THALES

Ponemon INSTITUTE

2018 MIDDLE EAST ENCRYPTION TRENDS

MULTI-CLOUD USE DRIVES A NEW ERA OF ENCRYPTION AND KEY MANAGEMENT

MAY 2018

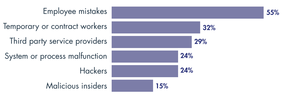
Survey results from over 300 respondents in the United Arab Emirates and Saudi Arabia

34%

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

This is below the global average but growing steadily

Threats to sensitive data



Multi-cloud encryption

55%

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

40%

Encryption in public cloud services grew from 37% to 40%

81%

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

Encryption of private cloud infrastructure and docker containers grew significantly over 2017

But *control* over the cloud is important

51%

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

44%

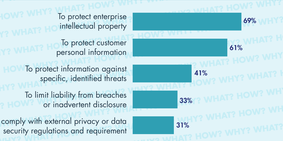
of organizations that use HSMs in conjunction with public cloud-based applications prefer to own/operate those HSMs *on-premise*

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

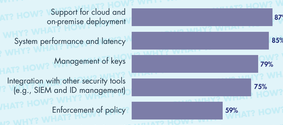
The Why, What, and How of encryption

Why organizations are challenged by encryption

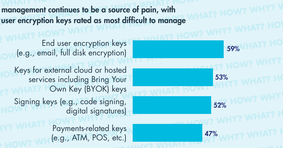
What are the drivers for encryption



How important are specific features



Key management continues to be a source of pain, with end user encryption keys rated as most difficult to manage



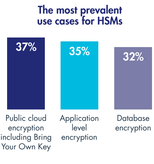
The important role of Hardware Security Modules

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

56%

HSMs were rated as either *very important or important* **today** by 56% of respondents

The most prevalent use cases for HSMs



CLICK TO DOWNLOAD REPORT

FOLLOW US ON: