THALES

Ponemon INSTITUTE

2018 MEXICO ENCRYPTION TRENDS

MULTI-CLOUD USE AND THREAT PROTECTION DRIVE A NEW ERA OF ENCRYPTION AND KEY MANAGEMENT

JULY 2018

Survey results from 468 respondents in Mexico

30%
of organizations now have a consistent, enterprise-wide **encryption strategy**

Threats to sensitive data

Multi-cloud encryption

37%
Encryption in public cloud services grew **11% over last year!**

46%
of respondents are using **more than one public cloud provider**

25% increase!

71%
will use **multiple public cloud providers** in the next two years

78%
of respondents either use the cloud for **sensitive/non-sensitive applications and data** today, or will do so in the next 12-24 months

But *control* over the cloud is important

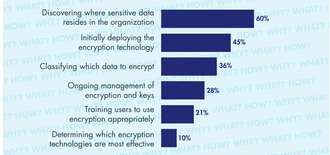
45%
of organizations indicate that they will only use keys for data-at-rest encryption that ***they*** control

41%
of organizations that use HSMs in conjunction with public cloud-based applications prefer to own/operate those HSMs ***on-premise***

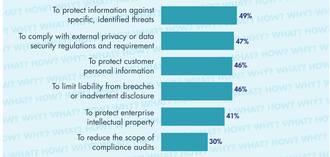
A Hardware Security Module (HSM) is a certified, trusted platform for performing cryptographic operations and protecting keys

The Why, What, and How of encryption

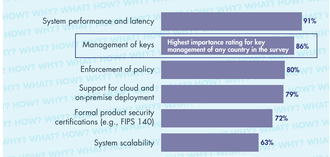
Why organizations are challenged by encryption



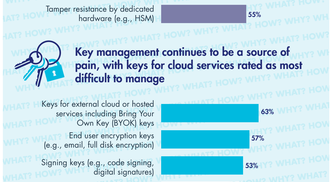
What are the drivers for encryption



How important are specific features



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

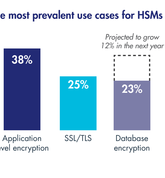


The important role of Hardware Security Modules

HSMs are increasingly important for encryption and key management, and are being used to support leading edge applications

42%
HSMs were rated as either *very important or important* **today** by 42% of respondents

The most prevalent use cases for HSMs



CLICK TO DOWNLOAD REPORT

FOLLOW US ON: