CLOUDSEC2019

PICTURE THIS!

SEE. SECURE. GO FURTHER.

CLOUDSEC2019

PICTURE THIS!

SEE. SECURE. GO FURTHER.

"Trust Me. Your Data is Safe."

Joseph Ling | Senior Solutions Architect
@nCipherSecurity

nCIPHER
AN ENTRUST DATACARD COMPANY

Data: The Most Valuable Strategic Asset in the World

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

British Airways faces record $230 million fine over data theft

LONDON (Reuters) - British Airways-owner IAG is facing a record $230 million fine for the theft of data from 500,000 customers from its website last year under tough new data-protection rules policed by the UK's Information Commissioner's Office (ICO).

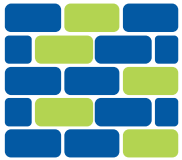
The ICO proposed a penalty of 183.4 million pounds, or 1.5% of British Airways' 2017 worldwide turnover, for the hack, which it said exposed poor security arrangements at the airline.

BA indicated that it planned to appeal against the fine, the product of European data protection rules, called GDPR, that came into force in 2018. They allow regulators to fine companies up to 4% of their global turnover for data-protection failures.

https://reut.rs/2S7OWBK Reuters, 8 July 2019

Most Products Nowadays Do Protect Data

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



Network Security Appliance

SSL/TLS

Databases

TDE

(Privileged) Identity Management

Credential Vault

Cloud Service

Key Vault

They do protect Data properly

Do you feel safe?

Data Security "Anxiety"

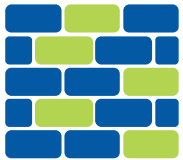
- **Reasons that you may not feel very comfortable:**
  - Systems are isolated and fragmented
  - Products are constrained by the environment
  - Risks are linked to vulnerabilities in products
  - Trust is based on the entire infrastructure
- **Data is usually assumed to be safe**
  - Network Security Appliance: **Certificates**
  - Database: **Encryption Keys**
  - Privileged Identity Management: **Credentials**
  - Cloud Service: **Keys**

Understanding Hardware Security Module (HSM)

Hardware
Security Module

- Is a cryptographic device that generates, uses, and stores **Keys** and their related functions, such as encryption
- Is able to **centralize** the Keys, a.k.a. the most sensitive data in the environment
- Is one of the most **robust** cybersecurity devices with tamper resistant capability (FIPS 140-2 Level 3 Certified)
- Has been a **trusted** tool for top-level Data Security for years

How to Enhance Network Security Appliance?



Network Security Appliance

There is sensitive data getting through

Enforce SSL to encrypt the traffic

↓

Decrypt and inspect the traffic for antivirus, anti-spyware, network forensics, etc.

↓

Protect the Certificates (Keys) by Hardware Security Module (HSM)

The risk is transferred to HSM

How to Enhance Identity Management?

Manage the Identities

(Privileged) Identity Management

Protect the privileged accounts by privileged identity management (PIM) product

There are various rights and permissions

Activate the encryption in the PIM product

The risk is transferred to HSM

Protect the encryption Key by Hardware Security Module (HSM)

How to Enhance Database Encryption?

Databases

There are data files in Servers

Activate the encryption (Transparent Data Encryption, TDE) in the Database product

Protect the encryption Key by Hardware Security Module (HSM)

The risk is transferred to HSM

How to Enhance Cloud Service Security?

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Cloud Service

There are lots of data in these Services

Subscribe the Key Management Service

↓

Encrypt the data in the Services using the Keys in the Key Management Service

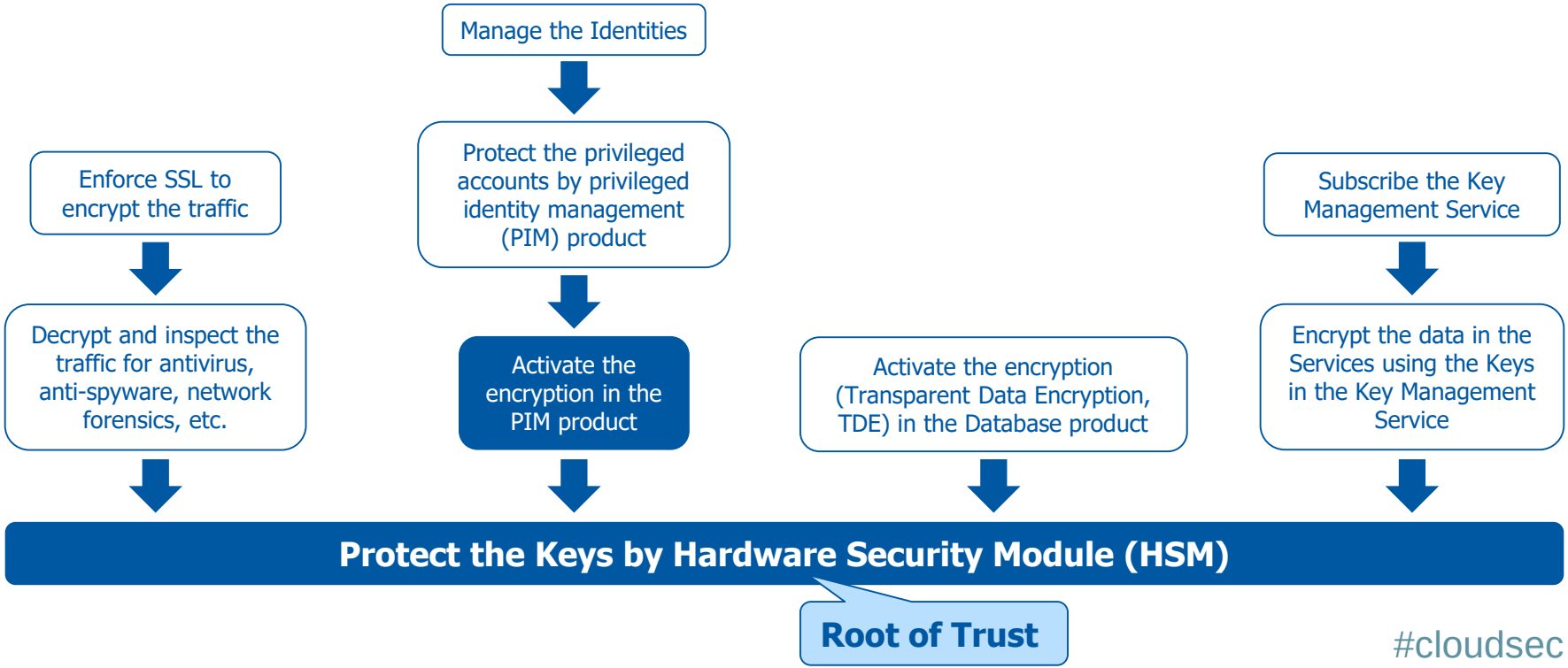
↓

Protect the Keys in the Key Management Service by Hardware Security Module (HSM)

The risk is transferred to HSM

Most Cybersecurity Products Come from the Same Origin

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



Protecting the Keys in products by Hardware Security Module (HSM) **simplifies** and **consolidates** the Data Security in the entire infrastructure

However, HSM is a **hardware**,
could I utilize it for cloud environments?

Key Management Service and Key Vault

Cloud Service

There are lots of data in these Services

Subscribe the Key Management Service

A service from Cloud Providers, utilizing the **HSMs** in their datacenters

You will be provisioned a "Key Vault", which is a logical location storing your Keys in the Cloud

Protect the Keys in the Key Management Service by Hardware Security Module (HSM)

How Your Data is Encrypted in Cloud

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

2. Data Encryption Key (DEK) is **generated by** the Cloud and **stored in** the Key Vault

3. Data Encryption Key (DEK) is **delivered to** the Cloud Service

4. The Cloud Service **uses** the Data Encryption Key (DEK) to **encrypt** the data in the Service

Cloud Key Vault

Secured Cloud Service
(e.g. Storage, Database TDE)

1. The Master Key encryption Key (KEK) is usually **generated** when the Key Vault service is **activated**

6. Data Encryption Key (DEK) is usually **protected / encrypted by** the Master Key encryption Key (KEK) in the Key Vault

5. The Data Encryption Key (DEK) could be **deleted** after validity period

What are the Responsibilities?

Self Managed

Provider Managed

On Premise	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Physical Servers	Physical Servers	Physical Servers	Physical Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Cloud infrastructure offers **the same or even more** than traditional on premise infrastructure

However, all resources are literally **the Provider's asset**

How Bring Your Own Key (BYOK) Works

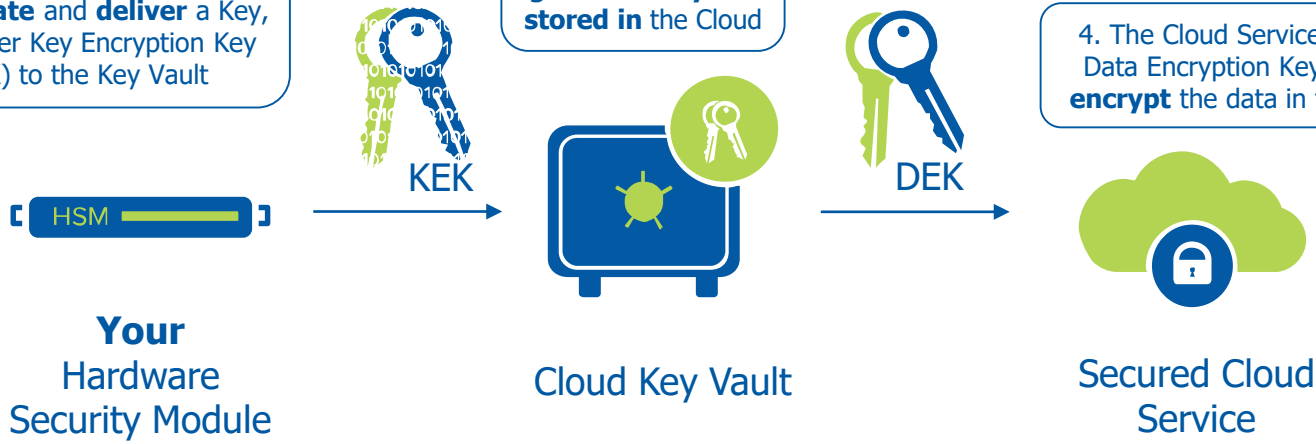
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

1. Cloud **requested** the Hardware Security Module (HSM) to **generate** and **deliver** a Key, the Master Key Encryption Key (KEK) to the Key Vault

2. Data Encryption Key (DEK) is **generated by** and **stored in** the Cloud

3. Data Encryption Key (DEK) is **delivered to** the Cloud Service

4. The Cloud Service **uses** the Data Encryption Key (DEK) to **encrypt** the data in the Service



Your Hardware Security Module

Cloud Key Vault

Secured Cloud Service

7. Key Encryption Key (KEK) could be **deleted** in the Cloud after validity period and has to be **retrieved from** Hardware Security Module (HSM) again

6. Data Encryption Key (DEK) is usually **encrypted by / generated from** the Key encryption Key (KEK)

5. The Data Encryption Key (DEK) could be **deleted** after validity period

Key Management Service vs Bring Your Own Key

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

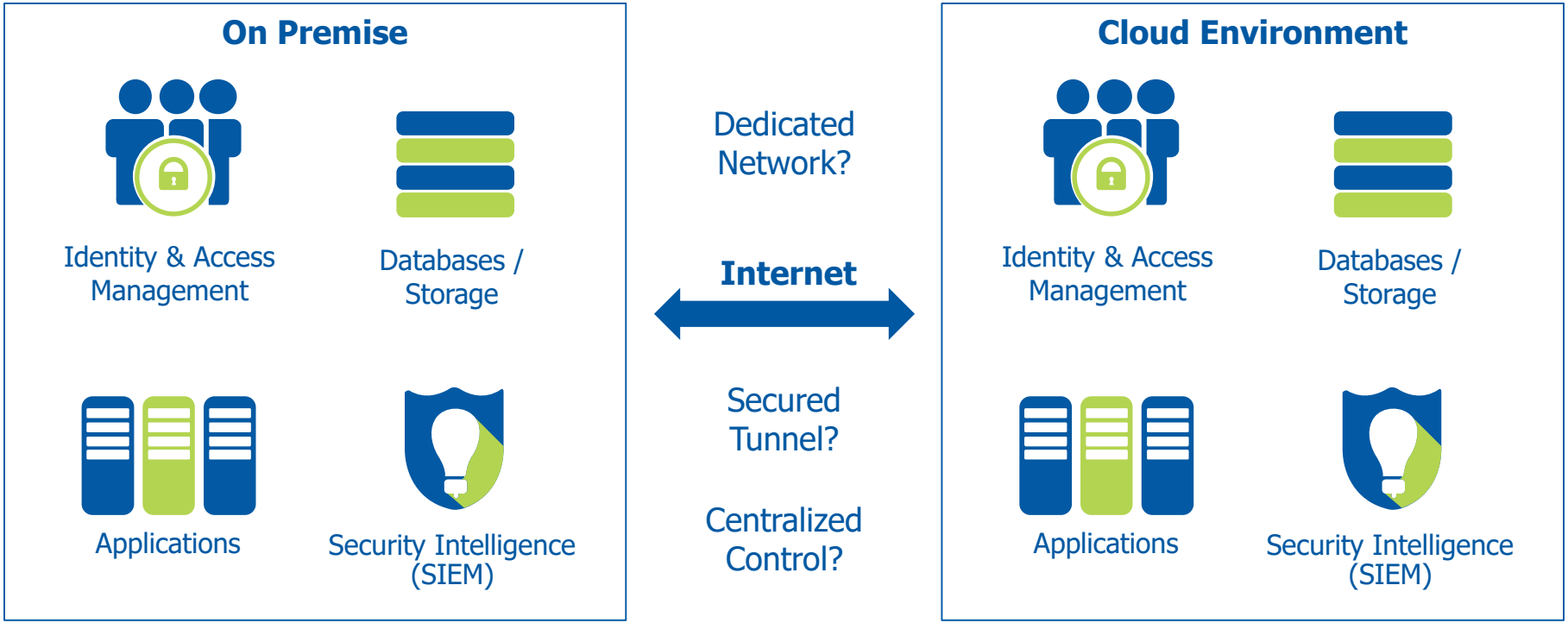
Cloud Key Vault

Bring Your Own Key

Cloud Key Vault	Bring Your Own Key
You have proper Key management	You have proper Key management
You are granted **Privileges**	You have **Ownership**
You can manage Keys	You can manage Keys
	You can encrypt Data, validate Signature, etc.

More Complicated When the Cloud is Hybrid

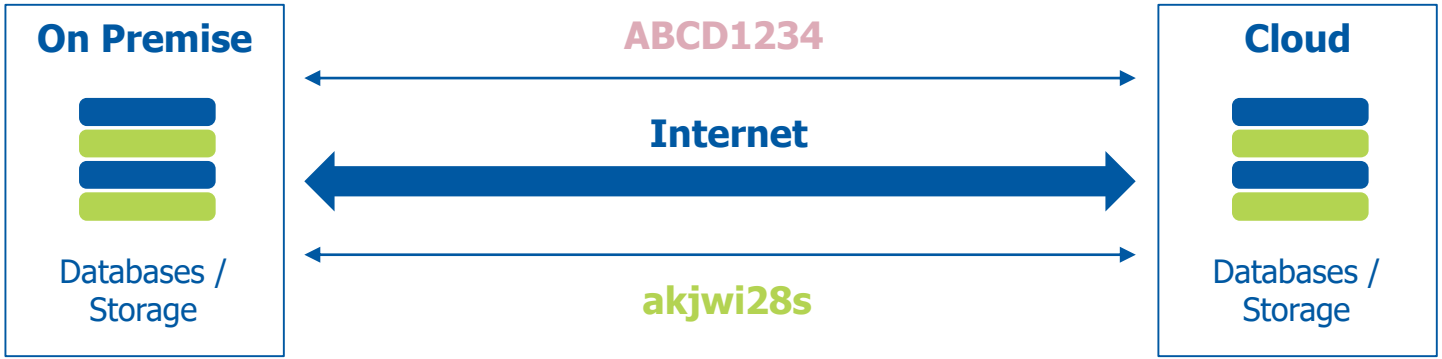
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



Security Regardless of Infrastructure

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

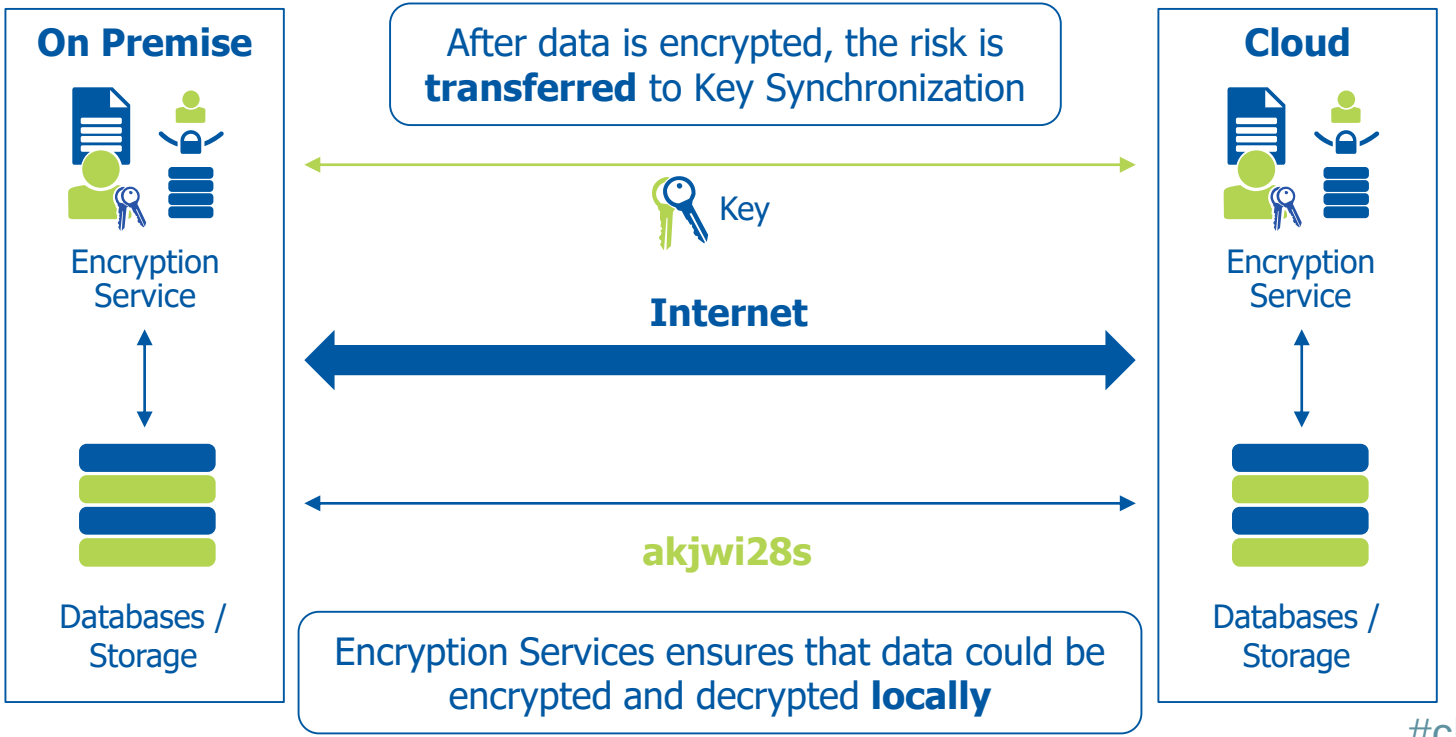
Network Security: If data is sync in plain text, the protection is subject to network



Data Security: If data is sync in ciphertext, data is protected anywhere

Data Security: Transferring the Risk

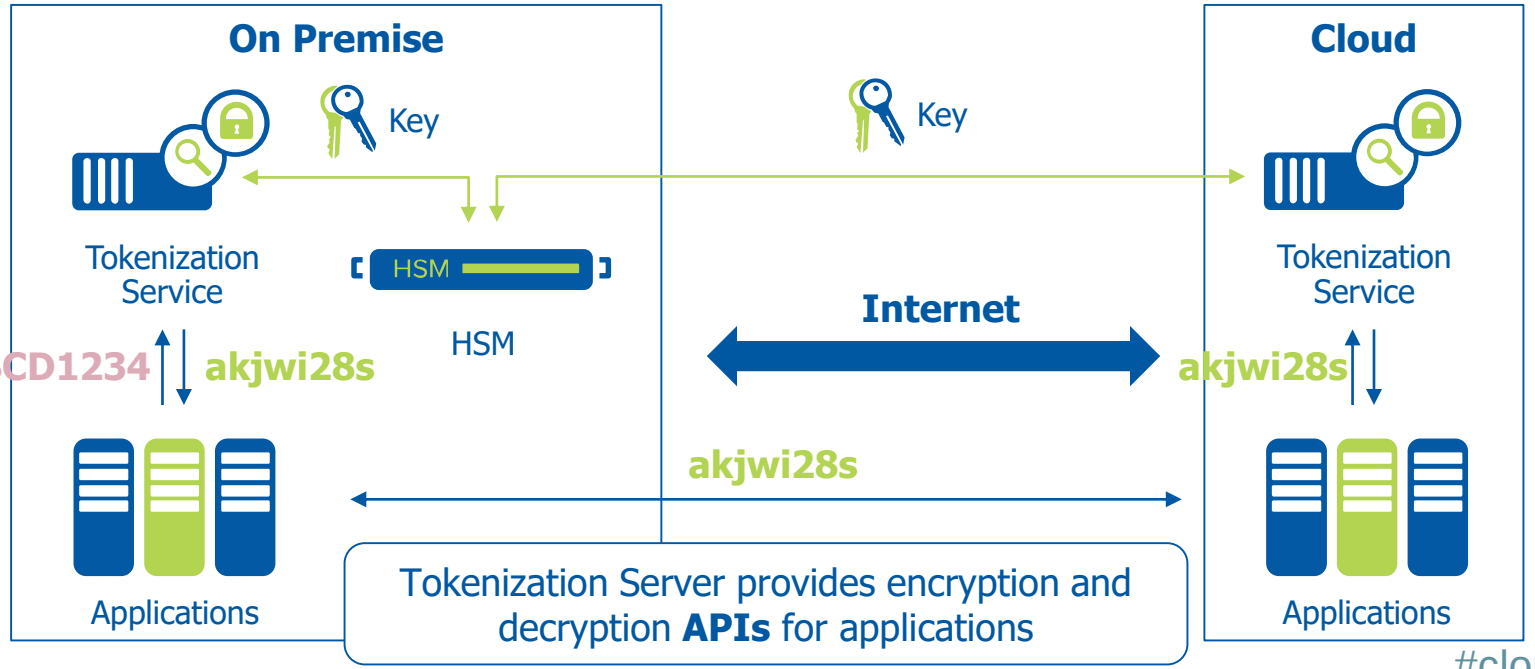
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



Hybrid Cloud Encryption: Encryptions in Applications

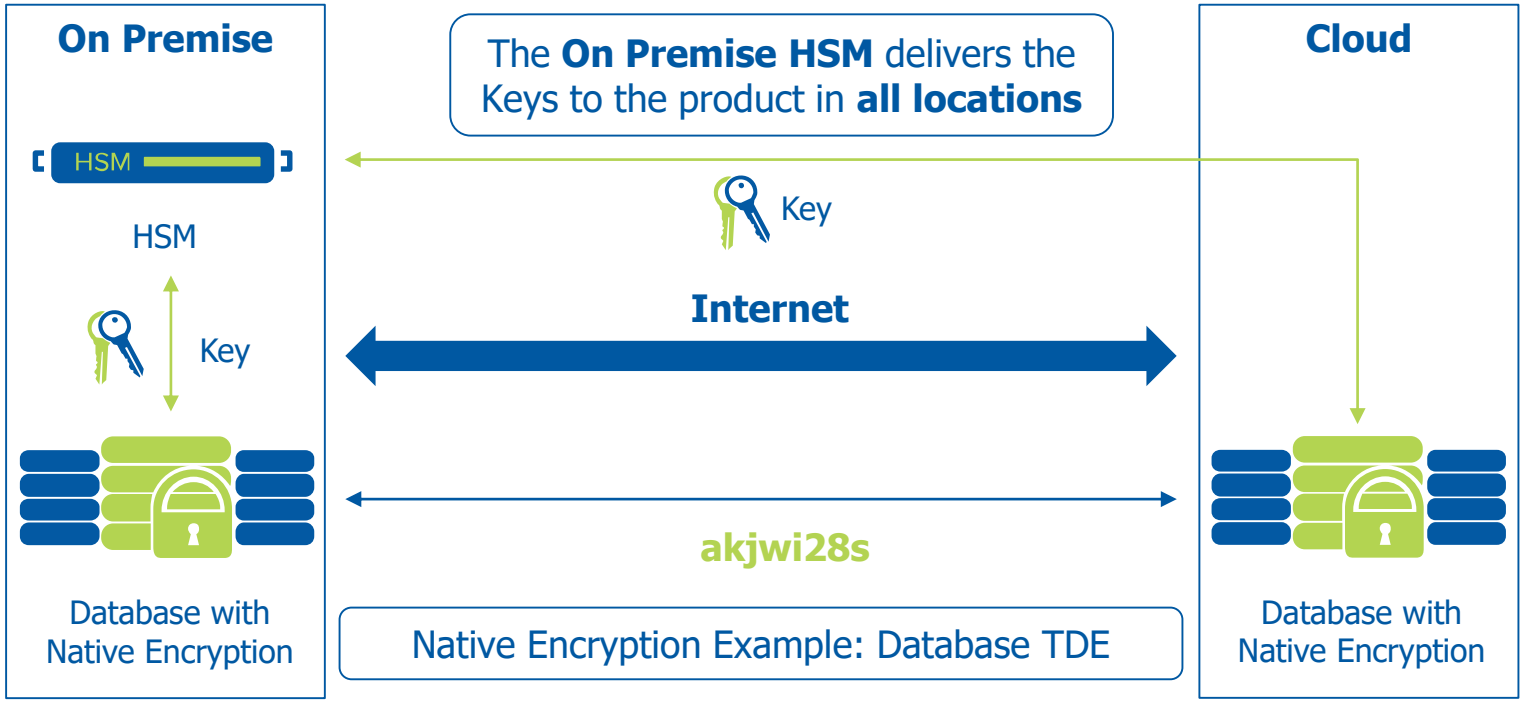
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

The **On Premise HSM** delivers the Keys to Tokenization Service in **all locations**



Hybrid Cloud Encryption: Native Encryption

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



Key Management Service vs Bring Your Own Key

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Cloud Key Vault

You have proper Key management

You are granted **Privileges**

You can manage Keys **in Cloud Services** only

Bring Your Own Key

You have proper Key management

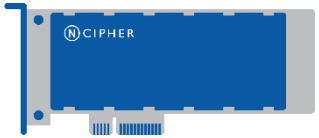
You have **Ownership**

You can manage Keys **on Premise and in Cloud Services**

You can encrypt Data, validate Signature, etc.

nCIPHER
AN ENTRUST DATACARD COMPANY

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.


nCipher is an **HSM market leader** with a long history of industry certifications and validation

Cloud Enabled Security

Data Ownership and Privacy

Enterprise Level Encryption

Digital Signature and Identity

nCipher creates **solutions delivering trust** for business critical applications and information

nCipher Services

nCIPHER
AN ENTRUST DATACARD COMPANY

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

PKI Professional Services

Design, deploy and manage world-class PKIs

Custom Cryptographic Solutions

Leverage our knowledge to protect your customers

Training and Certification

Learn best practices

Product Deployment

Complete important data protection projects quickly and correctly

nCipher Services comprise local experts, accelerate deployments, learn best practices, and maximize return on your investment in data protection and security solutions


CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
THANK YOU
Joseph Ling | Senior Solutions Architect
@nCipherSecurity
nCIPHER
AN ENTRUST DATACARD COMPANY
www.cloudsec.com | #cloudsec