THALES

Ponemon INSTITUTE

BRAZIL ENCRYPTION TRENDS STUDY

July 2018

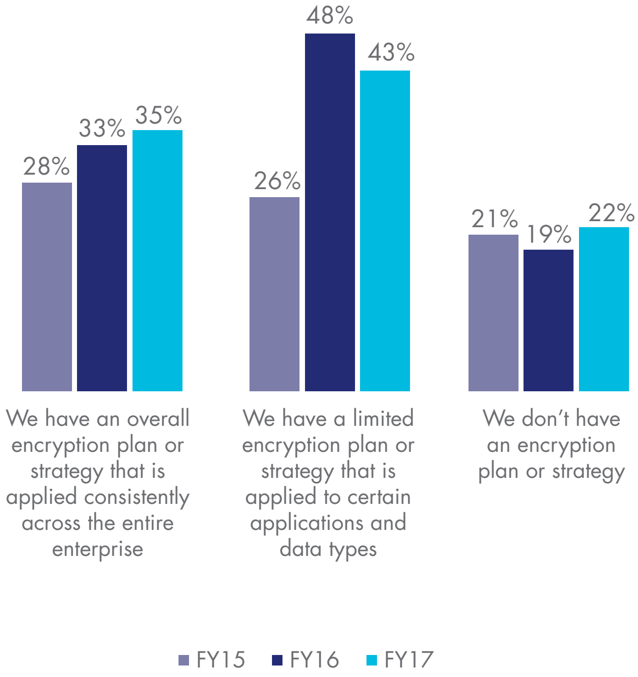
EXECUTIVE SUMMARY

Ponemon Institute is pleased to present the findings of the *2018 Brazil Encryption Trends Study,* sponsored by Thales eSecurity. We surveyed 507 individuals in Brazil to examine the use of encryption and the impact of this technology on the security posture of organizations in this region.

The first encryption study 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 Brazil. The 11 countries include: Australia, France, Germany, India, Japan, Mexico, the Middle East, the Russian Federation, the United Kingdom, the United States and, for the first time, South Korea.

As shown in Figure 1, more organizations represented in this research continue to recognize the importance of having an encryption strategy, either an enterprise-wide (35 percent of respondents) or a limited strategy that targets certain applications and data types (43 percent of respondents).

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



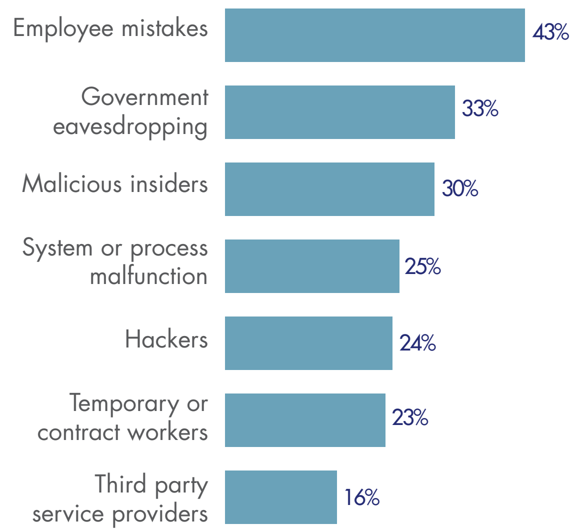
Following is a summary of our key findings. More details are provided for each key finding listed below in the next section of this report.

IT operations continue to have the most influence in directing encryption strategies. While responsibility for the encryption strategy is dispersed throughout the organization, IT operations (33 percent of respondents) has the most influence. Twenty-eight percent of respondents say no one single function is responsible for encryption strategy.

Which data types are most often encrypted? More companies are encrypting financial records and payment-related data. Fewer companies are encrypting employee/HR data and non-financial business information in this year's research.

Employee mistakes are the most significant threats to sensitive data. The most significant threats to the exposure of sensitive or confidential data are employee mistakes, according to 43 percent of respondents. Thirty-three percent of respondents say government eavesdropping and 30 percent of respondents say malicious insiders pose the most significant threat to sensitive or confidential data.

Threats to sensitive data

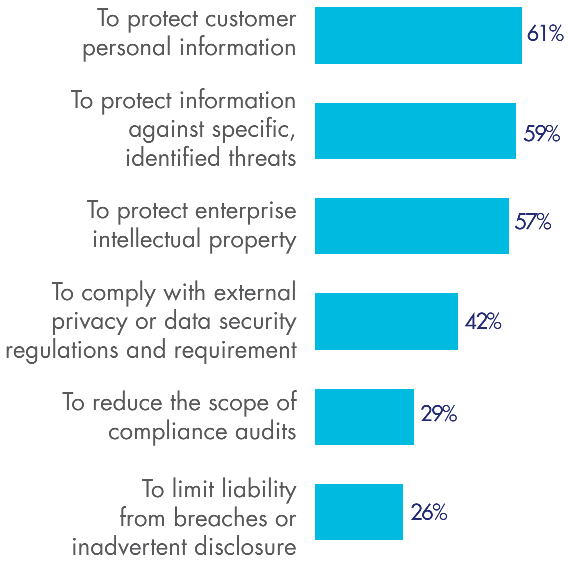


35%

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

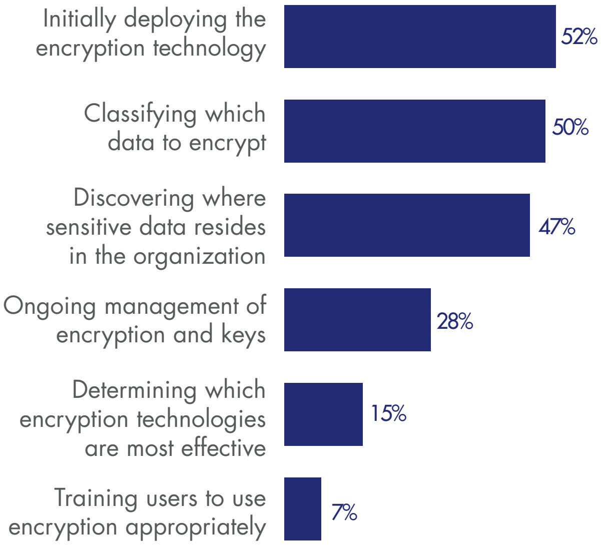
Protection of customers' personal information is the main driver for using encryption technologies. The importance of protecting customers' personal information has increased significantly in the past three years (50 percent of respondents vs. 61 percent of respondents in this year's research). The protection of information against specific, identified threats has also increased significantly from 37 percent of respondents in 2015 to 59 percent of respondents in this year's research. In contrast, compliance with external privacy or data security regulations and requirements (42 percent of respondents) and to reduce the scope of compliance audits (29 percent of respondents) have declined as drivers for using encryption technologies.

What are the drivers for encryption?



The initial deployment of encryption technology continues to be the biggest challenge. Fifty-two percent of respondents say initially deploying the encryption technology is the biggest challenge in planning and executing a data encryption strategy. In the past three years, the challenge of classifying which data to encrypt has increased from 42 percent of respondents to 50 percent of respondents in this year's research.

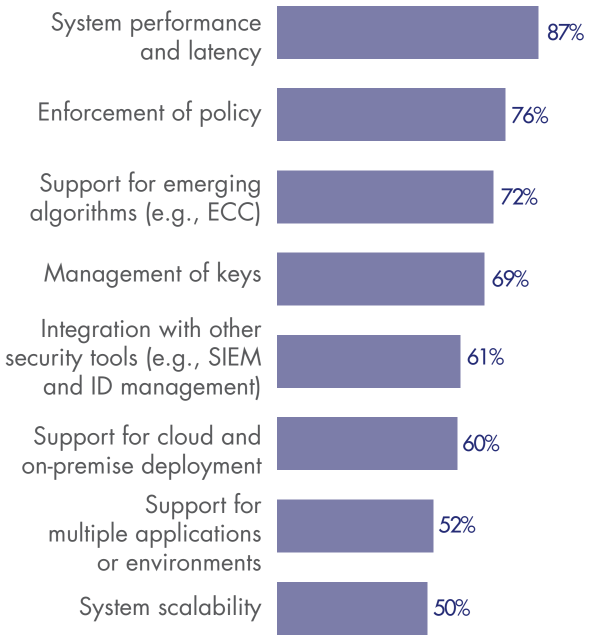
Why organizations are challenged by encryption



No single encryption technology dominates because organizations have very diverse needs. Internet communications, encryption of databases and internal networks 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 the least likely to be deployed.

Certain encryption features are considered more critical than others. In the past three years, enforcement of policy and system scalability features have increased the most in importance. Management of keys, support for cloud and on-premises deployment and support for multiple applications or environments have decreased but remain at high levels.

How important are specific features?



How painful is key management? Fifty-nine percent of respondents report the management of keys is painful. The top reasons for the pain are: lack of skilled personnel, no clear ownership, systems are isolated and fragmented, and 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).

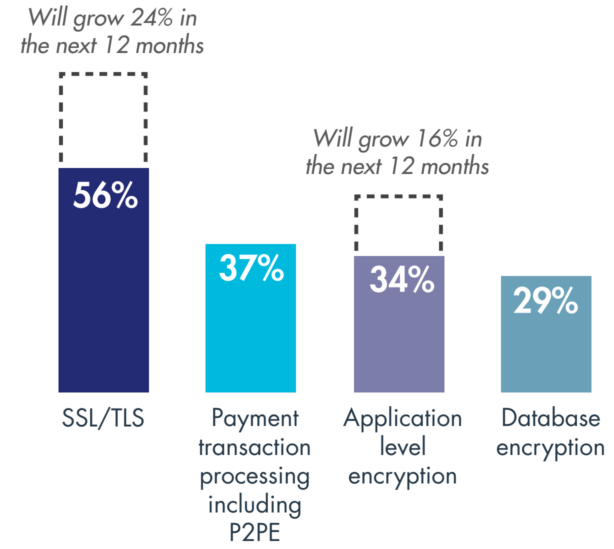
Which keys are most difficult to manage? The keys most difficult to manage are keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys, signing keys, and SSH keys. These keys have demonstrated modest decreases in management difficulty but still remain at significant levels.

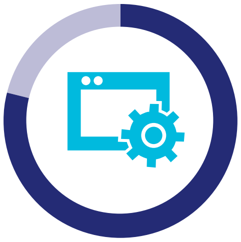
Key management continues to be a source of pain, with **keys for cloud services rated as most difficult to manage**

The importance of HSMs to an encryption or key management strategy will grow in the next 12 months. Forty-four percent of respondents say they are important today and 51 percent of respondents say they will be important in the next 12 months. SSL/TLS, payment transaction processing including P2PE, application level encryption, database encryption, payment service provider interface and payment credential provisioning are growing use cases for HSMs.

"FIFTY-NINE PERCENT OF RESPONDENTS REPORT THE MANAGEMENT OF KEYS IS PAINFUL. THE TOP REASONS FOR THE PAIN ARE: LACK OF SKILLED PERSONNEL, NO CLEAR OWNERSHIP, SYSTEMS ARE ISOLATED AND FRAGMENTED, AND KEY MANAGEMENT TOOLS ARE INADEQUATE."

The most prevalent use cases for HSMs





79%

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 organizations are using HSMs. Fifty-five percent of respondents say they have a centralized team that provides cryptography as a service and 45 percent of respondents say each individual application owner/team is responsible for their own cryptographic services. The global average for the use of a centralized team is 61 percent of respondents.

46% 46%

Respondents were evenly split on preference for ***on-premise*** vs. ***cloud-hosted*** HSMs to support public cloud applications

Most organizations transfer sensitive or confidential data to the cloud. Forty-six percent of respondents say their organizations currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism) and 39 percent of respondents plan to in the next 12 to 24 months. Thirty-seven percent of respondents say it is the cloud provider who is most responsible for protecting sensitive or confidential data transferred to the cloud.

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

> “FORTY-THREE PERCENT OF RESPONDENTS SAY ENCRYPTION IS PERFORMED IN THE CLOUD USING KEYS THE CLOUD PROVIDER GENERATES AND MANAGES.”

> “FORTY-SIX PERCENT OF RESPONDENTS SAY THEIR ORGANIZATIONS CURRENTLY TRANSFER SENSITIVE OR CONFIDENTIAL DATA TO THE CLOUD (WHETHER OR NOT IT IS ENCRYPTED OR MADE UNREADABLE VIA SOME OTHER MECHANISM) AND 39 PERCENT OF RESPONDENTS PLAN TO IN THE NEXT 12 TO 24 MONTHS.”

Ponemon INSTITUTE

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.

THALES

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.

CLICK HERE TO READ THE FULL REPORT

OUR SPONSORS

VENAFI

GEOBRIDGE

CSA cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com