THALES

Ponemon INSTITUTE

JAPAN ENCRYPTION TRENDS STUDY

September 2018

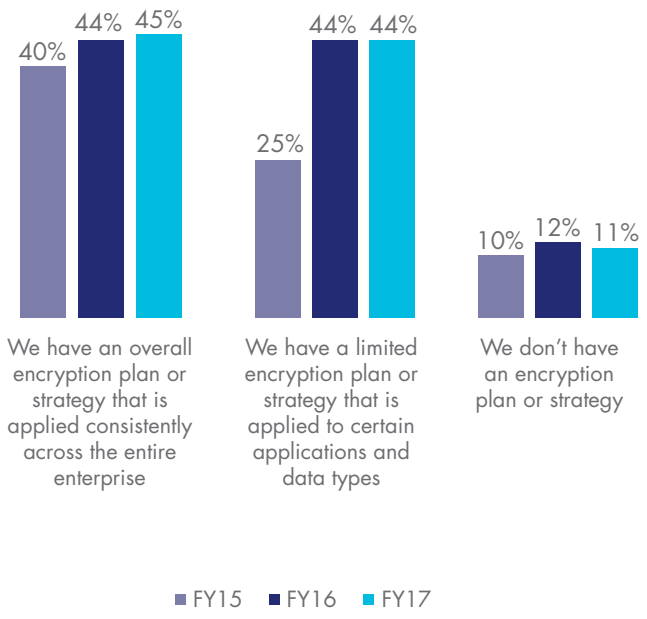
EXECUTIVE SUMMARY

Ponemon Institute is pleased to present the findings of the *2018 Japan Encryption Trends Study*, sponsored by Thales eSecurity. We surveyed 468 individuals in Japan to examine the use of encryption and the impact of this technology on the security posture of organizations in this region.

The first encryption trends study was conducted in 2005 for a U.S. sample of respondents. Since then, we have expanded the scope of the research to include respondents in 11 countries, plus Japan. The 11 countries include the following: Australia, Brazil, France, Germany, India, Mexico, the Middle East[1], the Russian Federation, South Korea, the United Kingdom, and the United States.

As shown in Figure 1, more of the organizations represented in this research continue to recognize the importance of having an encryption strategy, either an enterprise-wide strategy (45 percent of respondents) or a limited strategy that targets certain applications and data types (44 percent of respondents).

Figure 1. What best describes your organization's encryption strategy?



Following is a summary of our key findings. More details are provided in the next section of this report for each key finding listed below.

IT operations increases its influence in directing encryption strategies. While responsibility for the encryption strategy is dispersed throughout the organization, IT operations increased its influence from 41 percent of respondents last year to 45 percent of respondents in this year's research. In contrast, lines of business influence decreased from 31 percent of respondents to 27 percent of respondents.

Which data types are most often encrypted? More companies are encrypting intellectual property and financial records. Fewer companies are encrypting employee/HR information than in previous years.

Employee mistakes and hackers are the top two threats to sensitive data. The most significant threats to the exposure of sensitive or confidential data are employee mistakes and hackers, according to 55 percent and 43 percent of respondents. Forty percent of respondents say a system or process malfunction is a top threat.

Threats to sensitive data

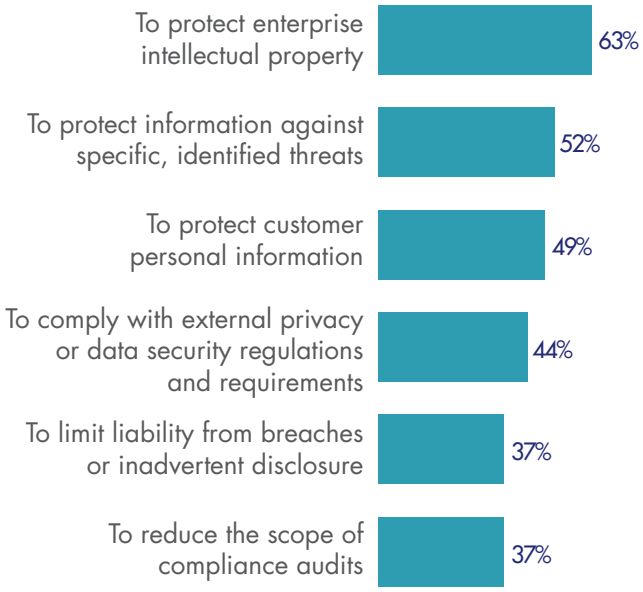
[1] The Middle East region includes the United Arab Emirates and Saudi Arabia.

45%

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

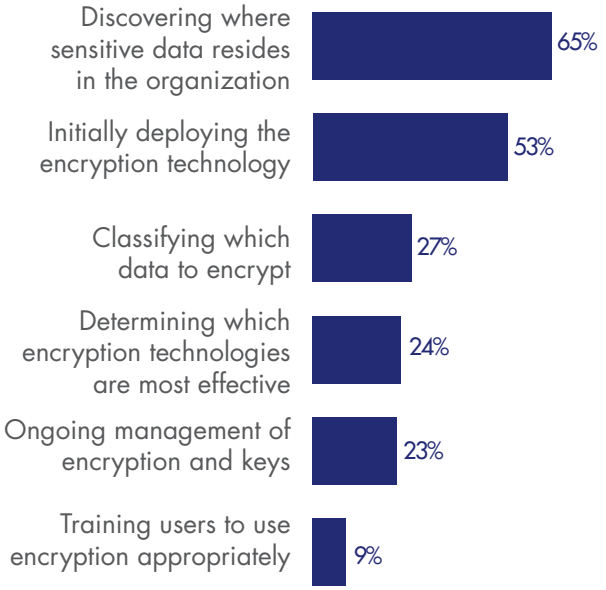
Protection of intellectual property is the main driver for using encryption technologies. According to 63 percent of respondents, the primary reason for encryption is to protect enterprise intellectual property, and 52 percent of respondents say encryption is used to protect information against specific, identified threats.

What are the drivers for encryption?



Discovering where sensitive data resides in the organization continues to be the biggest challenge. The challenge of discovering where sensitive data resides in the organization is the biggest challenge in planning and executing a data encryption strategy, according to 65 percent of respondents. The second biggest challenge, as noted by 53 percent of respondents, is the initial deployment of encryption technology.

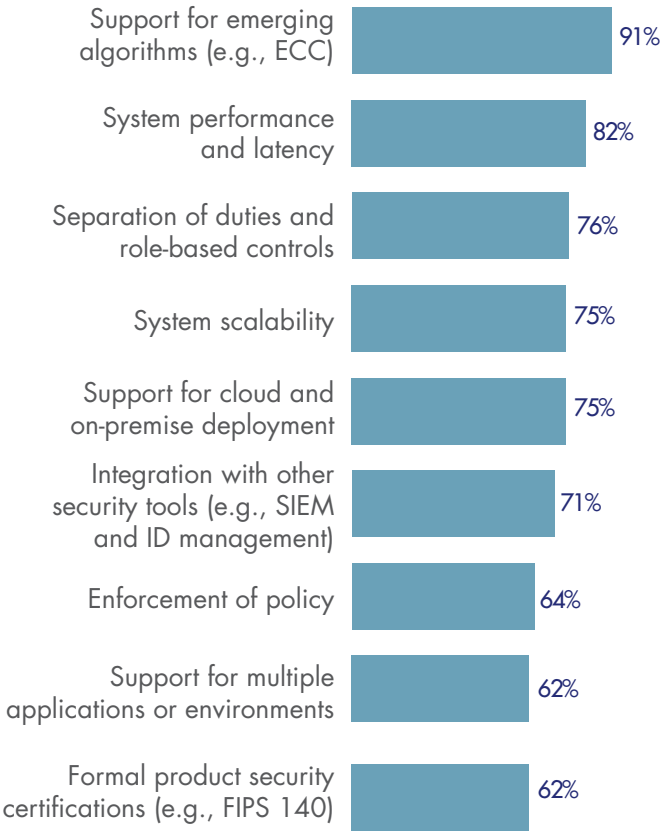
Why organizations are challenged by encryption



No single encryption technology dominates because organizations have very diverse needs. Encryption of Internet communications, backup and archives, and laptop hard drives are most likely to be extensively deployed. In contrast, Internet of Things (IoT) platforms and devices, a nascent but emerging use case, and Docker containers are less likely to be fully or partially deployed.

Certain encryption features are considered more critical than others. During the past three years, the following features have increased in importance: support for emerging algorithms, system performance and latency, separation of duties and role-based controls, integration with other security tools, formal product security certifications and support for regional segregation. Features that have decreased in importance yet remain important are system scalability (75 percent of respondents) and support for multiple applications or environments (62 percent of respondents).

How important are specific features?



How painful is key management? Fifty-two percent of respondents report the management of keys is painful. The top reasons for the pain are: systems are isolated and fragmented, no clear understanding of requirements and no clear ownership.

"Fifty-two percent of respondents report the management of keys is painful. The top reasons for the pain are: systems are isolated and fragmented, no clear understanding of requirements and no clear ownership."

Which keys are most difficult to manage? The pain of managing SSH keys has increased significantly since last year. These keys have decreased in difficulty: signing keys (e.g., code signing, digital signatures), end user encryption keys and encryption keys for backups and storage.

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

The importance of HSMs to an encryption or key management strategy will see significant growth in the next 12 months. We asked respondents in organizations that currently deploy HSMs how important they are to their encryption or key management strategy. Sixty-three percent of respondents say they are important today, and 70 percent of respondents say they will be important in the next 12 months. SSL/TLS, database encryption, payment credential provisioning and issuing, and payment service provider interface are use cases that are expected to increase. Payment transaction processing including P2PE, private cloud encryption, and cloud access security brokers (CASBs) for encryption key management are use cases expected to decrease.

63%

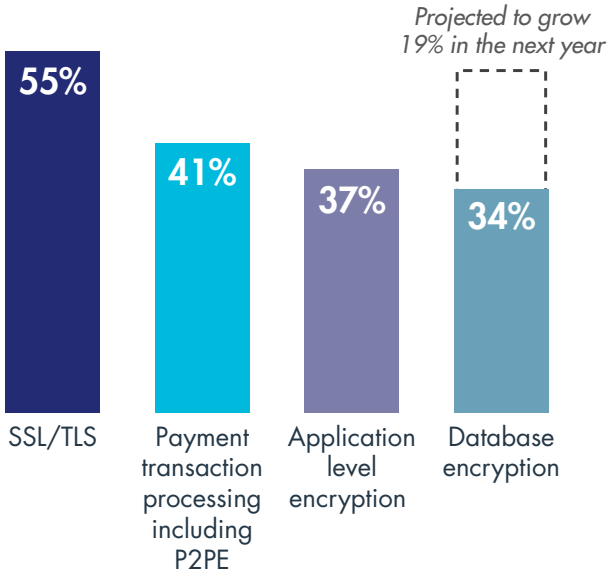
HSMs were rated as either *very important or important* **today** by 63% of respondents

76%

will use **multiple public cloud providers** in the next two years

How organizations are using HSMs. Sixty-five percent of respondents say they have a centralized team that provides cryptography as a service. The global average is 61 percent. Thirty-five percent of respondents say that each individual application owner/team is responsible for their own cryptographic services.

The most prevalent use cases for HSMs



Most organizations transfer sensitive or confidential data to the cloud. Sixty-eight percent of respondents say their organizations currently transfer sensitive or confidential data to the cloud (regardless of whether it is encrypted or made unreadable via some other mechanism), and 14 percent of respondents plan to do so in the next 12 to 24 months. Forty-five percent of respondents say the cloud provider is the most responsible for protecting sensitive or confidential data transferred to the cloud.

74%

of respondents either extensively or partially **encrypt in public cloud services**

How is data at rest in the cloud protected? Forty percent of respondents say encryption is performed on-premises prior to sending data to the cloud using keys the organization generates and manages, and 38 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider.

"Forty percent of respondents say encryption is performed on-premises prior to sending data to the cloud using keys the organization generates and manages."

47%

Overall HSM usage in Japan is 47%

This is ***6% higher*** than the global average

"SIXTY-EIGHT PERCENT OF RESPONDENTS SAY THEIR ORGANIZATIONS CURRENTLY TRANSFER SENSITIVE OR CONFIDENTIAL DATA TO THE CLOUD (REGARDLESS OF WHETHER IT IS ENCRYPTED OR MADE UNREADABLE VIA SOME OTHER MECHANISM), AND 14 PERCENT OF RESPONDENTS PLAN TO DO SO IN THE NEXT 12 TO 24 MONTHS."

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 a 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.

CLICK HERE TO READ THE FULL REPORT

OUR SPONSORS

VENAFI

GEOBRIDGE

cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com