CLOUDSEC 2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
Data Protection Strategies with Cloud

陳昶旭, CISSP
Security Consultant, GCK
Thales CPL
The business environment is changing
Challenge: Compliance in a Cloudy World

GOAL: All data is secured

- Multiple borders and data silos
- Too many solutions, high management overhead
- Skills scarce and investment is prohibitive
- Individual SaaS providers become Crypto custodians
- Struggle to define a unified security policy
- Lost of portability and control
- Migration over time requires hybrid models

Result: 60% of data is NOT protected ..... 
.... which makes Data Protection and thus compliance TOUGH!!
APAC is MORE ready than most !!

<table>
<thead>
<tr>
<th>Rank, Economy</th>
<th>CRI 2018 Score (/100)</th>
<th>Rank Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>#01 Singapore</td>
<td>76.6</td>
<td>+1</td>
</tr>
<tr>
<td>#02 Hong Kong</td>
<td>74.1</td>
<td>-1</td>
</tr>
<tr>
<td>#03 New Zealand</td>
<td>71.1</td>
<td></td>
</tr>
<tr>
<td>#04 Japan</td>
<td>67.1</td>
<td>+1</td>
</tr>
<tr>
<td>#05 Taiwan</td>
<td>66.9</td>
<td>+1</td>
</tr>
<tr>
<td>#06 Australia</td>
<td>66.3</td>
<td>-2</td>
</tr>
</tbody>
</table>

Comparison with non-APAC economies

<table>
<thead>
<tr>
<th>Country</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>49.6</td>
</tr>
<tr>
<td>Germany</td>
<td>69.2</td>
</tr>
<tr>
<td>South Africa</td>
<td>50.1</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>61.0</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>73.5</td>
</tr>
<tr>
<td>United States</td>
<td>68.9</td>
</tr>
</tbody>
</table>

Source: Asia Cloud Computing Association
Enterprise Cloud Strategy

- **30%** Single Cloud
- **30%** Multi-Cloud (e.g. multiple providers without integration)
- **40%** Hybrid (e.g. integration between multiple providers, managed as a single cloud)

Resource: (ISC)2 2018 Cloud Security Report
Thread Landscape

Breached ever
60%

Breached in the past
- Last year: 30%
- Multiple times: 14%

Average cost of data breach
- $3.86M per case
- $148 per record

Threat actors

- Cyber-criminals
- Cyber-terrorism
- Hacktivists (non-national status with political goals)
- IT administrators with access to sensitive resources
- Partners with internal access
- Competitors (industrial espionage)
- Service provider accounts
- Executive management
- Ordinary (non-privileged) employee accounts

Source: Thales Data Threat Report 2019, IBM.com 2018

#cloudsec
No organization is immune from data security threats
# Broad Cloud Security Concerns

## 2018 Thales Data Threat Report

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks at the Service Provider</td>
<td>64%</td>
</tr>
<tr>
<td>Lack of control over location of data</td>
<td>62%</td>
</tr>
<tr>
<td>Security of my organization’s data in the cloud</td>
<td>58%</td>
</tr>
<tr>
<td>Multiple cloud encryption key management</td>
<td>58%</td>
</tr>
<tr>
<td>Custodianship of encryption keys</td>
<td>57%</td>
</tr>
<tr>
<td>Meeting compliance requirements</td>
<td>54%</td>
</tr>
</tbody>
</table>
Complex Environment is the Top Barrier to Data Security

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Concerns about impacts on performance and business process</th>
<th>Lack of budget</th>
<th>Lack of staff to manage</th>
<th>Lack of organizational buy-in/Low Priority</th>
<th>Lack of perceived need</th>
</tr>
</thead>
</table>

Source: 2019 Thales Data Threat Report Survey, IDC, November 2018
Enterprise Reality -- Islands of Encryption

Database Encryption
- Customer Records

Full Disk Encryption
- Physical Security

Data Masking
- PHI

Tokenization
- PCI

Cloud Encryption
- Cloud Migration

File Encryption
- Big Data

Access Policies
- Privileged User Control

$ + $ + $ + $ + $ + $ + $ + $

Each use case requires individual infrastructure, management consoles and training

Complex • Inefficient • Expensive
"It’s not that organizations don’t recognize the importance of **data security**; they clearly do. However, they realize that implementing data security is challenging and they need **better, simpler solutions** that allow them to address these challenges."
Shared Responsibility Model for Cloud Data Security

Infrastructure as a Service (IaaS)
- Data
- Application
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Platform as a Service (PaaS)
- Data
- Application
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Software as a Service (SaaS)
- Data
- Application
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

#cloudsec
You are responsible for data security. What do you do?
What First Comes to Mind When Protecting Data?

- Top six data security tools already deployed, or planned to be deployed in the next year.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Deployed Now</th>
<th>Planned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Encryption</td>
<td>92%</td>
<td></td>
</tr>
<tr>
<td>File Encryption</td>
<td>91%</td>
<td></td>
</tr>
<tr>
<td>Data Access Monitoring</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td>Cloud Native Encryption</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td>DLP</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td>Application Encryption</td>
<td>89%</td>
<td></td>
</tr>
</tbody>
</table>

Source:
2019 THALES DATA THREAT REPORT GLOBAL EDITION

#cloudsec
Edward Snowden:

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.”
IDC Recommendation: Encrypt Data and Control Your Keys

Encrypt Data At Rest

- Encryption is one of the most effective methods for protecting business information, personal data, and intellectual property

Centralize Key Management

- Build a robust key management infrastructure
- Essential components are a flexible key management platform, the data encryption, and access control


But Where To Put the Keys?

- EKM-04

- [Encryption] Keys shall not be stored in the cloud but maintained by the cloud consumer or trusted key management provider.
Bring Your Own Key (BYOK)
What is BYOK?

Utility for BYOK

wrappedData (key) with BYOK certificate

CSP KMS
BYOK

Keys Generated by local key store

Local Key Store (KMS/HSM)
Cloud Key Management Pain Points

- Encryption
- Key Visibility
- Data Loss
- Vendor Lock
- Attaining Compliance
- Key Lifecycle Mgmt
CipherTrust Cloud Key Manager

- Centralized, multi-cloud key control and management for IaaS and SaaS
- As a service or on-premises deployment
- Secure Key Storage
- Logging and Reporting for enhanced visibility and compliance
BUT...
Different environment has different encryption mechanisms...

Different Cloud Service Provider has different Key Management practices...
Bring Your Own Encryption (BYOE)
On-Premises HSM as Root of Trust

- AWS
- Azure
- IBM

File Server
- VM
- Protect V

Database
- VM
- Protect File
- TDE

ProtectApp
- VM

KMS

#cloudsec
Encryption Data at Rest – How to Protect Data Against Threat

Data Flow

- Users, Browsers, Mobiles, Apps
- Application Layer
- Databases / SQL Layer
- File System Layer
- Storage

Protection points:
- Endpoint Admins
- App Admins
- DB Admins
- Sys Admins
- Storage Admins
Challenge

- Must support multi-cloud, hybrid cloud environment such as AWS, Azure, VMWare, IBM Softlayer...etc.
- Encryption keys must be centralize store and management. A unified key management policy. Encryption keys will never store in any application or devices.
- Requirement for high security, high availability, and future scalability. Provide security controls such as audit logs, access control.
- Must be able to integrate with third-party solutions such as cloud encryption gateway, database encryption, and storage encryption solutions.
Phase I – VM Disk Encryption

On-Prem Prod. HSM Cluster

On-Prem DR HSM Cluster

Cloud A

KMS Cluster

Disk are encrypted over 1000 VM Servers
Windows Server, RedHat, Ubuntu... etc.

#cloudsec
Phase II – Expand Usage

On-Prem Prod.
- HSM Cluster

On-Prem DR
- HSM Cluster

Cloud A
- KMS Cluster
- VM Encryption

Database encryption with various databases such as Oracle, SQL Server, DB2. Keys are stored and managed by a centralized KMS.

#cloudsec
Phase III – Expand to Multi-Cloud

On-Prem Prod.
- HSM Cluster

Cloud A
- KMS Cluster
- VM Encryption
- DB Encryption

Cloud B
- VM Encryption
- DB Encryption

On-Prem DR
- HSM Cluster
Future

On-Prem Prod.
- HSM Cluster

Cloud A
- KMS Cluster
- File Encryption
- Document Signing
- De-identification
- Applications

Cloud B

Storage
- Tape
- File Server
- Application

#cloudsec
KEEP CALM AND ENCRYPT
THANK YOU

陳昶旭, CISSP
Security Consultant, GCK
Thales CPL