RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: BAC-F03

Key Management Architectures for Multinational Compliance

Sundaram Lakshmanan

Chief Technology Officer
CipherCloud, Inc.
https://www.linkedin.com/in/sundaramlakshmanan

Agenda

- A perfect storm (Hint: there are several problems here)
- Challenges with compliance for multinationals
- Challenges with key management in the cloud era
- Developing a plan for cloud applications
  - Understanding data and data proliferation in the cloud
  - Understanding the shared responsibility model
  - Key management architectural choices
- What can you do?

A perfect storm in the making for multinationals…

Staying compliant

- Regulations at all levels: industry, regional, and global
- Multiple products and solutions required
- Lack of expertise
- Varying requirements

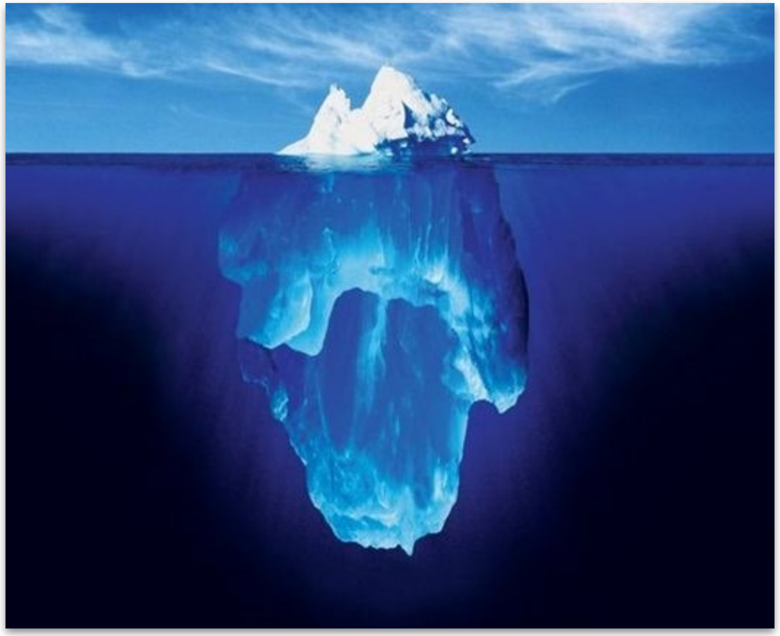
Key management

- It’s all about the data
- Data is in isolated and fragmented systems
- Data proliferation is in disparate applications
- Shortage of talent, processes, and tools

Global presence

- Moving to the cloud
- Working across international boundaries
- Centralized vs. regional processing
- In-house vs. off-the-shelf (SaaS) applications

Topic will be touching the tip of the iceberg



Not just one,

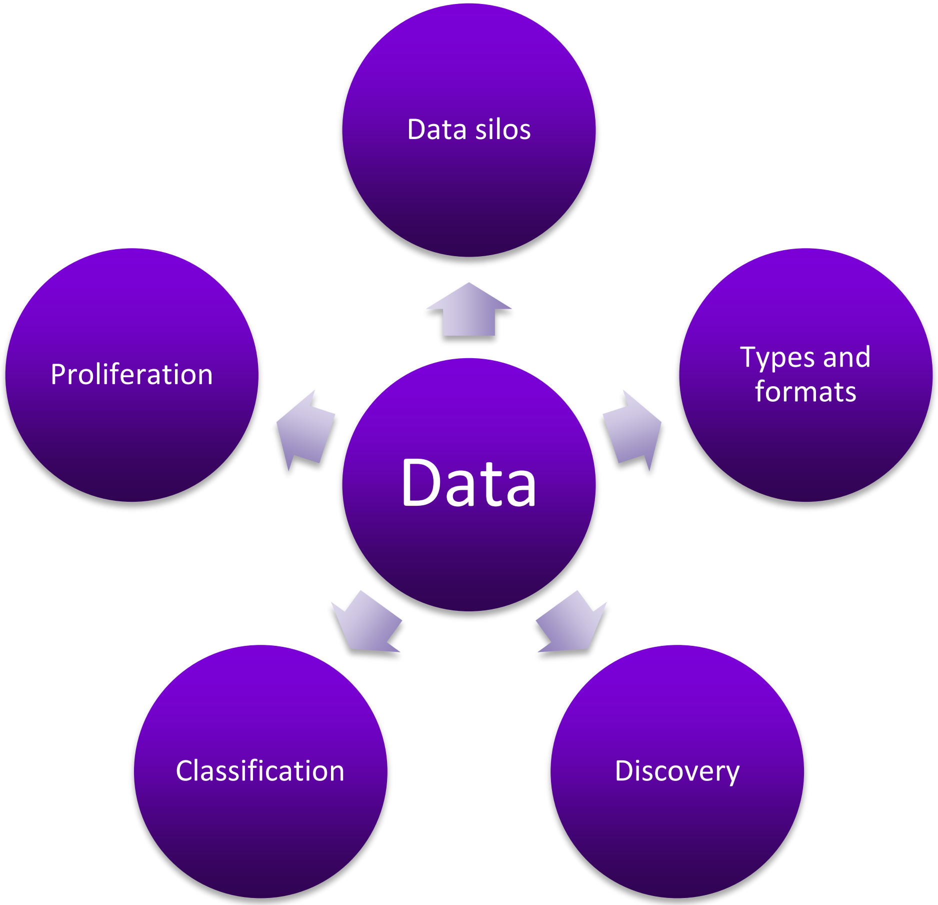
but many

Challenges with compliance for multinationals

Understanding compliance

- Regulations are implemented by governing bodies to protect PII and related sensitive data.
- Data privacy, residency, and ownership is at the heart of all regulations.
- Define controls on data access and usage: Who, what, when, where, why, and how?
- Enterprises are required to own their data and govern its use by having right set of controls in place and having a way to audit.
- Stay notified, and notify all those involved when data breaches occur.

Challenges with data



Multinational compliance: extensive and diverse

USA Federal
CALEA, CCRA, CIPA, CIOPPA, EFTA, FACTA, ECPA, FCRA, FISMA, FERPA, GLBA, HIPPA, HITECH, PPA, RFPA, Safe Harbor, US PATRIOT Act

Mexico
Personal Data Protection Law

Colombia
Data Privacy Law 1266

Chile
Law for the Protection of Private Life

Canada
ICO Privacy, PIPEDA, FOIPPA, PIPA

US States
Breach Notifications in 48 States

Brazil
Article 5 of Constitution

Argentina
Personal Data Protection Law
Information Confidentiality Law

United Kingdom
ICO Privacy & Electronic Communications Regulations

European Union
EU General Data Protection Regulation
State Data Protection Laws

Morocco
Data Protection Act

South Africa
Electronics Communications & Transactions Act

Europe
28 Privacy Laws in Countries

Thailand
28 Privacy Laws in Countries

India
Pending laws under discussion

Singapore
Personal & Financial Data Protection Acts

Australia
National Privacy Principles, State Privacy Bill, Email Spam and Privacy Bills

South Korea
Network Utilization & Data Protection Act

Japan
Personal Information protection Act

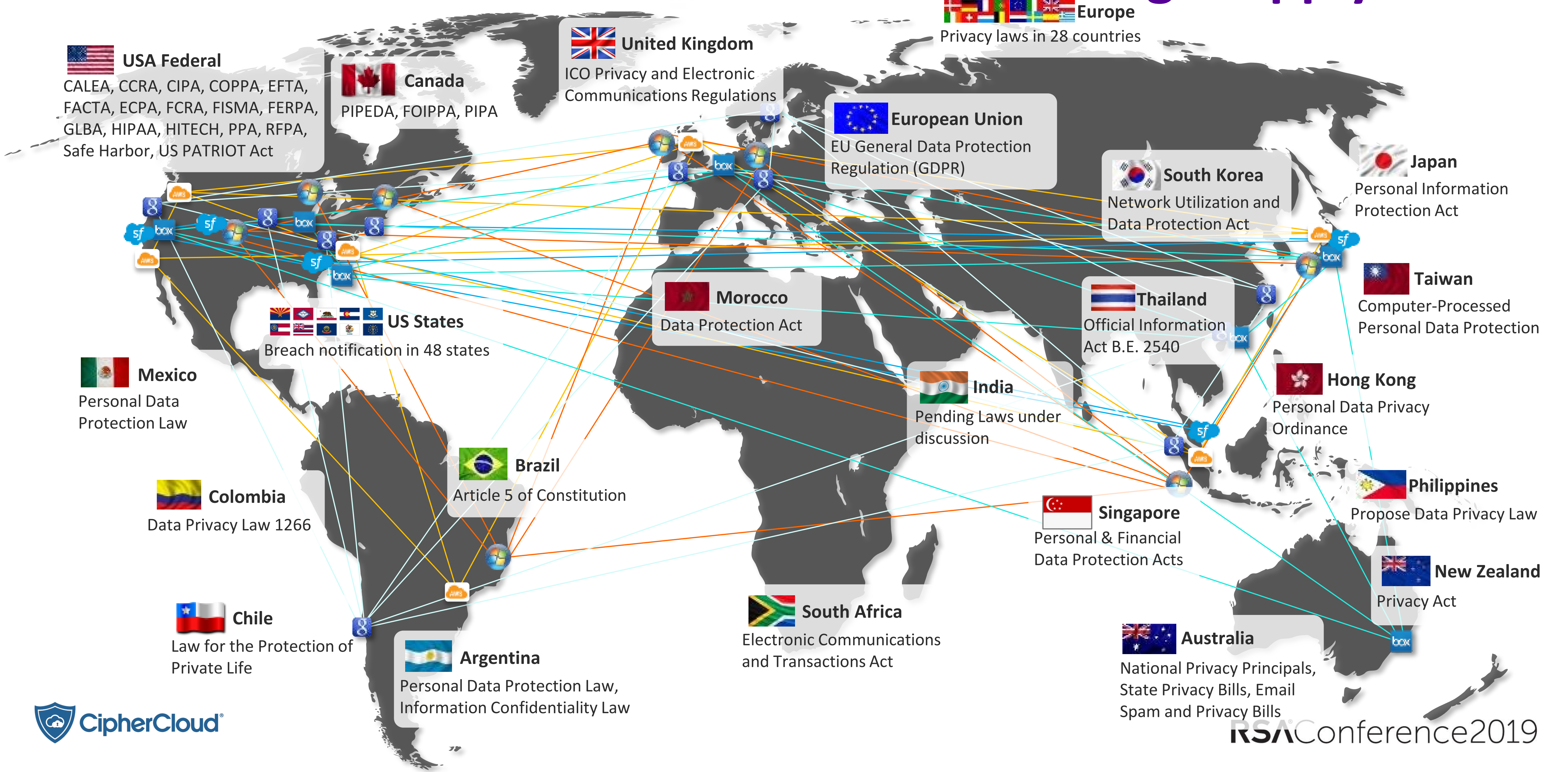
Taiwan
Computer-Processed Personal Data Protection

Hong Kong
Personal Data Privacy Ordinance

Philippines
Personal Data Privacy Law

New Zealand
Privacy Act

Where cloud data resides and what laws might apply



USA Federal
CALEA, CCRA, CIPA, COPPA, EFTA, FACTA, ECPA, FCRA, FISMA, FERPA, GLBA, HIPAA, HITECH, PPA, RFPA, Safe Harbor, US PATRIOT Act

Canada
PIPEDA, FOIPPA, PIPA

United Kingdom
ICO Privacy and Electronic Communications Regulations

Europe
Privacy laws in 28 countries

European Union
EU General Data Protection Regulation (GDPR)

South Korea
Network Utilization and Data Protection Act

Japan
Personal Information Protection Act

Taiwan
Computer-Processed Personal Data Protection

Morocco
Data Protection Act

Thailand
Official Information Act B.E. 2540

US States
Breach notification in 48 states

Mexico
Personal Data Protection Law

India
Pending Laws under discussion

Hong Kong
Personal Data Privacy Ordinance

Brazil
Article 5 of Constitution

Colombia
Data Privacy Law 1266

Philippines
Propose Data Privacy Law

Singapore
Personal & Financial Data Protection Acts

New Zealand
Privacy Act

South Africa
Electronic Communications and Transactions Act

Chile
Law for the Protection of Private Life

Argentina
Personal Data Protection Law, Information Confidentiality Law

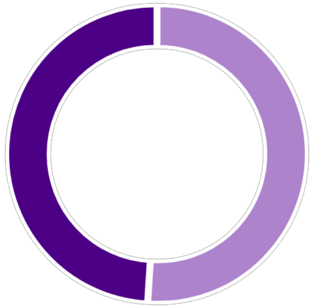
Australia
National Privacy Principals, State Privacy Bills, Email Spam and Privacy Bills

CipherCloud®

Challenges with key management in the cloud era

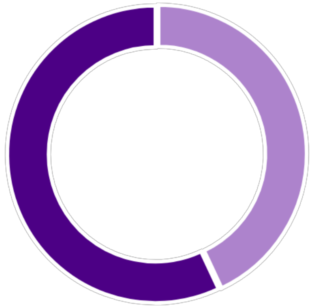
Why does compliance need key management?

Enterprises encrypt data for compliance, and encryption needs key management.



49%

of respondents rate compliance with regulations as a significant driver for encryption.*



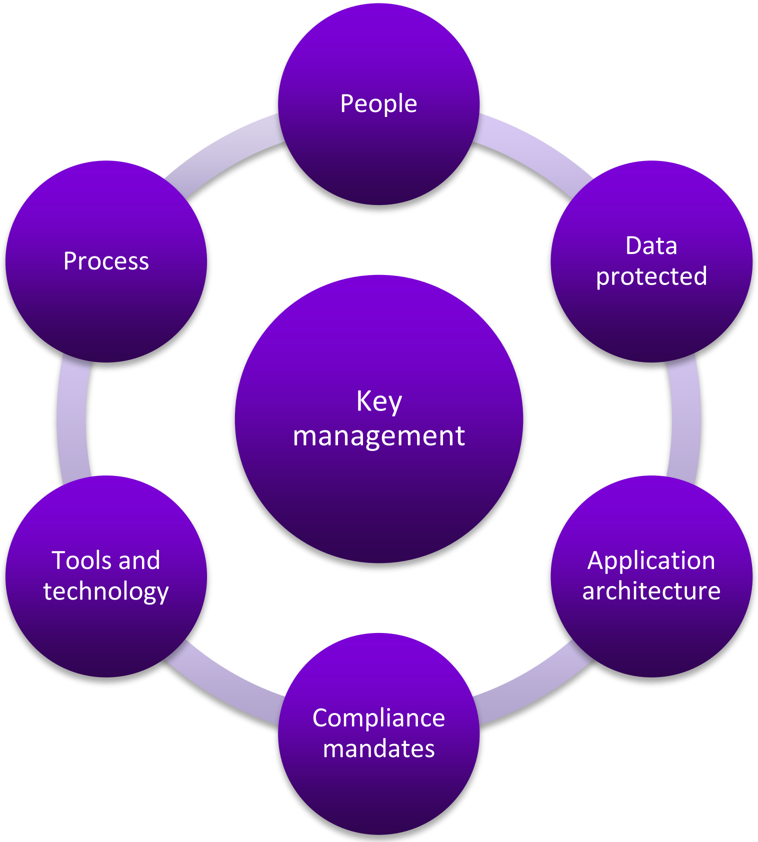
57%

of respondents in FY17 chose key management pain ratings at or above 7, suggesting a high pain threshold.*

**Source: Ponemon Institute, 2018 Global Encryption Trends Study, out of 5252 respondents*

Challenges with key management in the cloud era

Influenced by:



Key management

People

Data protected

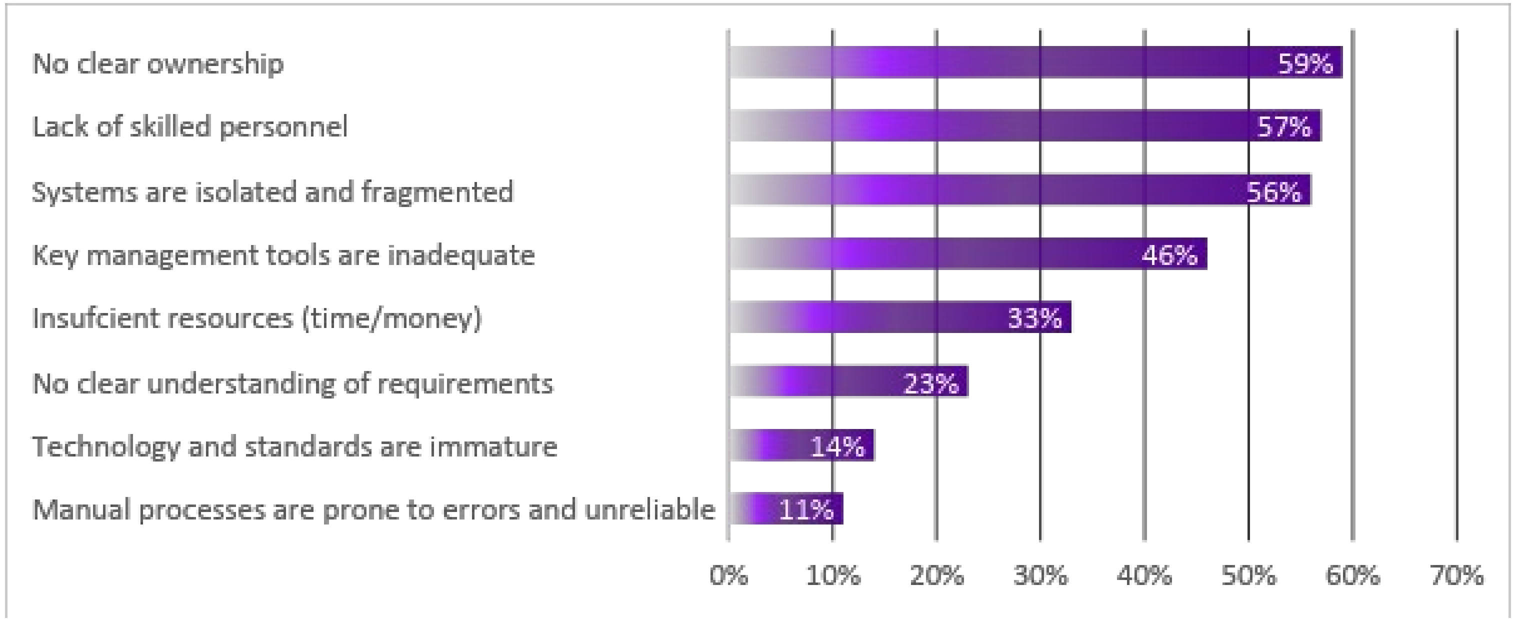
Application architecture

Compliance mandates

Tools and technology

Process

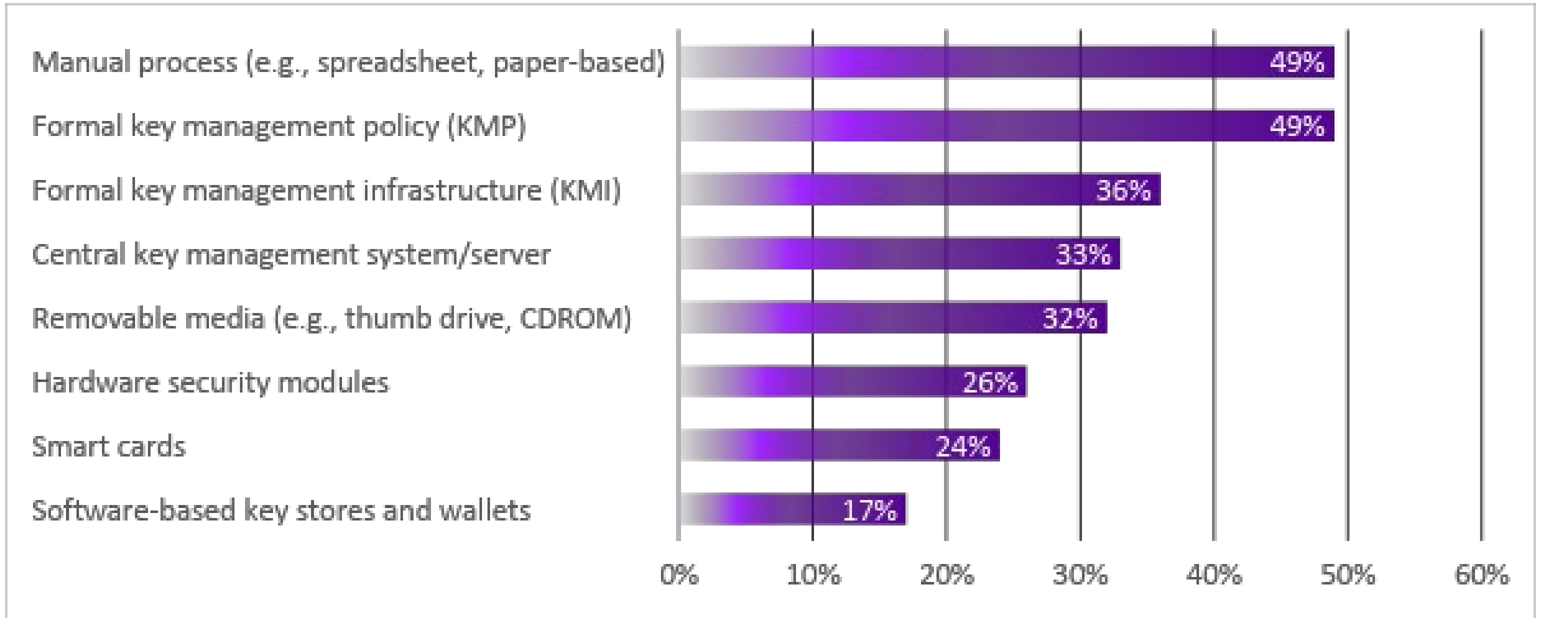
Key management pain points*



Source: Ponemon Institute, 2018 Global Encryption Trends Study, out of 5252 respondents

Manual process continues to be the most commonly deployed key management system

What key management systems does your organization presently use?*



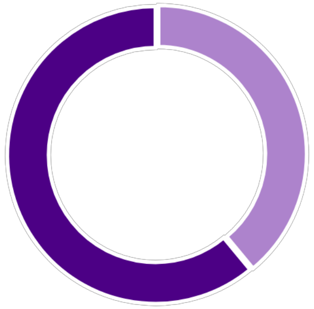
**Source: Ponemon Institute, 2018 Global Encryption Trends Study, out of 5252 respondents*

RSAConference2019

Developing a plan for the cloud

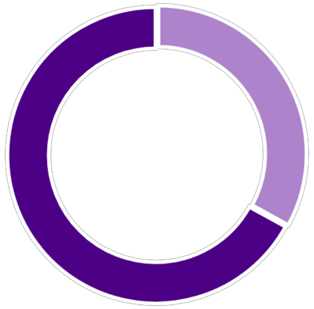
Understanding data and data proliferation in the cloud

Biggest hurdle in protecting sensitive data



61%

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



67%

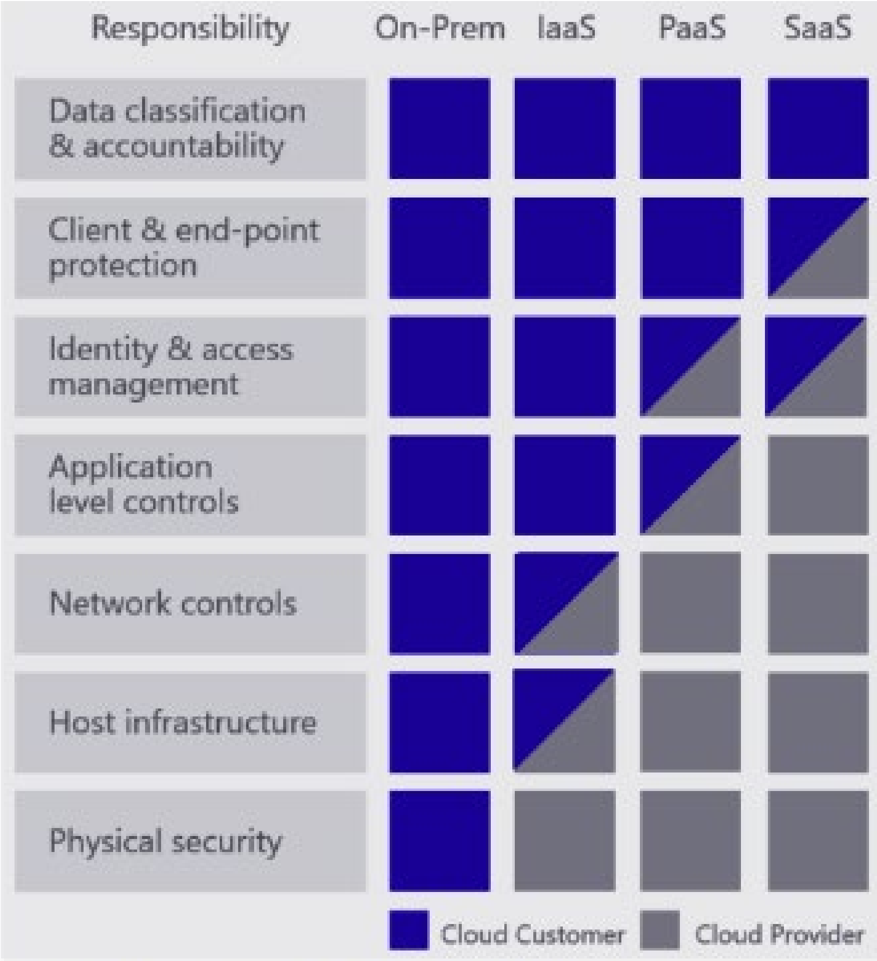
of respondents say discovering where sensitive data resides is the number one challenge.*

**Source: Ponemon Institute, 2018 Global Encryption Trends Study, out of 5252 respondents*

Data has a long life and a long tail

- There are two types of data: **structured** (e.g. email), and **unstructured** (e.g. files).
- Data is copied and transformed in many ways: big data pipelines, repositories, logs, queues, search indexes, emails, reports (CSV, XLS, PDF, DOC), images, and backups, in addition to databases and file systems.
- Data is shared between applications and with external users in the cloud.
- Data is exported to personal devices, printed, and copied effortlessly. *Data left on public computers and on lost devices can result in major breaches.*
- Data must be protected *at the source, or before it leaves enterprise control.*

Understanding the shared responsibility model



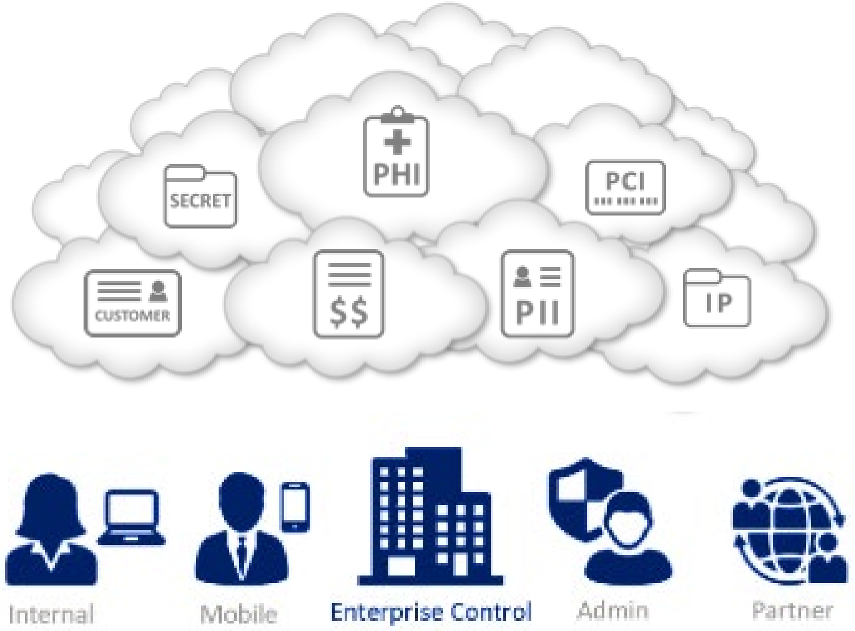
Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	■	■	■	■
Client & end-point protection	■	■	■	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	▨
Network controls	■	◩	▨	▨
Host infrastructure	■	◩	▨	▨
Physical security	■	▨	▨	▨

■ Cloud Customer ▨ Cloud Provider

Figure 1: Shared responsabilities for different cloud service models

© 2017, Microsoft Corporation

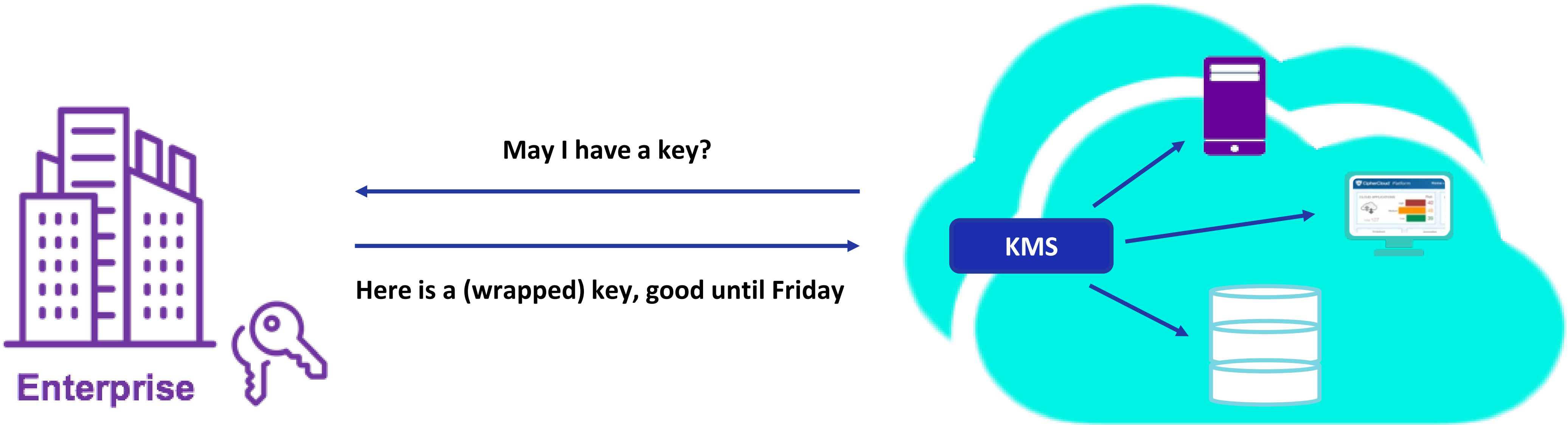
Data is the customer's responsibility.



Customer responsibility

- Users and devices
- Regulatory compliance
- Customer data
- Malware
- Malicious insiders
- Abuse and errors
- Identity / access control
- API / integration
- Data leak liability

Key management architectural choices - BYOK



May I have a key?

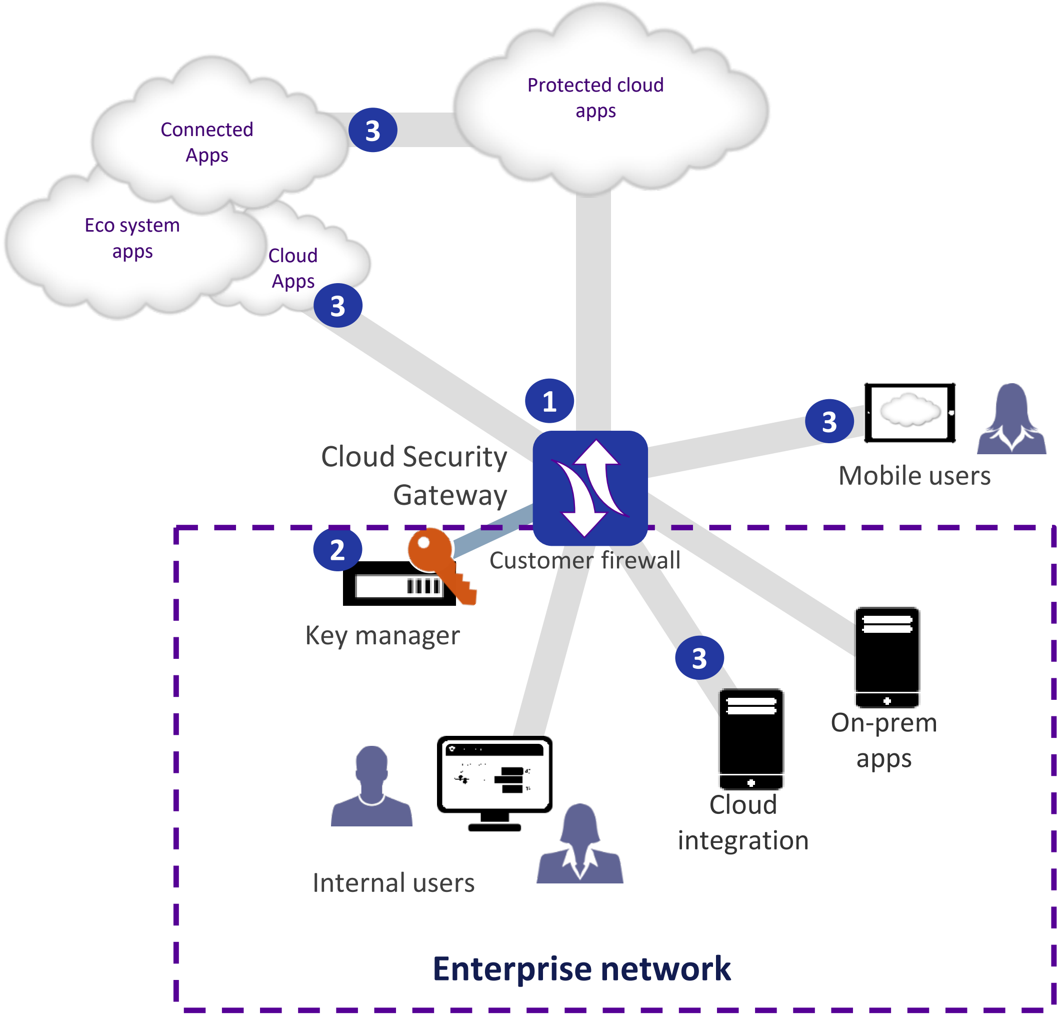
Here is a (wrapped) key, good until Friday

Your premises / your control

Cloud service provider

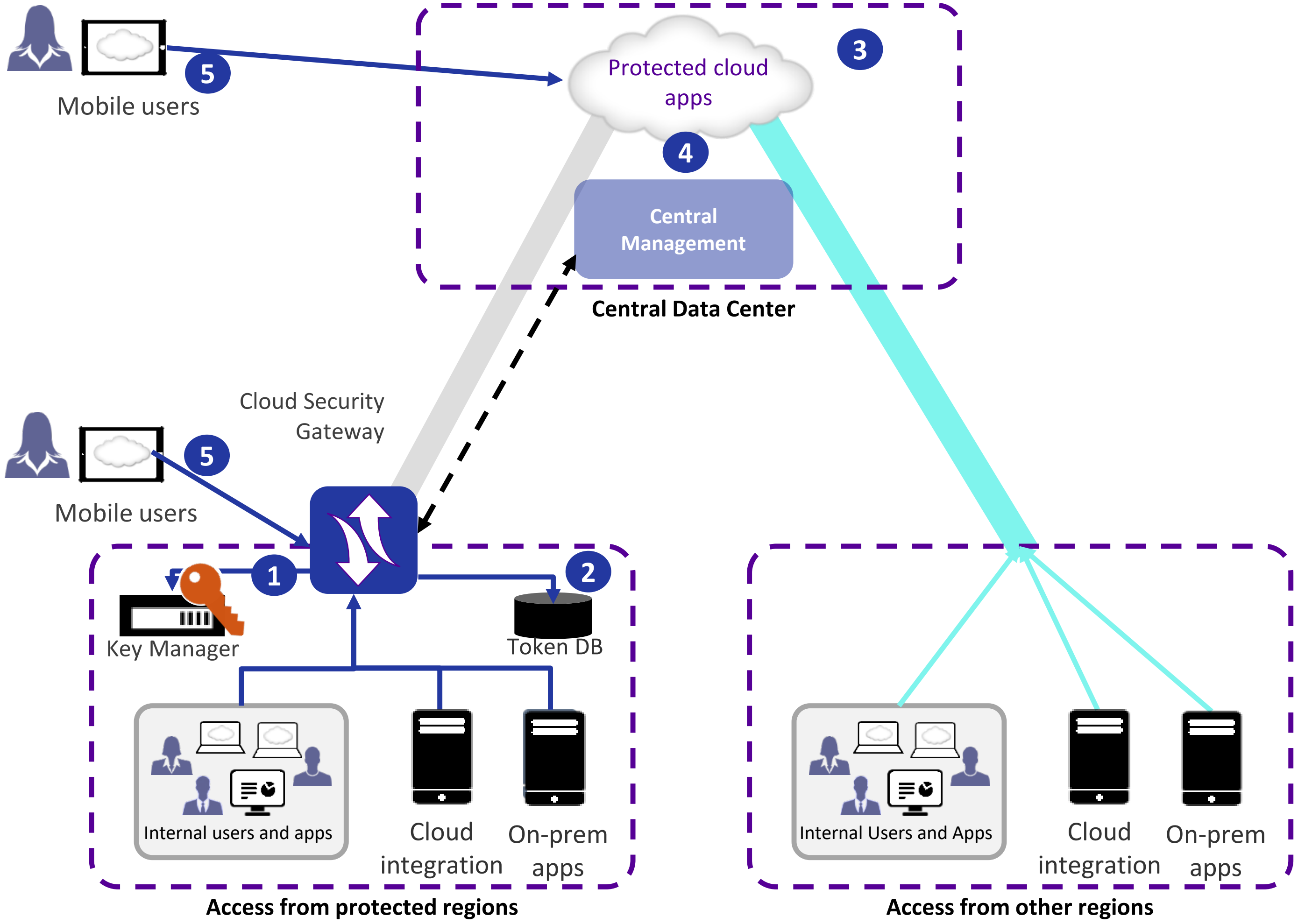
Key management architectural choices – cloud gateways

Multi-App Cloud Security Gateway



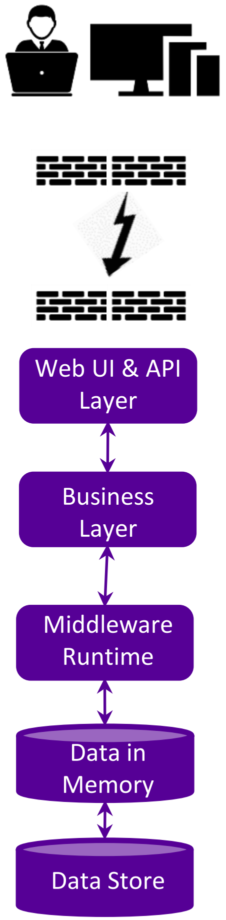
1. **Customers deploy cloud security gateway at their perimeter.**
   - CSG proxies traffic between enterprise and cloud applications.
   - CSG protects sensitive data (PII) before it leaves enterprise control.
   - Information remains protected at all times in the cloud, *even in cloud provider log files and big data repositories and generated reports.*
   - With CASB technologies, exported data can be protected on devices.
   - CSG encryption/tokenization is policy driven and can preserve:
     - Cloud application functionality: search, sort, report, filter
     - Formats: email, URL, phone number
2. **Customers have sole control of the encryption key.**
   - CSGs can manage the keys in leading HSMs.
3. **Connected cloud applications, on-prem applications, and mobile devices connect or integrate via CSG.**
   - Applications get policy-based access to protected or unprotected data.
   - CSG supports many forms of integration: HTTP(S), ODATA, REST, SOAP, SFTP, email, etc.
   - CSG supports many document formats: HTML, JSON, XML, CSV, XLS, PDF, DOC.

Key management architectural choices – advanced distributed cloud gateways



1. **Users and systems from protected regions access cloud applications via a CSG.**
   - Regional data remains protected at all times, in use and at rest, outside the region.
   - Data cannot be searched or sorted outside the region.
   - Users from unprotected regions can access directly.
2. **Encryption key/token DB is under regional control.**
   - Real data stays protected within the regional data center.
3. **Data can be processed by central application.**
   - For example, reports, invoices, POs, and HR letters can be generated.
   - Generated documents contain tokenized data.
4. **CSG and protection policy can be centrally managed.**
   - Gateway and tools can be deployed regionally.
   - Data can be encrypted or tokenized based on policy.
5. **Depending on access needs, mobile users will need to access the right regional CSG.**

Key management architectural choices - comparison



	End-to-end data flow	Cloud Security Gateway	BYOK for SaaS	Audit scope with BYOK
Enterprise	Enterprise Data	🔒 Audit	X	
	Enterprise Gateway	🔑 🔒	X	
	Internet / HTTPS	🔒	X	Crossing border
SaaS provider	SaaS Network FW	🔒	X	
	Web UI and API layers	🔒	X	
	Biz Application layer	🔒	X	Audit Scope
	Middleware/Runtime	🔒	X	
	Operating System	🔒	X	
	Servers, Hypervisor	🔒	X	
	Data in Memory	🔒	X	
	Data at Rest Storage	🔒 *	🔑 🔒 **	
	Physical Security	🔒	🔒	

Key is retained by customer

*****Key is shared with CSP***

CipherCloud

What can you do?

Today

- Up your cloud savvy…the cloud is a game changer.

This week

- Discover cloud applications in your environment.
- Classify applications -- by business use, architecture, and data use -- *before* you classify data.

This month

- Research cloud security vendors and technologies.
- Analyze risk. Develop a plan. Start small.
- Start blocking unwanted applications.

Next 3 months

- Leverage controls provided by the cloud service: authorization, access controls, data security, and monitoring.
- Discover and classify data in the cloud.
- Research and select the right data security strategy based on application types and usage – BYOK, CSG, CASB etc.
- Choose hybrid strategies to get the right balance between security and compliance: for example, BYOK for all fields, and CSG for limited fields.

Next 6 months

- Roll out enterprise-wide cloud controls, including data protection as needed.

RSA Conference 2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: BAC-F03

Questions?

Sundaram Lakshmanan

Chief Technology Officer
CipherCloud, Inc.
https://www.linkedin.com/in/sundaramlakshmanan