drivers and priorities

Employee mistakes are the most significant threat to sensitive data. 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 workers and malicious insiders. It is interesting to note that the employee mistake threat is almost equal to the combined threat by both hackers and insiders.

"Encryption challenges have remained steady, with the exception of sensitive data discovery, which has increased significantly in response to compliance activities."

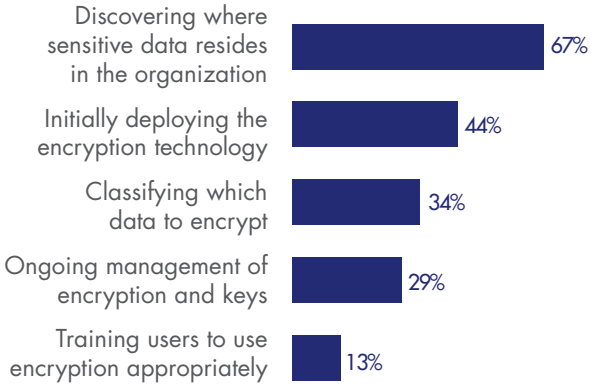
—Larry Ponemon, Chairman and Founder of the Ponemon Institute

The main driver for encryption is protection of information against identified threats. Organizations are using encryption to protect information against specific, identified threats (54 percent of respondents). The most critical information is the enterprise's intellectual property and the personal information of customers (52 percent and 50 percent of respondents, respectively). Compliance with regulations remains a significant driver for encryption, according to 49 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. This challenge has come into focus as compliance activities driven by GDPR and other privacy regulations have increased. In addition, 44 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-four percent cite classifying which data to encrypt as difficult.

Why organizations are challenged by encryption

Respondents from the U.K., Germany, the U.S., and France indicated the highest data discovery challenge levels



Deployment choices

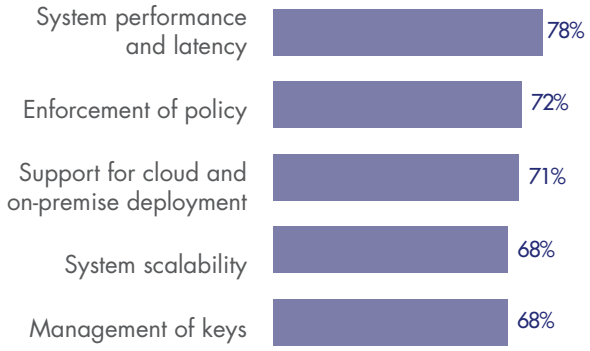
No single encryption technology dominates in organizations. Organizations have very diverse needs. Internet communications, databases and laptop hard drives are the most likely to be encrypted and correspond to mature use cases. For the first time, the study tracked the deployment of encryption on IoT devices and platforms. Forty-nine percent of respondents say IoT encryption has been at least partially deployed on both IoT devices and IoT platforms.

Encryption features considered most important

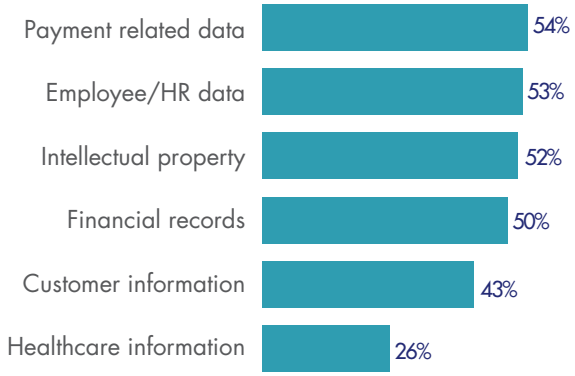
Certain encryption features are considered more critical than others. According to consolidated findings, system performance and latency, enforcement of policy and support for both cloud and on-premise deployment are the three most important features. Support for both cloud and on-premise deployment has risen in importance as organizations have increasingly embraced cloud computing and look for consistency across computing styles.

Which data types are most often encrypted? Payment related data and human resource data are most likely to be encrypted – which emphasizes the fact that encryption has now moved into the realm where it needs to be addressed by companies of all types. The least likely data types to be encrypted are health-related information and non-financial information, which is a surprising result given the sensitivity of health information and recent high profile healthcare data breaches. Healthcare information did, however, have the largest increase on this list over last year.

How important are specific features



What data organizations encrypt

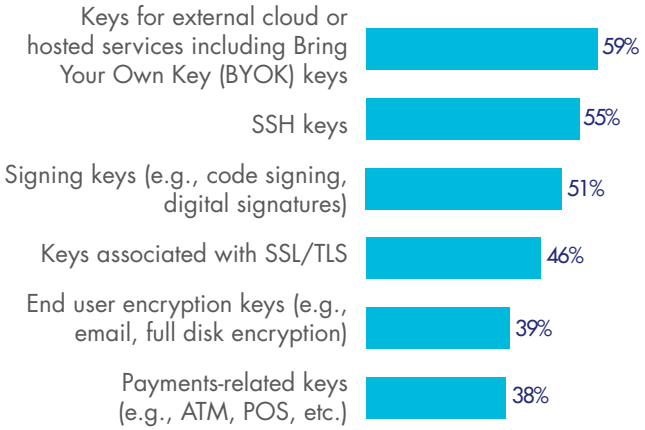


IoT ENCRYPTION IS EMERGING: " FORTY-NINE PERCENT OF RESPONDENTS SAY ENCRYPTION HAS BEEN AT LEAST PARTIALLY DEPLOYED ON BOTH IoT DEVICES AND IoT PLATFORMS."

Attitudes about key management

How painful is key management? Fifty-seven percent of respondents rate key management as very painful. The average percentage in all country samples is 57 percent, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 65 percent occurs in India. At 33 percent, the lowest pain level occurs in Russia.

Key management continues to be a source of pain, with keys for cloud services rated as most difficult to manage

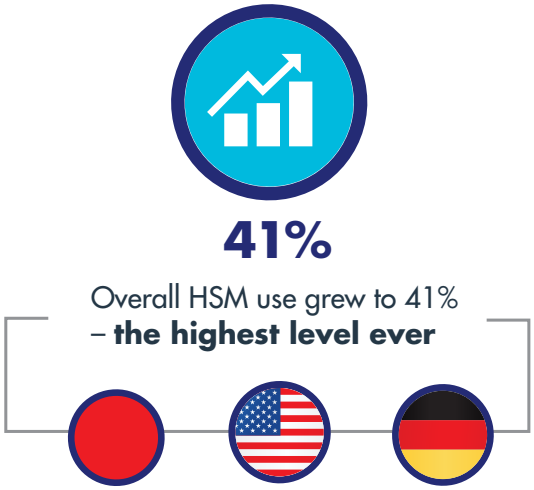


Companies continue to use a variety of key management systems. Although the use of manual key management processes continues to decrease, manual processes continue to be the most common form of key management systems. The next most commonly deployed systems are formal key management policy and formal key management infrastructure (KMI).

Importance of hardware security modules (HSMs)

Germany, U.S. and Japan organizations are more likely to deploy HSMs. Germany, U.S. and Japan are more likely to deploy HSMs for their organization's key management activities than other countries. The overall average deployment rate for HSMs is 41 percent.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. Forty-seven percent of respondents own and operate HSMs on-premise for cloud-based applications, and 36 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, both figures will increase, by 6 and 5 percent respectively. Interestingly, the use of HSMs with Cloud Access Security Brokers is expected to double in the next 12 months.



The overall average importance rating for HSMs, as part of an encryption and key management strategy, in the current year is 57 percent. The pattern of responses suggests Germany, India, U.S. and Japan are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

HSMs are increasingly important to an encryption and key management strategy

HSMs were rated as either *very important or important* **today** by 57% of respondents

HSMs were rated as either *very important or important* **over the next 12 months** by 65% of respondents

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. More respondents indicate the centralized approach in this year's study as compared to last year's.

What are the primary purposes or uses for HSMs? The two top uses are SSL/TLS and application-level encryption, followed by database encryption. The most significant increases predicted for the next 12 months, according to respondents, are SSL/TLS, database encryption and payment transaction processing. It is significant to note that HSM use for SSL/TLS will soon be deployed in 50 percent of the organizations represented in this study.

Budget allocations

The proportion of IT spending dedicated to security activities, including encryption, is increasing over time. According to the findings, 10.6 percent of the IT budget goes to IT security activities and 12.3 percent of the IT security budget goes to encryption activities.

Cloud encryption

61%
of respondents are using more than one **public cloud provider**

Sixty-one 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 21 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.

84%
of respondents either use the cloud for **sensitive/non-sensitive applications and data** today, or will do so in the next 12-24 months

How do organizations protect data at rest in the cloud? Forty-seven percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 38 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.

39%
Encryption in public cloud services grew from 28% to 39% in 2017 – 11% is the highest year-over-year growth of any encryption use case

What are the top three cloud encryption features? When asked specifically about features associated with cloud encryption, respondents list (1) Support for the KMIP standard for key management (66 percent of respondents), (2) SIEM integration and visualization and analysis of logs (62 percent of respondents) and (3) granular access controls (60 percent of respondents). This indicates a growing recognition of the importance of standards-based cloud key management and specifically support for KMIP.

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 Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and, with the internet of things (IoT), even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

About Thales

The people we all rely on to make the world go round – they rely on Thales. Our customers come to us with big ambitions: to make life better, to keep us safer. Combining a unique diversity of expertise, talents and cultures, our architects design and deliver extraordinary high technology solutions. Solutions that make tomorrow possible, today. From the bottom of the oceans to the depth of space and cyberspace, we help our customers think smarter and act faster – mastering ever greater complexity and every decisive moment along the way. With 65,000 employees in 56 countries, Thales reported sales of €15.8 billion in 2017.

TO READ THE FULL REPORT VISIT:
GETS.THALESESECURITY.COM

OUR SPONSORS

VENAFI

GEOBRIDGE

cloud security alliance SM

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com