THALES

Ponemon INSTITUTE

FRANCE ENCRYPTION TRENDS STUDY

September 2018

EXECUTIVE SUMMARY

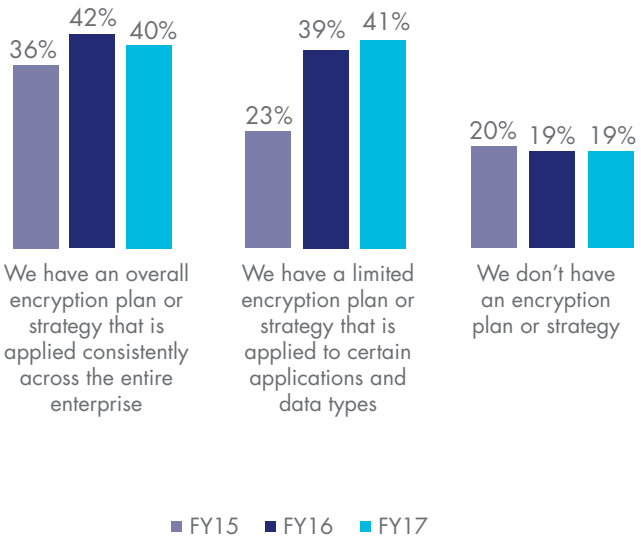
Ponemon Institute is pleased to present the findings of the *2018 France Encryption Trends Study*, sponsored by Thales eSecurity. We surveyed 370 individuals in France to examine the use of encryption and the impact of this technology on the security posture of organizations in this region.

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 12 countries including France. The countries include the following: Australia, Brazil, France, Germany, India, Japan, Mexico, the Middle East, the Russian Federation, South Korea, the United Kingdom, and the United States.[1]

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 (40 percent of respondents) or a limited strategy that targets certain applications and data types (41 percent of respondents).

Following is a summary of our key findings.

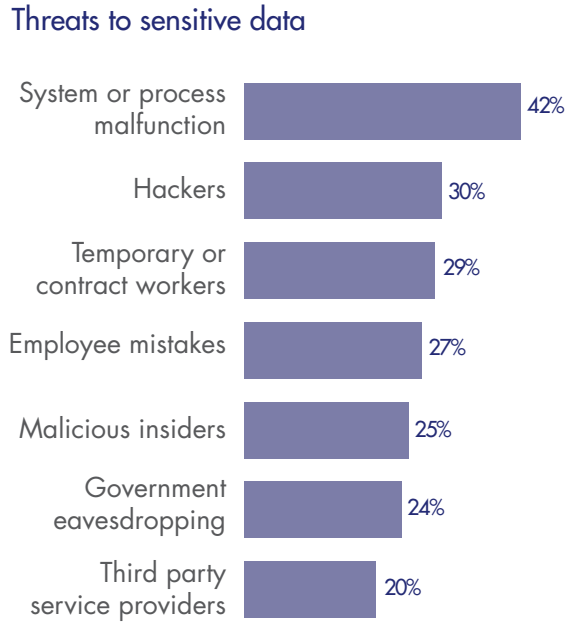
Figure 1. What best describes your organization's encryption strategy?



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 26 percent of respondents last year to 38 percent of respondents in this year's research. In contrast, lines of business influence decreased from 41 percent of respondents to 25 percent of respondents.

Which data types are most often encrypted? More companies are encrypting payment-related data, intellectual property, financial records, employee/HR data, customer information and healthcare information. Fewer companies are encrypting non-financial business information.

A system or process malfunction is the main threat to the exposure of sensitive or confidential data. According to 42 percent of respondents, the most significant threat to the exposure of sensitive or confidential data is system or process malfunctions. Thirty percent of respondents say hackers pose the greatest threat, while 29 percent of respondents say temporary or contract workers pose the greatest threat.



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

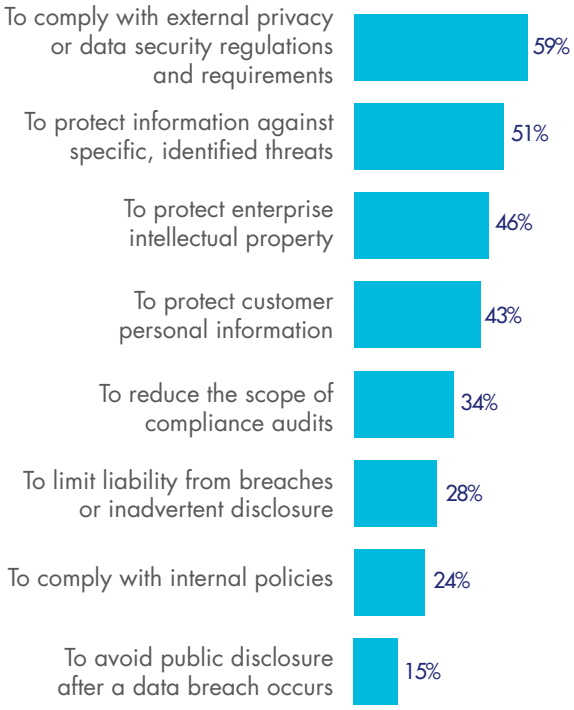
40%

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

Companies in France encrypt sensitive data at rates that exceed global averages

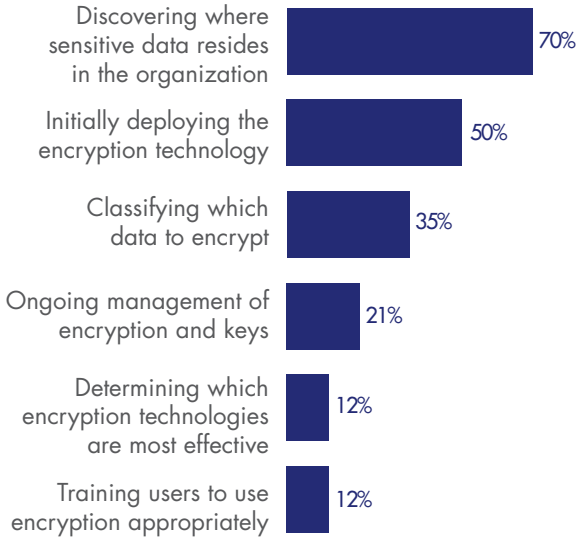
Compliance with privacy and data security regulations is the main driver for using encryption technologies. According to 59 percent of respondents, the importance of compliance with external privacy or data security regulations and requirements continues to be the top driver. Fifty-one percent and 46 percent of respondents say the protection of information against specific threats and protection of enterprise intellectual property are drivers.

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 70 percent of respondents. The second biggest challenge, as noted by 50 percent of respondents, is the initial deployment of encryption technology.

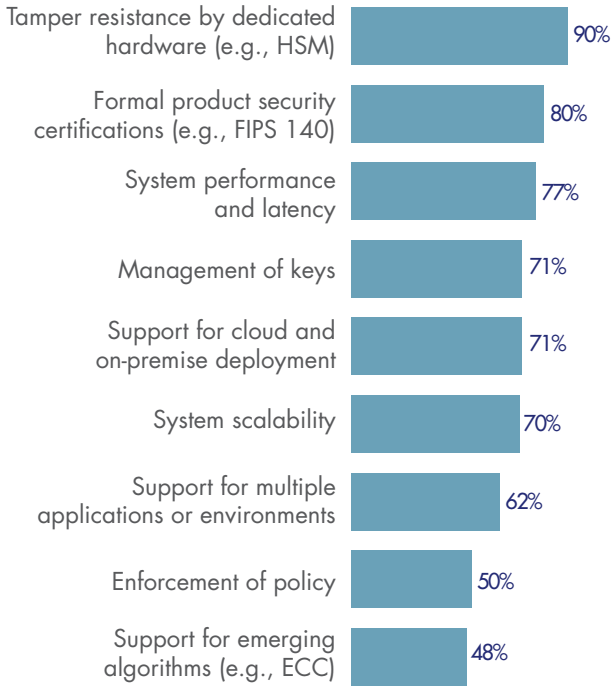
Why organizations are challenged by encryption



No single encryption technology dominates because organizations have very diverse needs. Encryption of laptop hard drives, Internet communications, and backups and archives 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 encrypted.

Certain encryption features are considered more critical than others. During the past three years, the following features have increased significantly in importance: tamper resistance by dedicated hardware, formal product security certifications, system performance and latency, support for cloud and on-premises deployment, system scalability and support for multiple applications or environments. A feature that has decreased in importance yet remains important for 50 percent of respondents is the enforcement of policy.

How important are specific features?



How painful is key management? Sixty percent of respondents report the management of keys is painful. The top reasons for the pain are: there is no clear ownership, the systems are isolated and fragmented and the key management tools are inadequate. Respondents' companies continue to use a variety of key management systems. The most commonly deployed systems are manual process (e.g., spreadsheet, paper-based) and formal key management policy (KMP).

Which keys are most difficult to manage? The pain of managing SSH keys has increased significantly since last year. These keys have modestly decreased in difficulty: signing keys (e.g., code signing, digital signatures); keys for external cloud or hosted services, including Bring Your Own Key (BYOK) keys; and end user encryption keys.

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

The importance of hardware security modules (HSMs) to an encryption or key management strategy will grow 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. Fifty-three percent of respondents say they are important today, and 63 percent of respondents say they will be important in the next 12 months. Payment transaction processing, database encryption and cloud access security brokers (CASBs) are use cases expected to increase in the next 12 months. Application level encryption and payment credential provisioning are use cases expected to decrease.

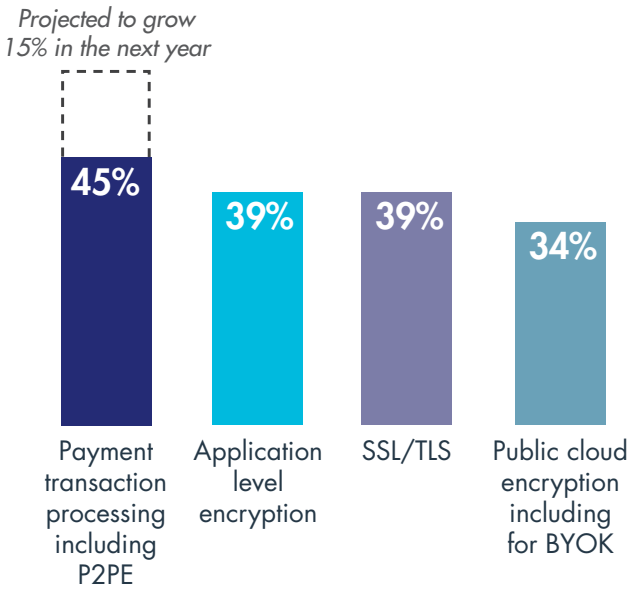
43%

Overall HSM usage in France

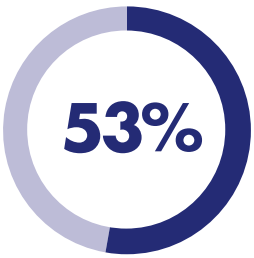
This is ***2% higher*** than the global average

How organizations are using HSMs. Sixty-three percent of respondents say they have a centralized team that provides cryptography as a service. The global average is 61 percent. Thirty-seven 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. Fifty-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 20 percent of respondents plan to do so in the next 12 to 24 months. Fifty percent of respondents say the cloud provider is the most responsible for protecting sensitive or confidential data transferred to the cloud.



HSMs were rated as either *very important or important* **today** by 53% of respondents

How is data at rest in the cloud protected? Forty-four percent of respondents say encryption is performed on-premises prior to sending data to the cloud using keys the organization generates and manages, and 40 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider.

58%

of respondents currently transfer **sensitive or confidential data to the cloud**

"FORTY-FOUR PERCENT OF RESPONDENTS SAY ENCRYPTION IS PERFORMED ON-PREMISES PRIOR TO SENDING DATA TO THE CLOUD USING KEYS THE ORGANIZATION GENERATES AND MANAGES."

"FIFTY-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 20 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

CSA cloud security alliance℠

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com