

# 2018 BRAZIL ENCRYPTION TRENDS

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

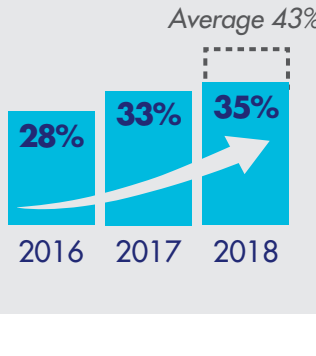
JULY 2018

Survey results from over 500 respondents in Brazil

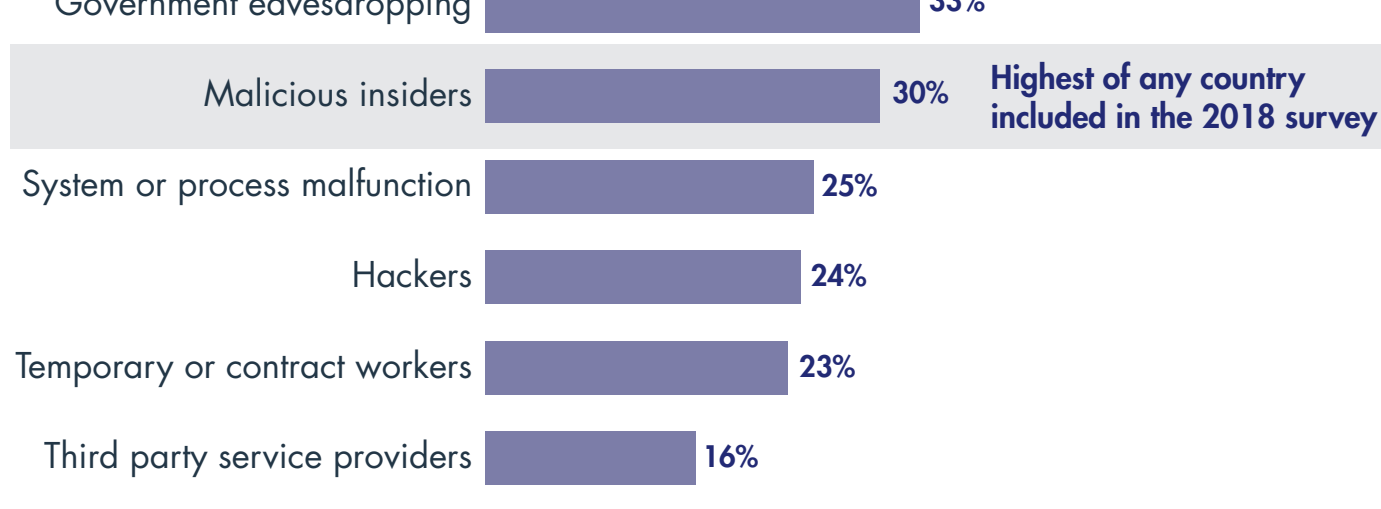


**35%** of organizations now have a consistent, enterprise-wide encryption strategy

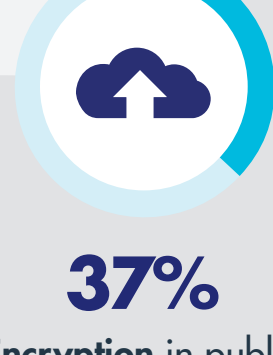
This is below the global average but growing steadily



## Threats to sensitive data



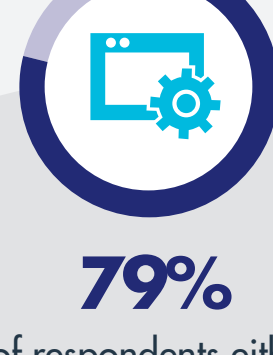
## Multi-cloud encryption



**37%** Encryption in public cloud services grew from 33% to 37%



**45%** of respondents are using more than one public cloud provider



**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



**56%** will use multiple public cloud providers in the next two years

## But control over the cloud is important



**34%**

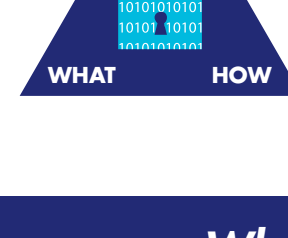
of organizations indicate that they will only use keys for data-at-rest encryption that **they** control



**46% 46%**

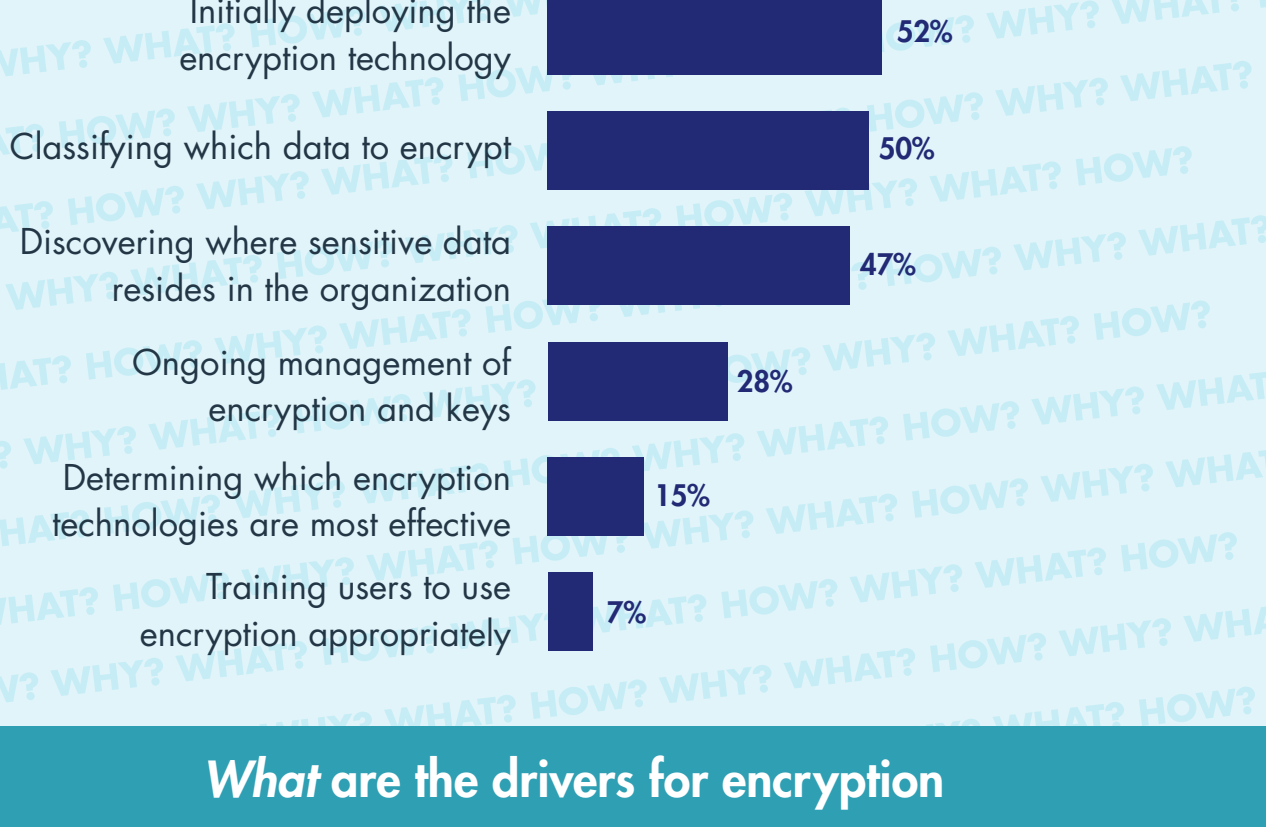
Respondents were evenly split on preference for **on-premise** vs. **cloud-hosted** HSMs to support public cloud applications

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

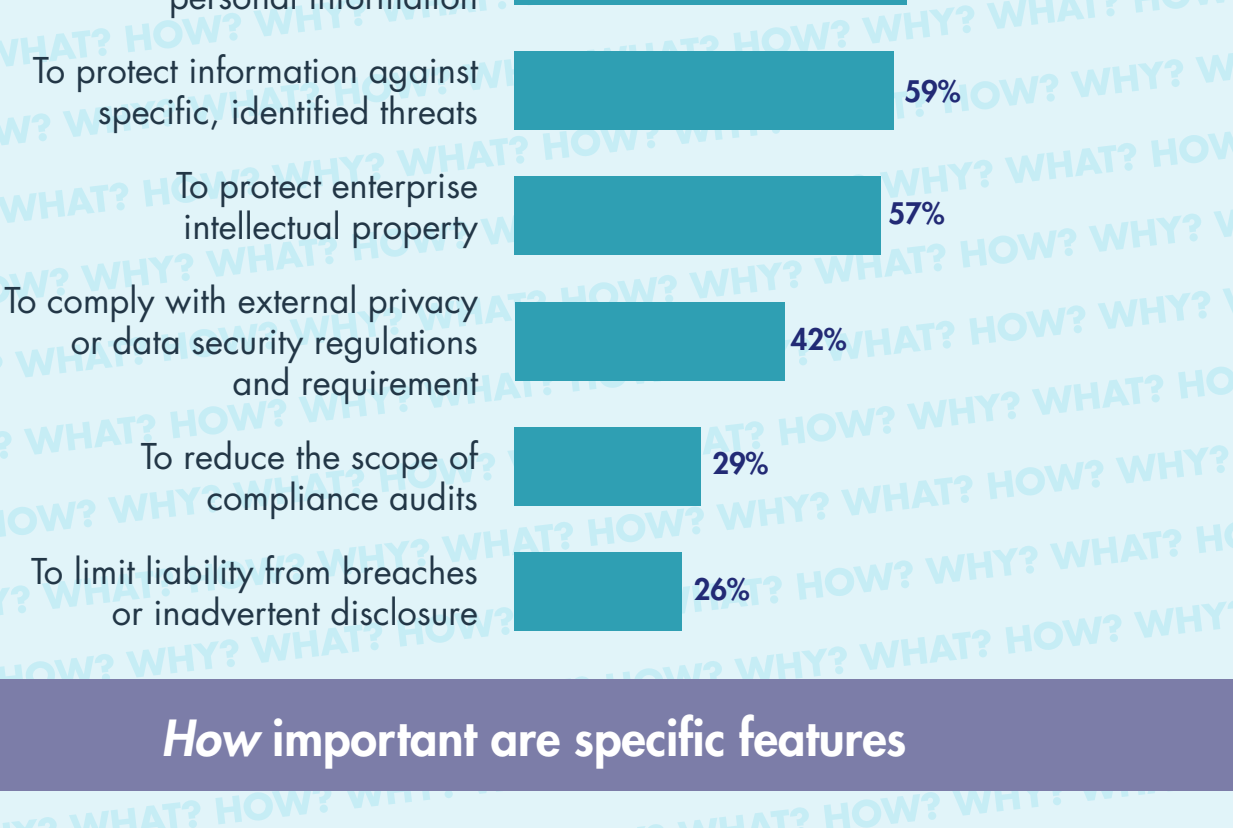


## The Why, What, and How of encryption

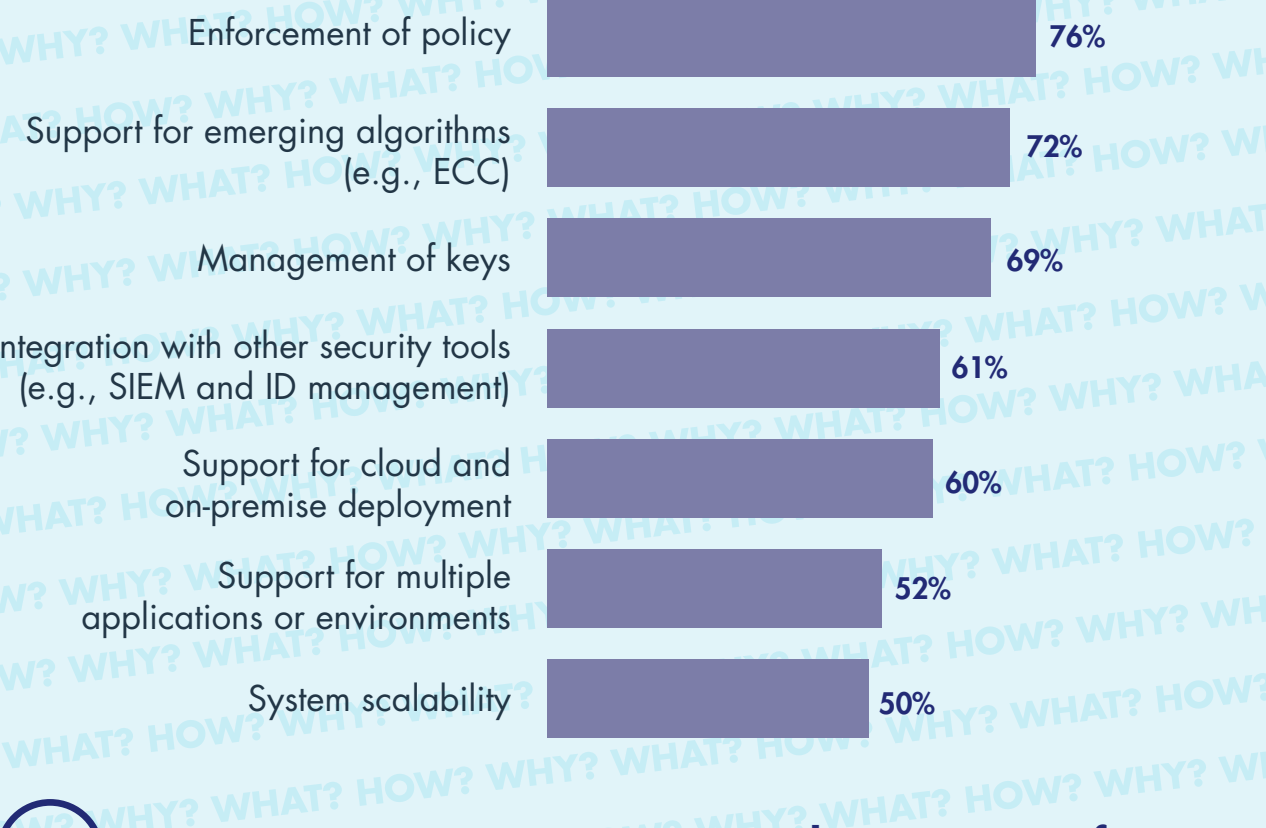
### Why organizations are challenged by encryption



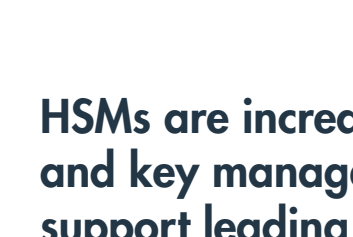
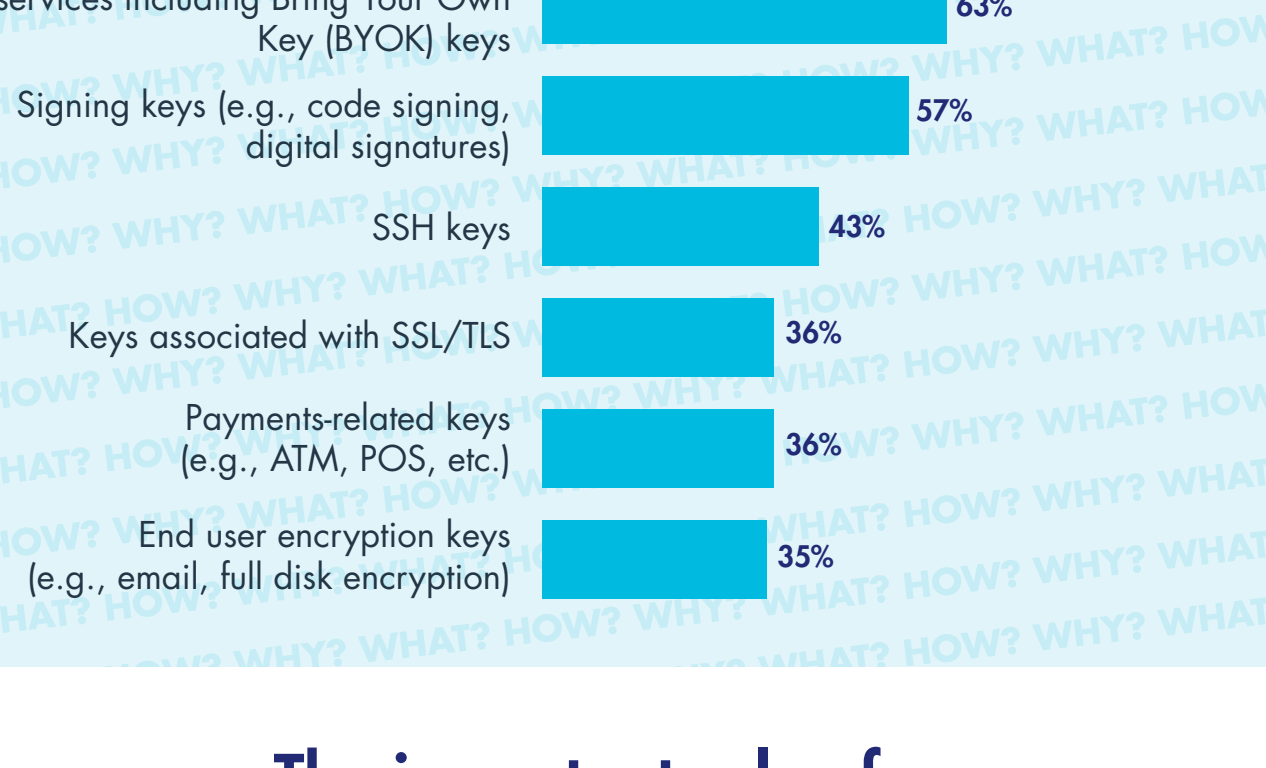
### What are the drivers for encryption



### How important are specific features



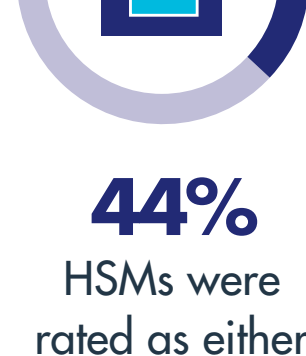
## Key management continues to be a source of pain, with keys for cloud services rated as most difficult to manage



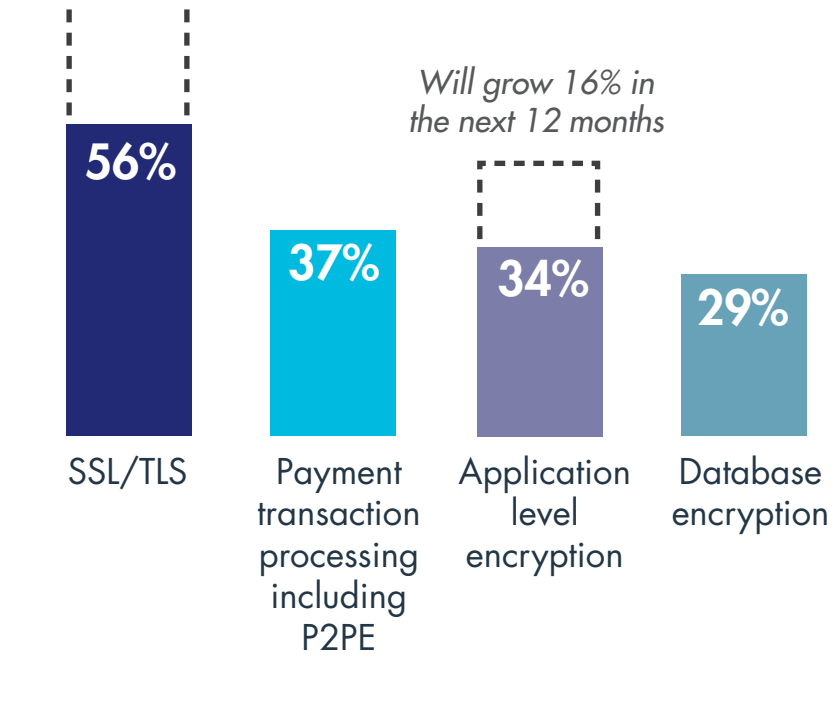
## The important role of Hardware Security Modules

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

### The most prevalent use cases for HSMs



**44%** HSMs were rated as either very important or important today by 44% of respondents



[CLICK TO DOWNLOAD REPORT](#)

FOLLOW US ON:

