2022 Thales Cloud Security Study

The Challenges of Data Protection in a Multicloud World

#2022CloudSecurityStudy

cpl.thalesgroup.com

Cloud Complexity Is a Major Concern

51% of EME respondents agree it is more complex to manage privacy and data protection regulations in the cloud than in on-premises networks.
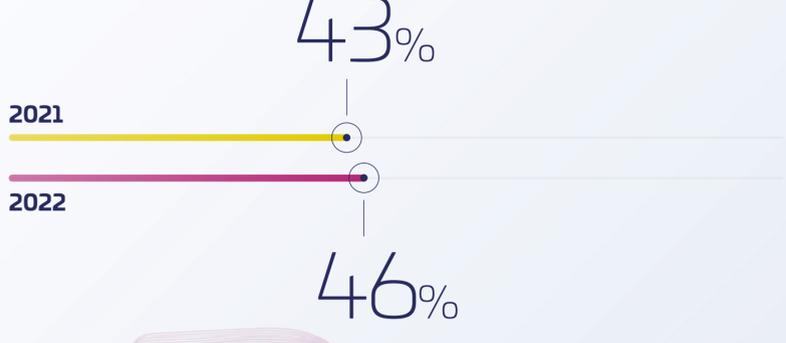
20% of EME customers store 60% or more of their sensitive data with external cloud providers.

Cloud Data Breaches and Failed Audits

More EME enterprises suffered a cloud data breach or failed an audit in 2022 compared to 2021.

2021 — **43%**

2022 — **46%**

46% of surveyed EME enterprises reported failing an audit within the past 12 months.

Encryption in the Cloud

41% of EME enterprises were able to avoid required breach notification processes thanks to the "safe harbor" provisions of regulations.
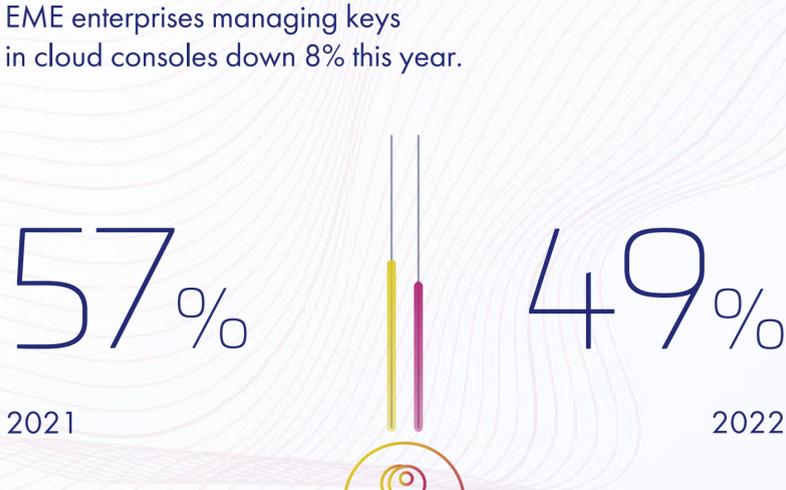
41% of EME respondents said regulatory compliance was the primary driver for where and how encryption is used in the cloud.

23% of respondents in EME said 61% or more of their sensitive data in the cloud is encrypted.

Encryption Key Management

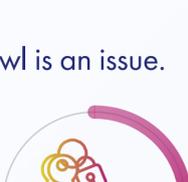EME enterprises managing keys in cloud consoles down 8% this year.

57% 2021

49% 2022

Key management sprawl is an issue.

9% of companies use 1-2 key management solutions
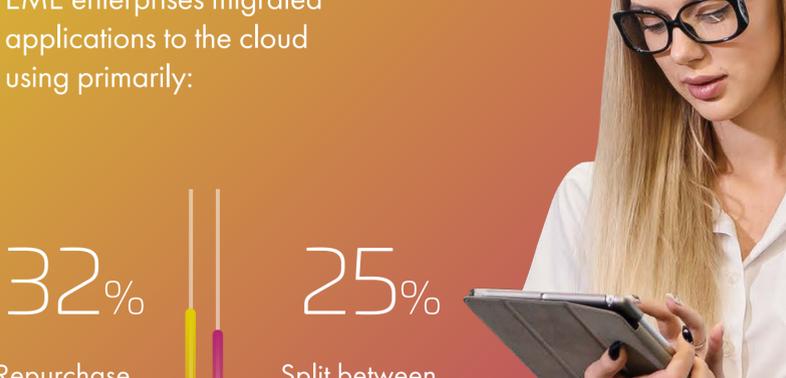
34% said they have 3-4 solutions

57% reported 5 or more solutions

EME Shifts into Multicloud Gear

EME enterprises migrated applications to the cloud using primarily:

32% Repurchase and shift

25% Split between lift and shift and re-architect

Modern Data Security for a Zero Trust World

- Discover Sensitive Data
- Encrypt Sensitive Data
- Secure Encryption Keys
- Control User Access