RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CPART4-W01

Should you trust your cloud providers with your encryption keys?

Sol Cates

VP of Research & Technology
Thales Group
@solcates

Agenda

- Cloud Trends
- Cloud Security is a Shared Responsibility so you must encrypt
- But Then The Keys
- BYOK vs HYOK
- HYOK Case Study – Google Cloud EKM
- Attributes of a Cloud Key Management solution

Cloud Trends

From the 2019 Thales Cloud Security Report

Businesses adopt a multi-cloud strategy when it comes their IT infrastructure and services needs

48%

of organizations have a multi-cloud strategy, with AWS, Microsoft Azure and IBM being the top three cited cloud providers

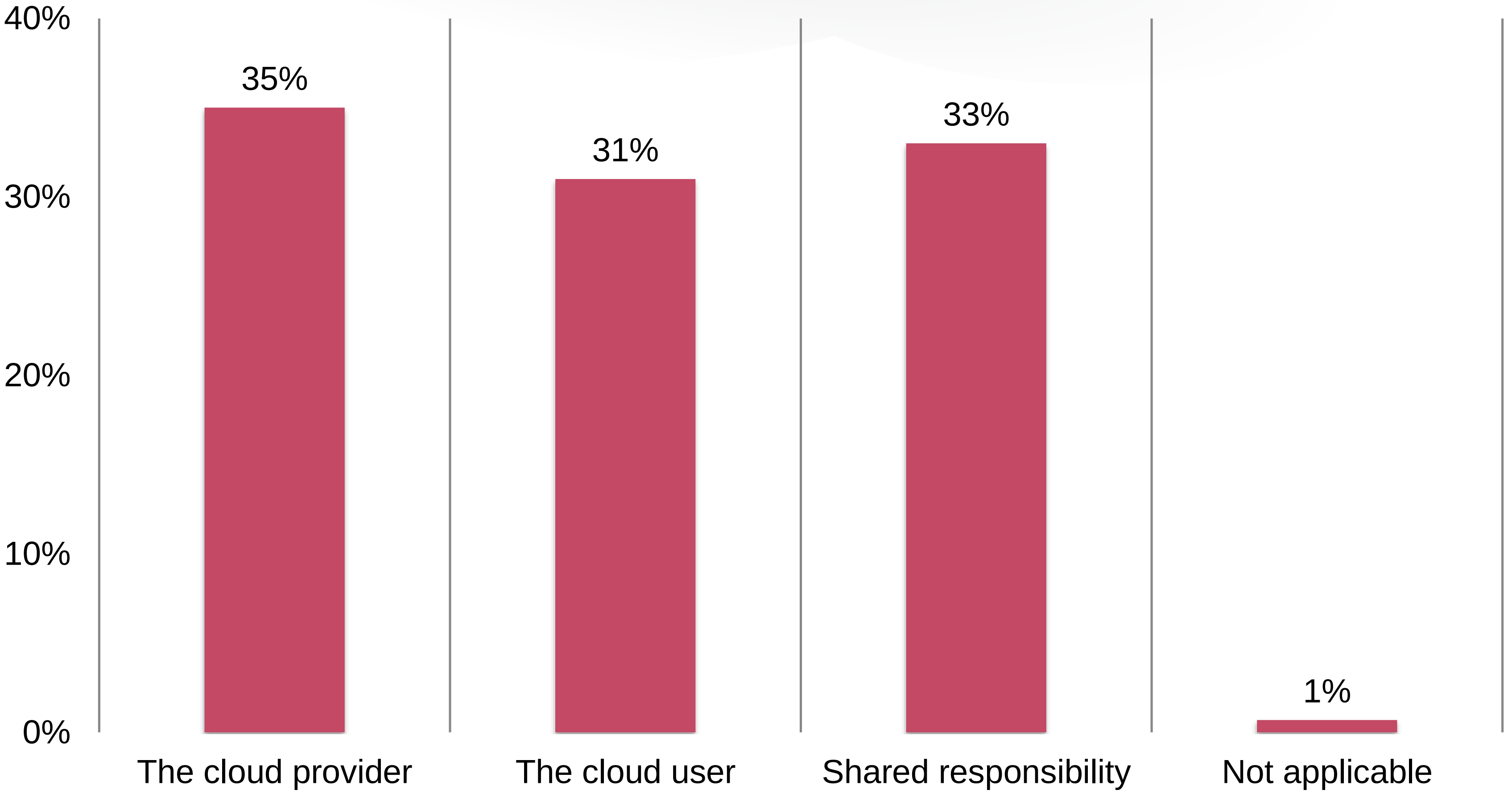
Businesses use 29 cloud applications on average, compared to 27 two years ago

over 10%

have more than 50 and the average US business has 41

Cloud security responsibility is distributed

Who is most responsible for protecting sensitive data stored in the cloud?



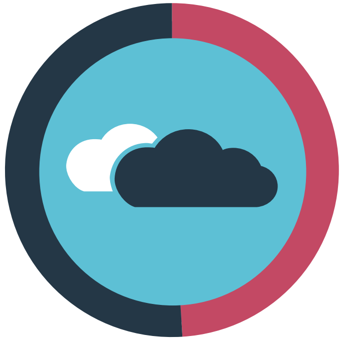
only 30 %

of organizations have a unified system for secure access to both cloud and on-premise applications

32%

don’t employ a security-first approach to storing data in the cloud

Businesses are not applying adequate security measures to protect sensitive data in the cloud



only 49%

of organizations are encrypting sensitive data in the cloud

Only half of businesses remain in control of the keys to their encrypted data stored in the cloud

53%

of businesses are controlling the encryption keys when data is encrypted in the cloud

despite

78%

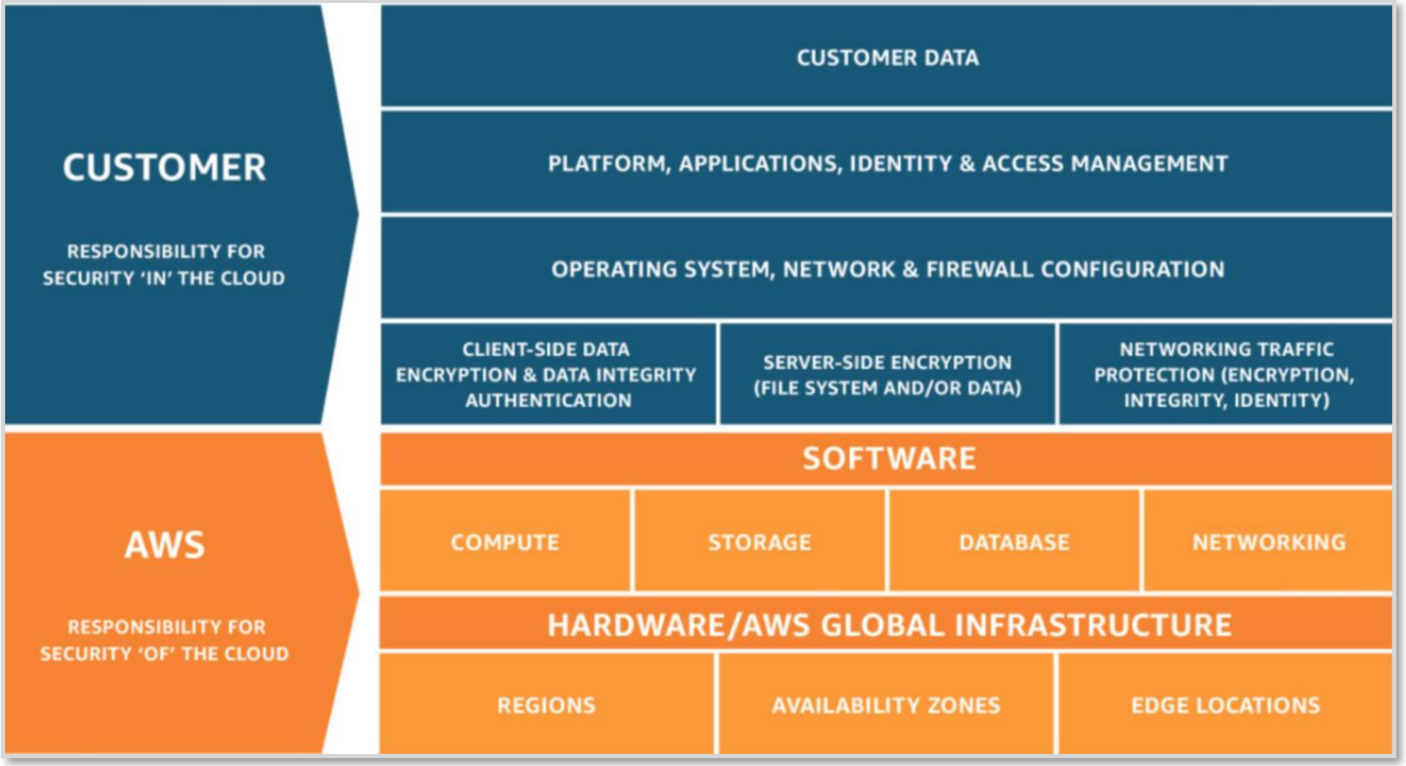
saying it's important to retain ownership of the encryption keys

“Cloud Security is a Shared Responsibility”

AWS on shared responsibility model

https://aws.amazon.com/compliance/shared-responsibility-model/

As shown in the chart below, this differentiation of responsibility is commonly referred to as Security **“of”** the Cloud versus Security **“in”** the Cloud



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

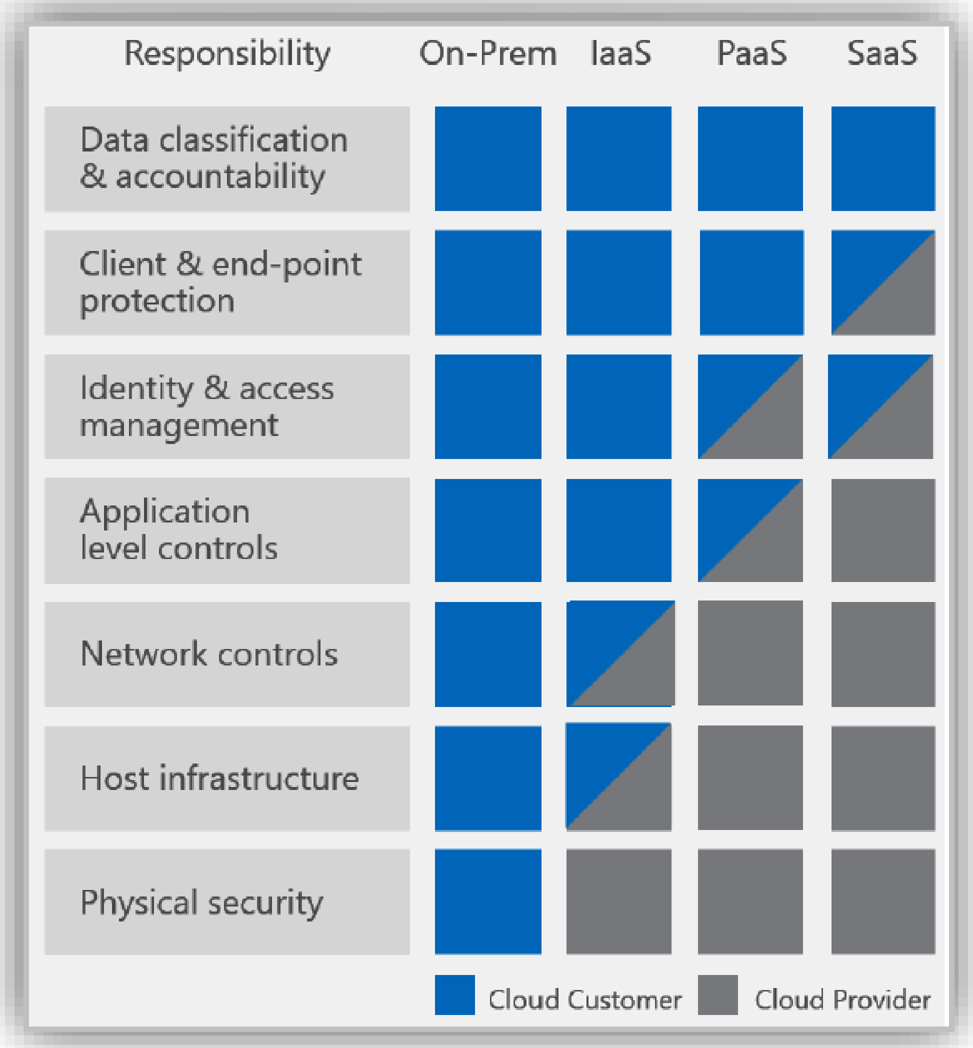
AVAILABILITY ZONES

EDGE LOCATIONS

Microsoft Azure on shared responsibility model

https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

The figure at right shows MSFT’s take on the shared responsibility model

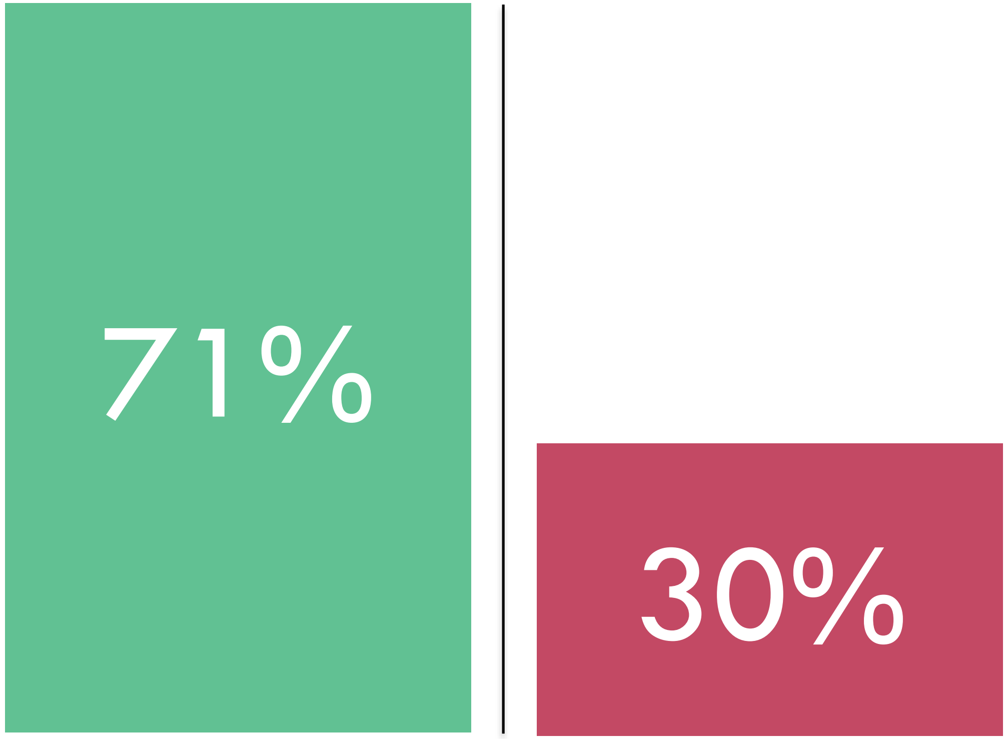


Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	🟦/◼
Identity & access management	🟦	🟦	🟦/◼	🟦/◼
Application level controls	🟦	🟦	🟦/◼	◼
Network controls	🟦	🟦/◼	◼	◼
Host infrastructure	🟦	🟦/◼	◼	◼
Physical security	🟦	◼	◼	◼

🟦 Cloud Customer ◼ Cloud Provider

But you’re not doing it

71% of enterprises use sensitive data in cloud environments



But only 30% use encryption in these environments

Source: 2019 Thales Data Threat Report by IDC

Cloud security alliance on cloud encryption keys

EKM-04

[Encryption] Keys shall not be stored in the cloud but maintained by the cloud consumer or trusted key management provider.

CSA cloud security alliance®

CCMv3.0.1™

CLOUD CONTROLS MATRIX VERSION 3.0.1

CSA says maintain the keys

What part of the key do you maintain?

- Do you create and upload the key?
- Does the provider create the key, and you manage it?

What does maintain mean?

- Is this full lifecycle management?
- How is key lifecycle management shared?

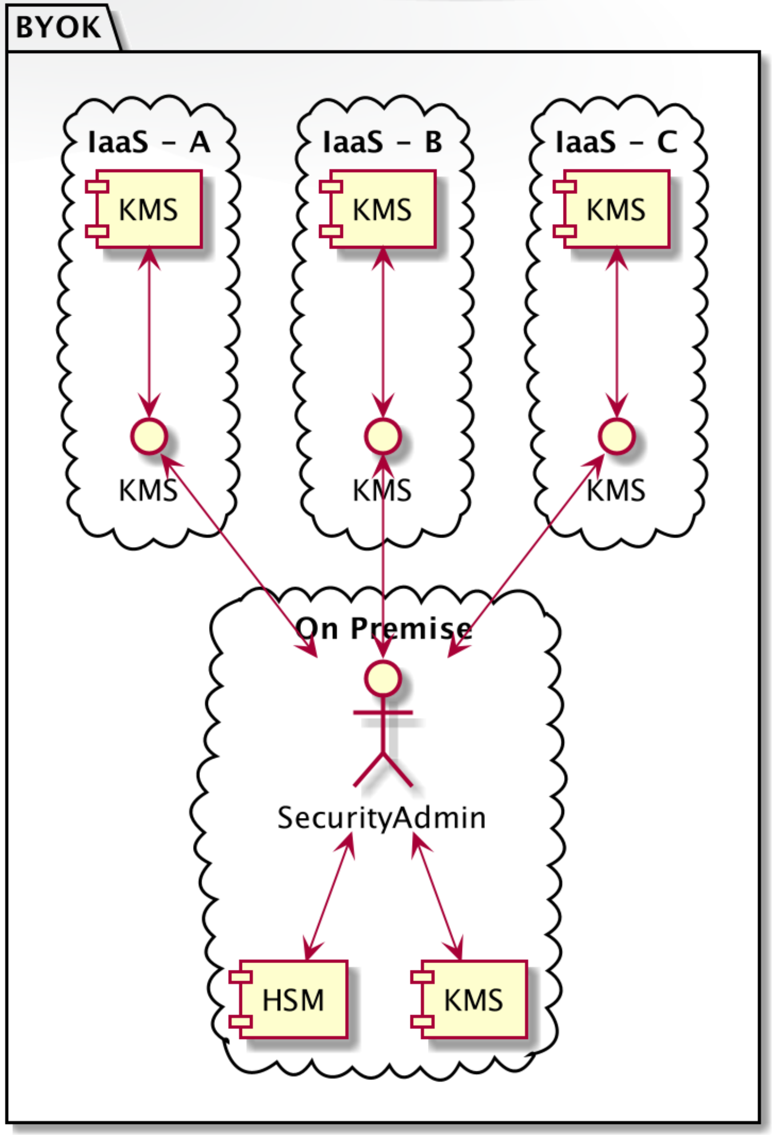
Sourcing your own keys

Generate and Securely store your keys

- OpenSSL? HSM? Private KMS?
- High Entrophy for good key quality
- Where does the secret sauce sit?

Managing your keys

- Rotate them? Remember each version's key material? In a spreadsheet?
- How will you maintain them?



BYOK vs HYOK

BYOK

Pluses

Wide spread, all IaaSs have a KMS

Many solutions in the marketplace to discover

Data Key Pedigree - **You** generated the DEK material

Minuses

Key is “granted” to the provider protected with **their** KEK on your behalf

Must trust the tools to tell you what is happening with your keys

HYOK

Pluses

DEK material is protected by **your** KEK in your EKM service

The provider has no direct access to your DEK/KEK

Minuses

Potential SLA impact to provider

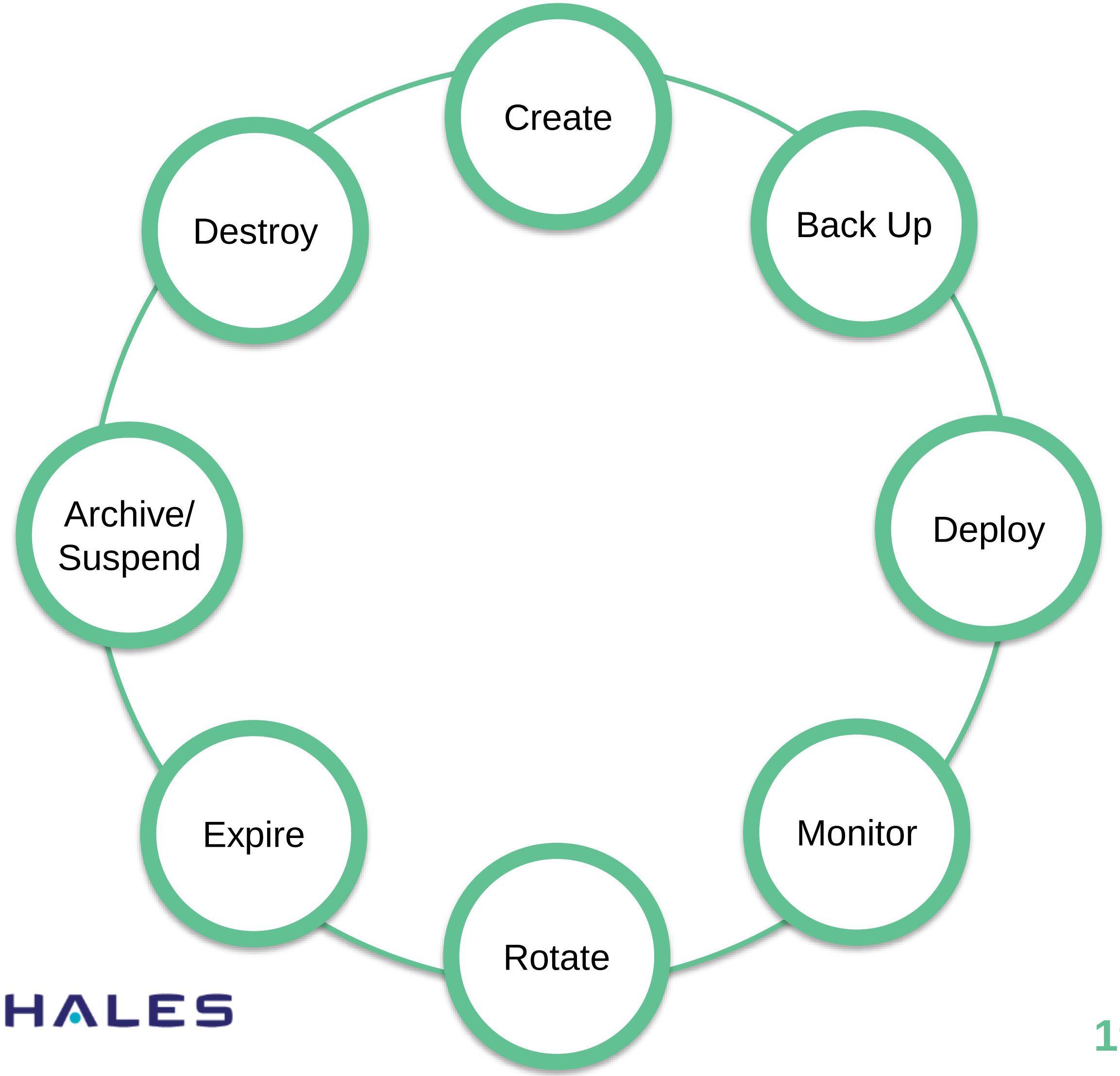
Data Key Pedigree - **provider** generates the DEK material

BYOK

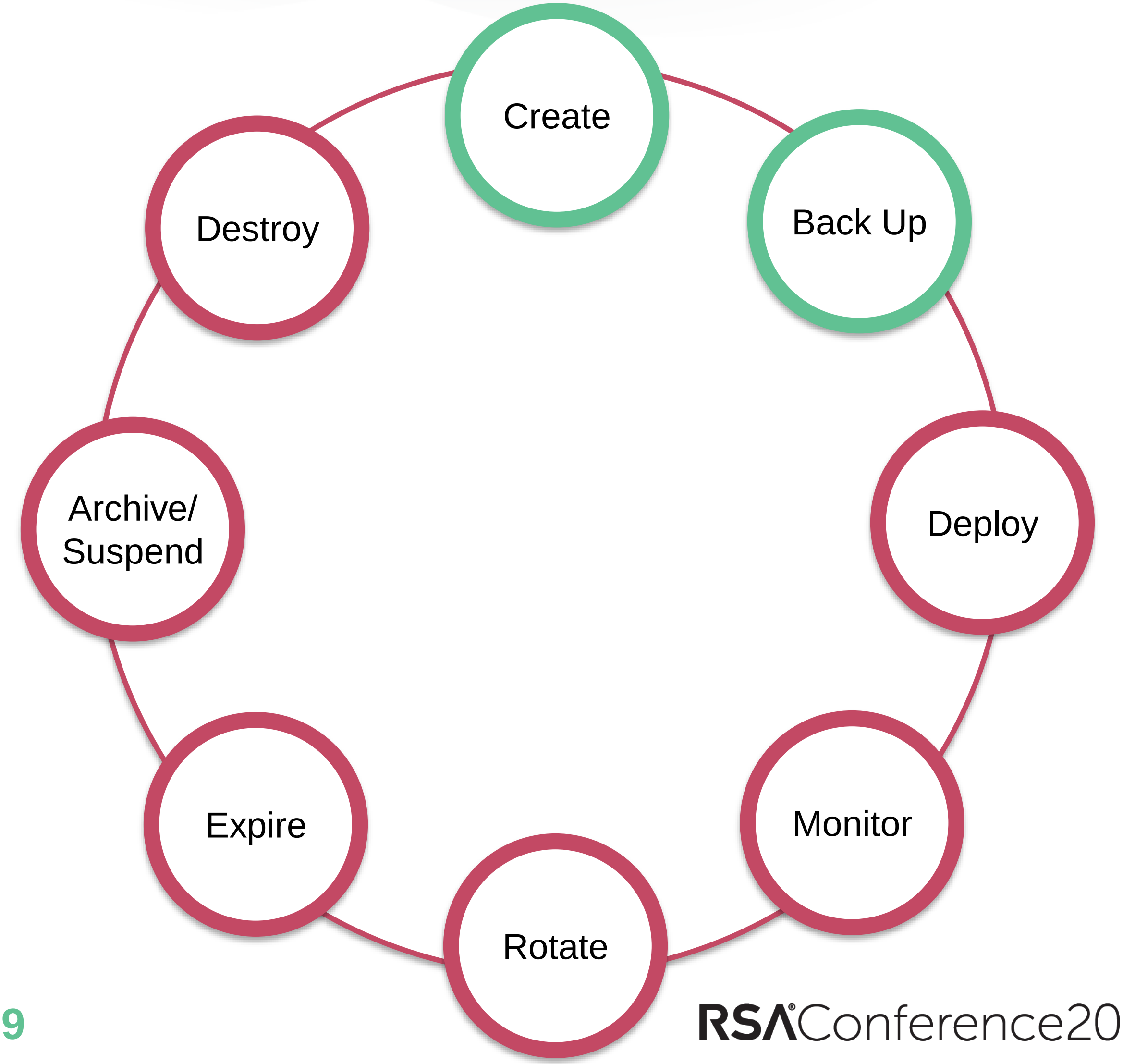
Requirements for Bring Your Own Encryption

Cloud key lifecycle management comparison

Automated Key Lifecycle Management



Admin in the middle Lifestyle management



How to bring your own key

Small Scale

- Major IaaS/PaaS providers enable you to upload a key to their cloud
- High scale operations are cumbersome
- Major challenge: quality of imported keys, and potential for human error

High Scale

Build-or-Buy decision

- Build and maintain a cloud key management using each provider's BYOK API
- Buy a multi-cloud key management solution

Requirements for multi-cloud key management

Most Common Clouds

AWS

MS Azure

MS Office365

Salesforce

Google Cloud

Requirements for Efficiency & ROI

Full key life cycle management

Create / upload / **ROTATE** / disable / delete
Federated login and corresponding access to key rights

Core Functionality

Secure key source and storage

Manage existing keys in the cloud

Revoke and delete keys

Operational Requirements

GUI for understanding and regular use

All clouds in one “pane of glass”

API for operating at scale

HYOK Case Study

Google Cloud Platform

HYOK

Some providers have introduced a few approaches to "HYOK"

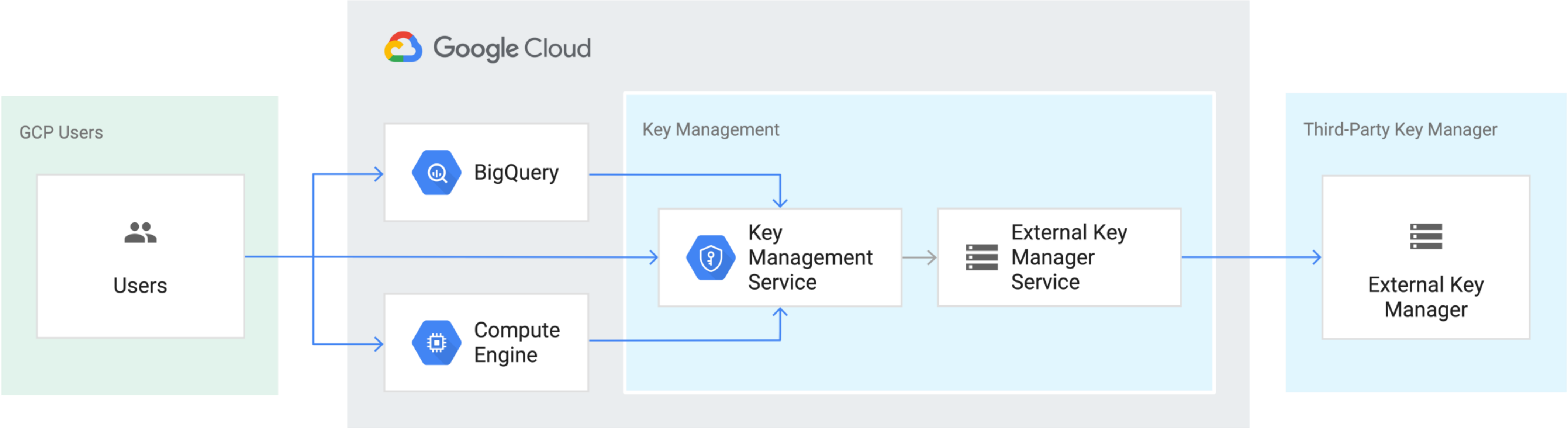
- Salesforce – Cache-Only Key Service
- Azure – Synchronize keys from off-cloud to cloud
- Google – External Key Management with Wrapping/Unwrapping

Differences in approaches mean unique solutions and implementations may be needed

- Can this be consolidated?

Google cloud - External key management

- EKM wraps Crypto Keys with an externally managed key
- CloudKMS requests that the key be unwrapped with context
- EKM evaluates the context and justification to see if authorized
- The EKM can be used to prevent undesired requests for data access



So What Do You Do First?

How can you start your journey?

Questions to start your journey tomorrow

Questions to ask each of your cloud providers

- Support encryption?
  - If so, what kind of Key Management?
  - Can I manage the keys off-cloud?

Questions to ask yourself

- What is our cloud management strategy?
- How do we bridge that to our enterprise key management?
- Do you have the tools or the staff for cloud key lifecycle management?

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CPRT4-W01

Thank You

Sol Cates

VP Research & Technology
Thales Group
@solcates