THALES

Digital Sovereignty: your data, their cloud

How to achieve Data, Software and Operational Sovereignty

Simone Mola
Regional Sales Manager
Thales CPL

Today's world

GOVERNANCE

The digital transformation accelerates the move of assets to untrusted environments: the cloud.

Cloud changes everything as assets move beyond the walls.

THALES

Today's world

GOVERNANCE

The digital transformation accelerates the move of assets to untrusted environments: the cloud.

RISK

Cyberattacks are growing and changing fast. Identity theft is the root, lost data the consequence.

of breach incidents came from **identity theft**

Breaches involving **unencrypted data**

THALES

Today's world

Governance

The digital transformation accelerates the move of assets to untrusted environments: the cloud.

Risk

Cyberattacks are growing and changing fast. Identity theft is the root, lost data the consequence.

Compliance

Regulation on data privacy is everywhere. Efficient controls are required in hybrid IT.

organizations reported a breach or **compliance audit** failure in the past year.

THALES

Impact of digital transformation

GOVERNANCE

Cloud Shared Responsibility

RISK

COMPLIANCE

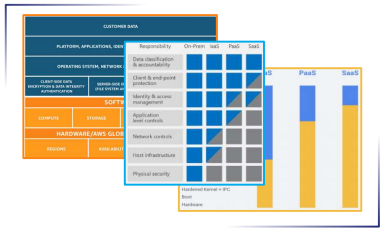
Control

← **USERS** responsibility

Cloud data Security

Cloud Infrastructure security

Responsibility: **CSP**→



THALES

Cloud Shared Responsibility

GRC impact of digital transformation

Cloud Shared Responsibility

GOVERNANCE

User cloud controls
- Data
- IAM
- Apps (I/PaaS)
- Key lifecycle/ctrl
- North/South Traffic

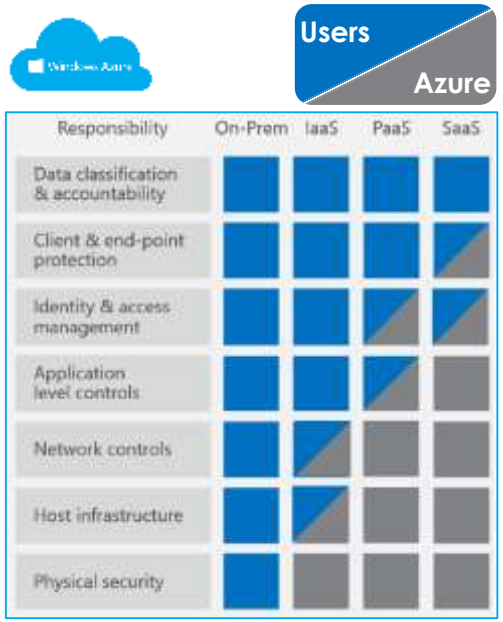
← **USERS** responsibility

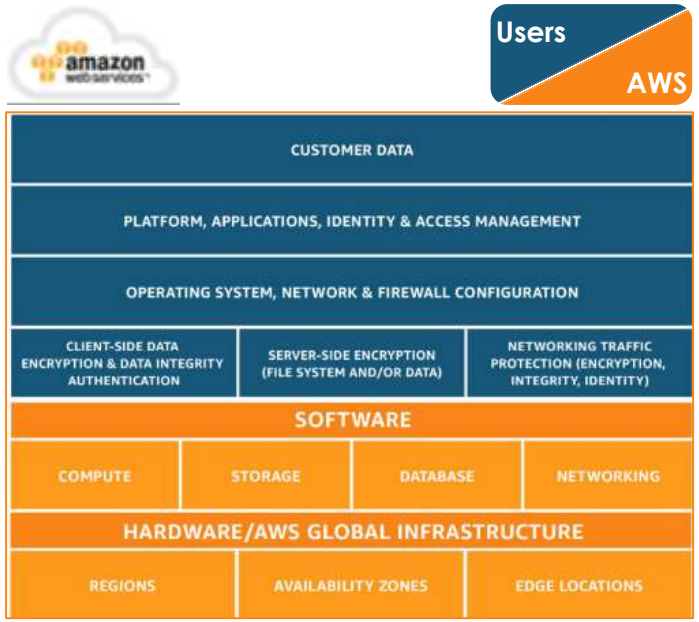
Cloud data Security / Cloud Infrastructure security

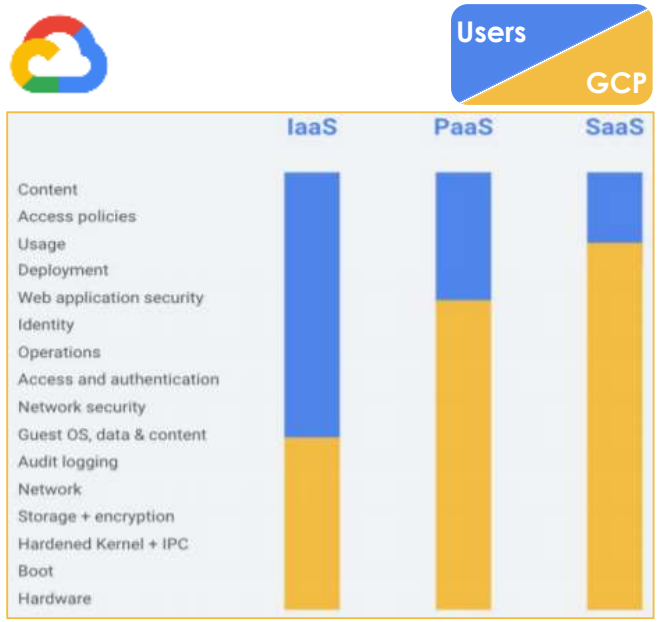
Responsibility: **CSP**→

Governance of Hybrid IT

- Big change: **cloud = a shared responsibility**
- Segregation of controls between the assets (identity, data, flows) and the infrastructure, the service







THALES

Impact of digital transformation

GOVERNANCE

Cloud Shared Responsibility

RISK

Top Cloud Security Risks

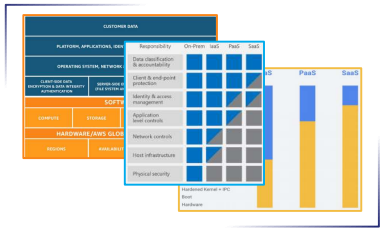
COMPLIANCE

Data privacy regulation

Control

← **USERS** responsibility

Responsibility: **CSP**→



Isolation

Top Cloud Security risks:

- Data Protection
- Isolation Failure
- Data Deletion
- Malicious Insider

Digital sovereignty

Regulations:

- GDPR, UKDP, CCPA
- PCI, PSD2, Telco, Hipaa
- ISO27001, CSA

THALES

What is digital sovereignty?

> Digital sovereignty refers to the ability to have control over your own digital destiny – the data, hardware, and software that you rely on and create.

WORLD ECONOMIC FORUM

THALES

How big is the digital sovereignty problem?

92%

of all the data in the western world is stored on US-owned servers[1]

$1.3 Trillion

Spending on cloud services, will surpass $1.3 trillion in 2025[2]

1: World Economic Forum: What is digital sovereignty and why is Europe so interested in it?
2: IDC: Worldwide Whole Cloud Forecast, 2021–2025

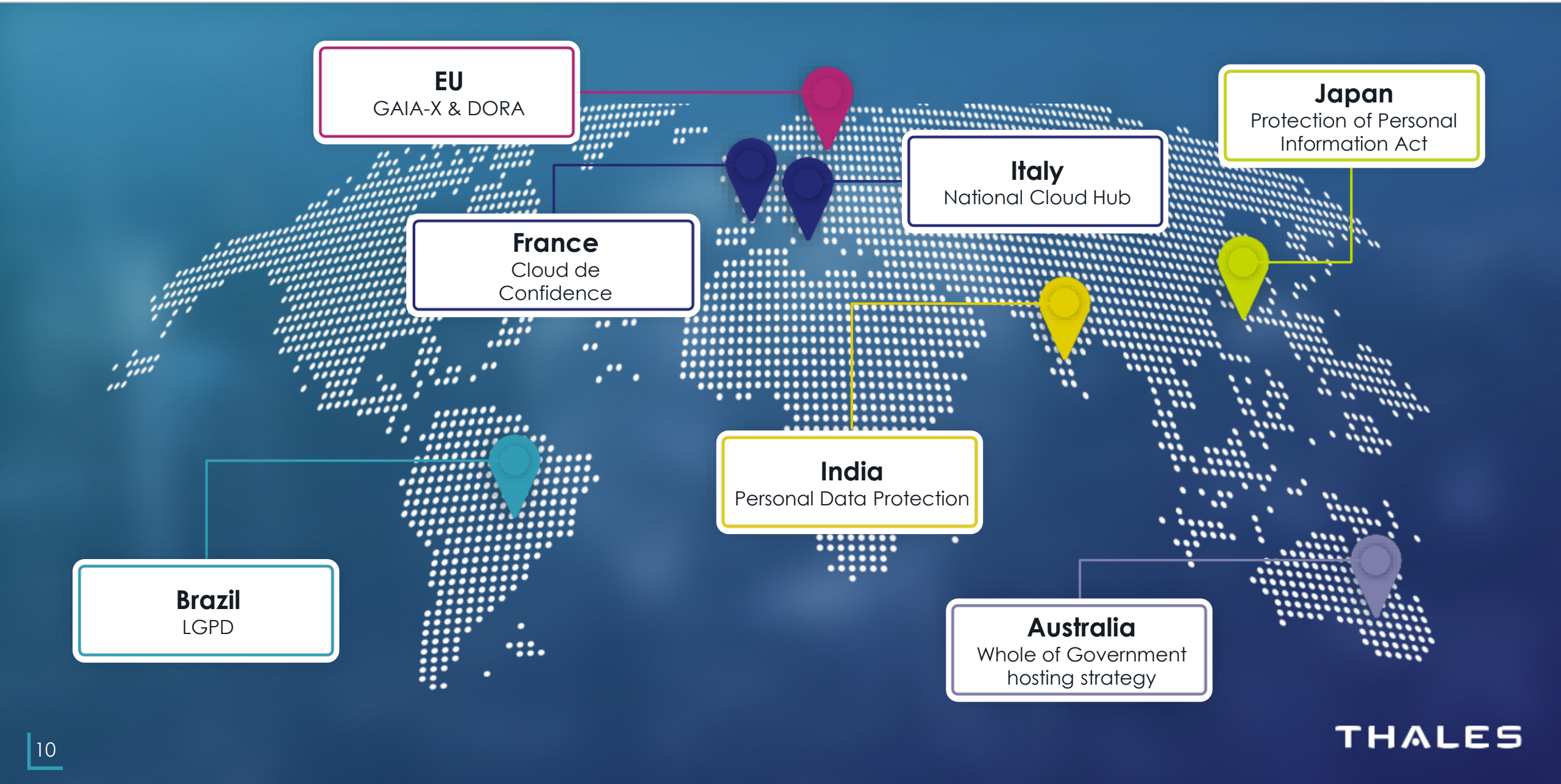
The concentration of data in just a few US-based platforms creates a situation of high dependence and a challenge for business resilience.

Digital sovereignty has become an important topic for many nation states, and new regulations from GDPR and Schrems II, to Gaia-X and DORA, emerge to manage these risks.

The challenges brought by digital sovereignty directly impact the entire cloud services industry.

THALES

Cloud sovereignty becomes a hot topic for governments around the world

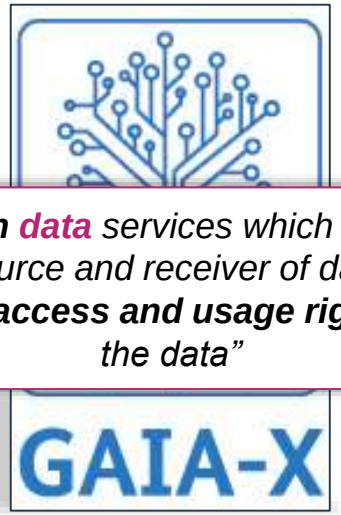


THALES

Moving fast from regulatory to societal & legislative matters

Gaia-X

- COVID highlighted gaps in **IT sovereignty** and dependency to US and China



*"**sovereign** **data** services which ensure the **identity** of source and receiver of data and which **ensure the access and usage rights** towards the data"*

Europe

- New EDBP supplementary measures guidance follows **Schrems-II ruling**

*"Personal **data** is processed using **strong encryption**"*
*"the **keys** are reliably **managed**" and "retained solely **under the control** of the data exporter"*

USA

- Following cyber attacks on critical infrastructure, **Prᵗ Biden Executive Order**

*"**Within 180 days** of the date of this order, agencies shall adopt **multi-factor** **authentication** and **encryption** for **data** at rest and in transit."*

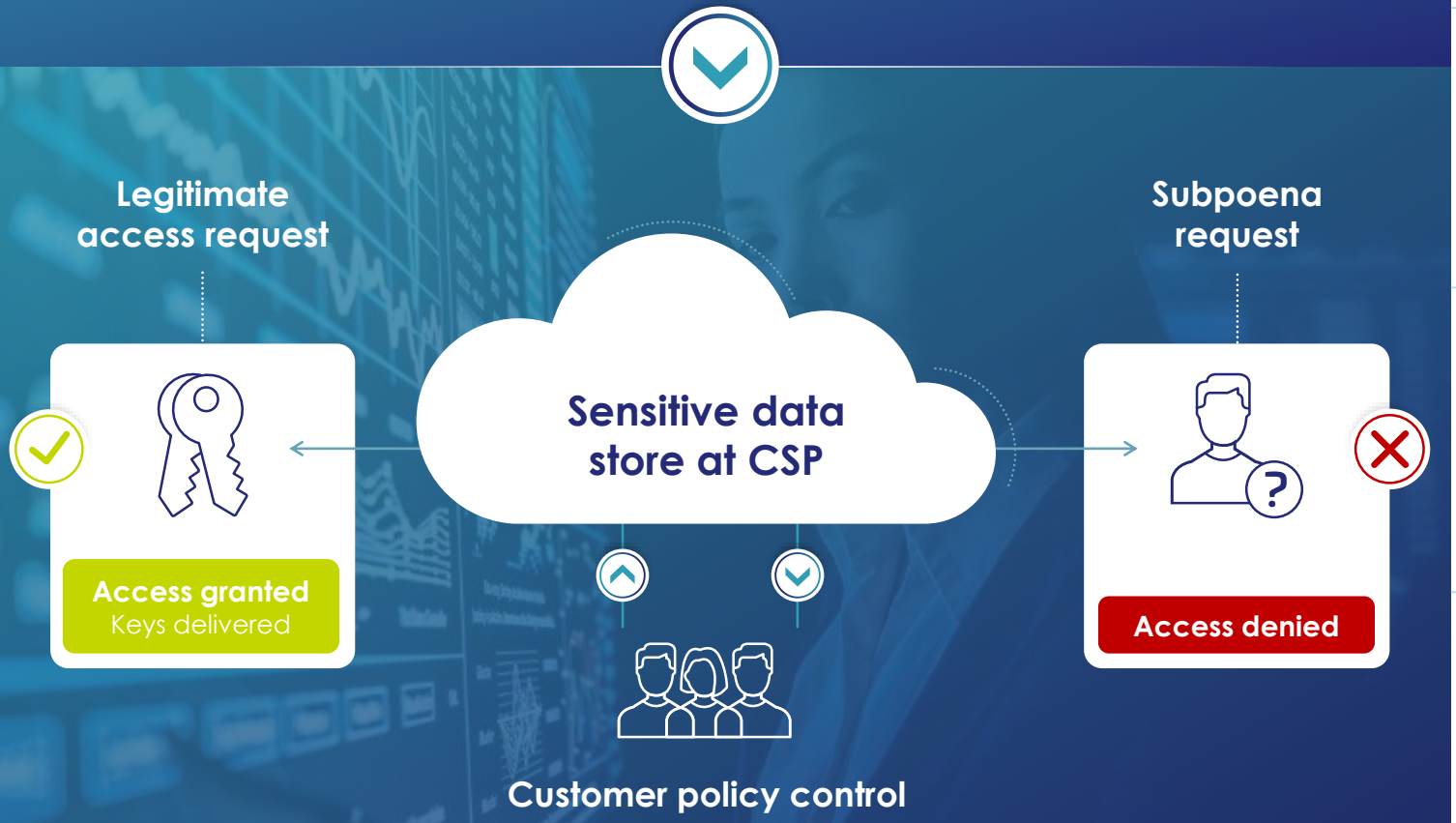
Sources:
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

THALES

Data Sovereignty example

Protect against subpoena threat

Data Sovereignty enables organizations to protect sensitive data from subpoena requests from foreign states to the CSP



Data sovereignty mitigates the threat of a foreign state issuing a **subpoena** to access private data in the clear.

Encryption keys must be held and controlled by the customer in the proper geographic legal jurisdiction.

An unauthorized subpoena request to the CSP would be denied by the customer policy control, if the customer has ownership of the keys.

This approach to key management was recommended by the European Data Protection Board.

THALES

Operational Sovereignty example

Prevent unauthorized access

Operational Sovereignty enables organizations to stop external attackers and even the CSP and its employees from accessing sensitive data in the cloud

Operational sovereignty ensures that **only authorized users or processes** with a valid reason and permission may access sensitive workloads.

Thales helps organizations mitigate risks by discovering, classifying and encrypting sensitive data as well as controlling the encryption keys to these sensitive files.

Unless a valid reason to access the data is provided, sensitive data stored in the cloud will not be accessible to unauthorized users.

THALES

Software Sovereignty example

Move workloads between clouds

Software Sovereignty increases the portability of workloads between on-premises and various cloud platforms

Consolidate 1000s of key stores externally, manage in one place using a single pane of glass

Software sovereignty enables **portability of workloads** between different cloud platforms as well as on-premises systems.

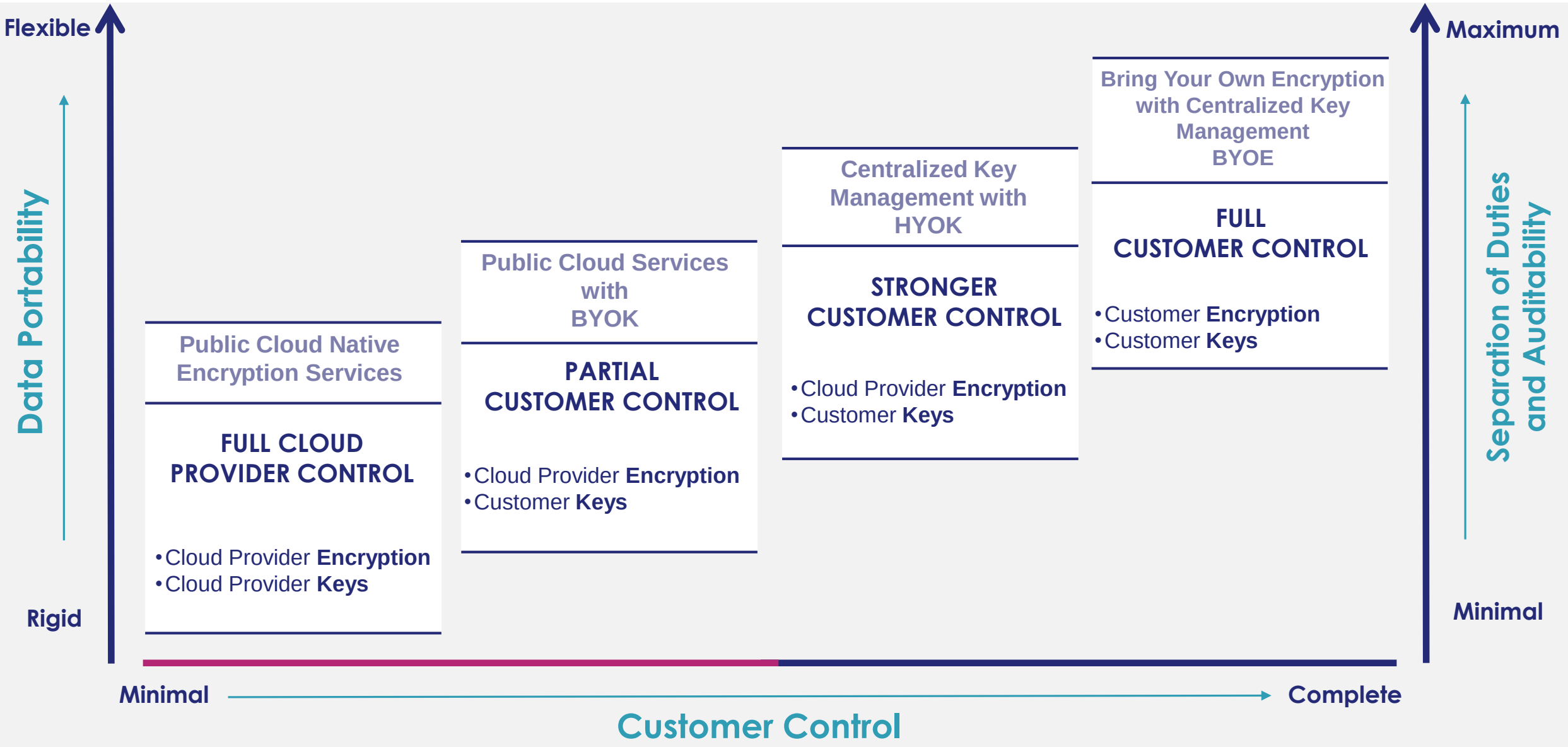
Thales can help streamline the task of external key management by consolidating keys from multiple clouds into a single pane of glass.

This increases operational efficiency through harmonization and automation, and reduces operational costs, risk of errors, and data breaches.

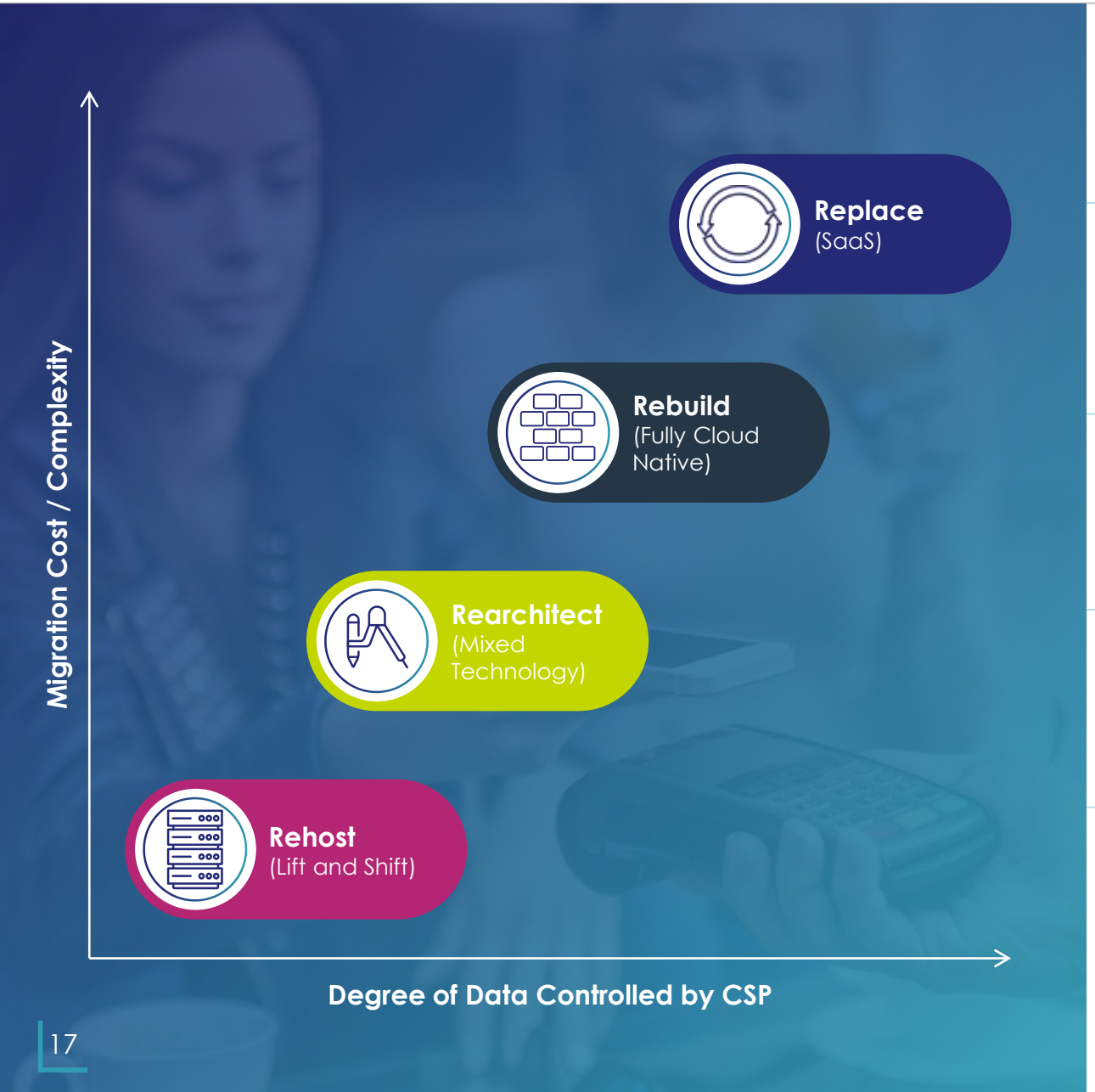
THALES

Cloud Security – The Encryption Key is Key

Data Protection Options for the Cloud



Thales supports all cloud migration approaches



Organizations are taking different approaches for cloud migration, including:

Re-hosting Virtual Machines (VMs) via Lift and Shift into an IaaS environment, redeploying existing data and applications on the cloud server.

Re-architecting applications with major code changes to take advantage of micro services and other cloud features.

Rebuilding a fully cloud native app from scratch, discarding the existing code base and replacing it with a new one built for the cloud.

Replacing legacy applications and migrating to a third-party, prebuilt application provided by a vendor with a SaaS model.

THALES

Thales sovereign controls for Hybrid IT

Thales sovereignty-enhancing controls for Hybrid IT help organizations **simplify governance**, achieve **regulatory compliance**, and **reduce risk** in the cloud.

Data Discovery and Classification: Enable organizations to identify where their data is located, classify it by risk and according to regulations, and automatically apply robust security measures.

Encryption and Tokenization: Allow organizations to secure all types of sensitive data across a variety of data stores, platforms, and IT environments, both at rest and in-motion.

Key Management: Streamline control across multiple on-premises and cloud systems enabling organizations to set granular policies and apply the right security control for sensitive data in virtually any situation.

THALES

Data & Cloud Security – How Thales CPL can help

A three-layered Architecture

- Combining hardware and software to protect data both on-premise and in the Cloud(s)

③ Software Connectors

Tokenization with Data masking

Application encryption

VAULT

CLOUD Key Manager

Transparent encryption

② Enterprise Key Manager

Hardware or Virtual

Use-cases:
> Symmetric encryption
> KMS, KMIP
> Thales connectors:
> Application encryption
> Database encryption

> TDE integration
> File-system encryption

① General Purpose Hardware Security Modules

Hardware

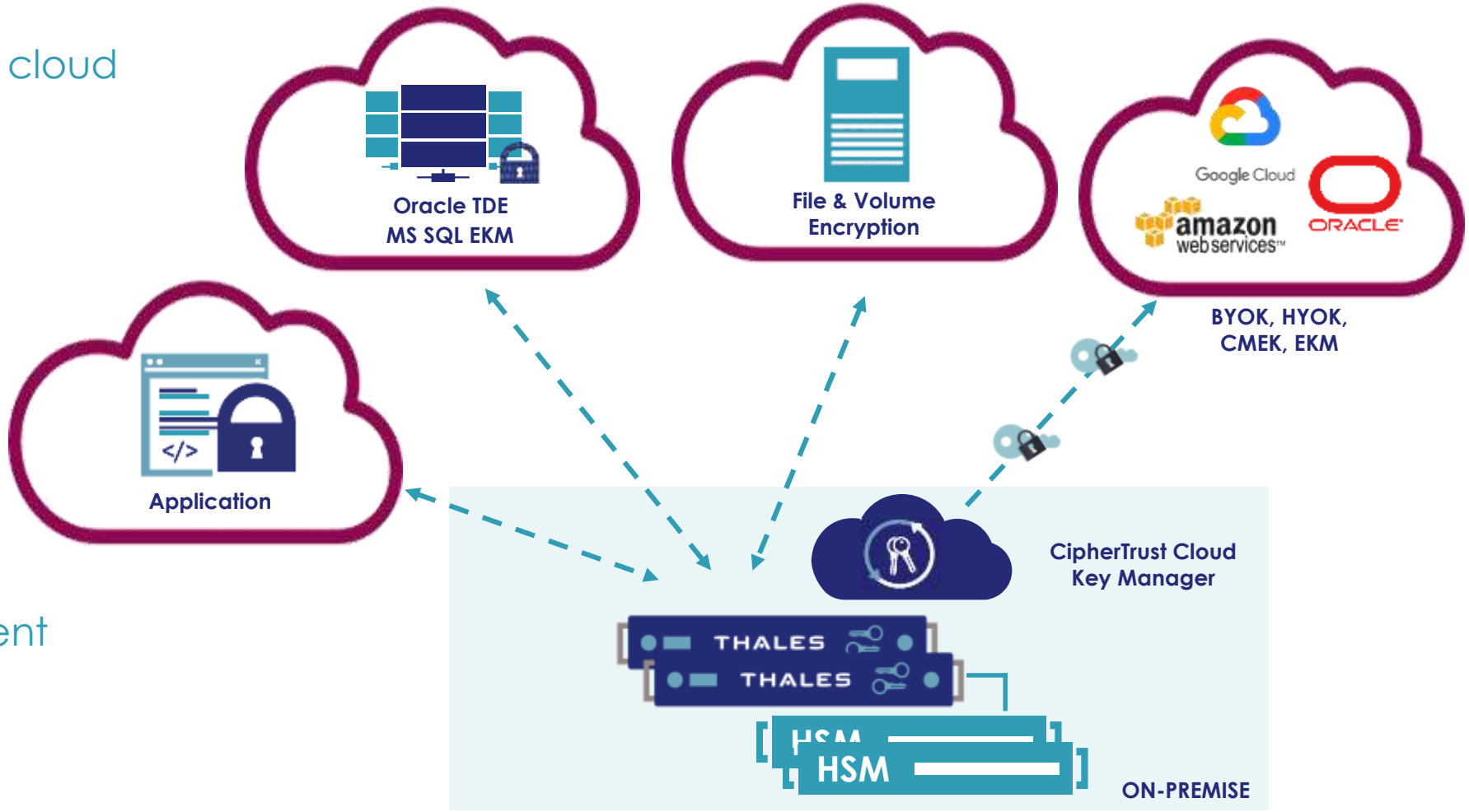
Use-cases:
> Asymmetric encryption
> CAs and PKI (IoT)
> Application encryption
> Database encryption (TDE integration)

> SSL/TLS offload
> Key generation (Cloud Key Vault integration)
> Code/Document signing
> Blockchain

THALES

Success case – Italian PA

Needs: secure migration to cloud with data sovereignty



How:

- External key management
- Native CSP encryption
- Native DB encryption
- Volume encryption
- Application encryption

THALES

CipherTrust Data Security Platform Products

Thales CipherTrust Data Security Platform

Discovery

Discovery and Classification

Encryption and Tokenization

File System Transparent Encryption

Database Protection

Application Data Protection

Tokenization

Key management

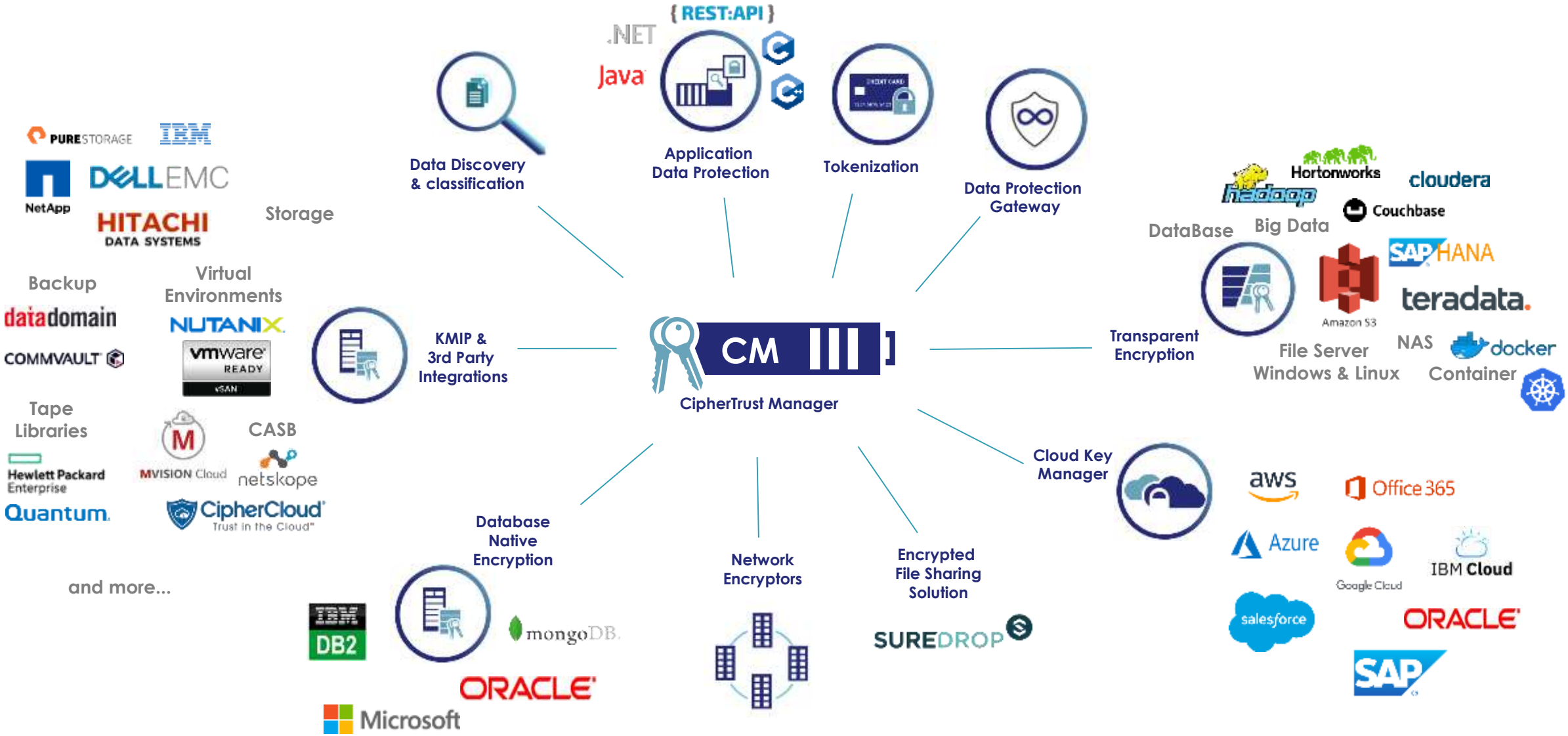
Enterprise Key Management

Cloud Key Manager

Secret Management

THALES

CipherTrust Data Security Platform



THALES

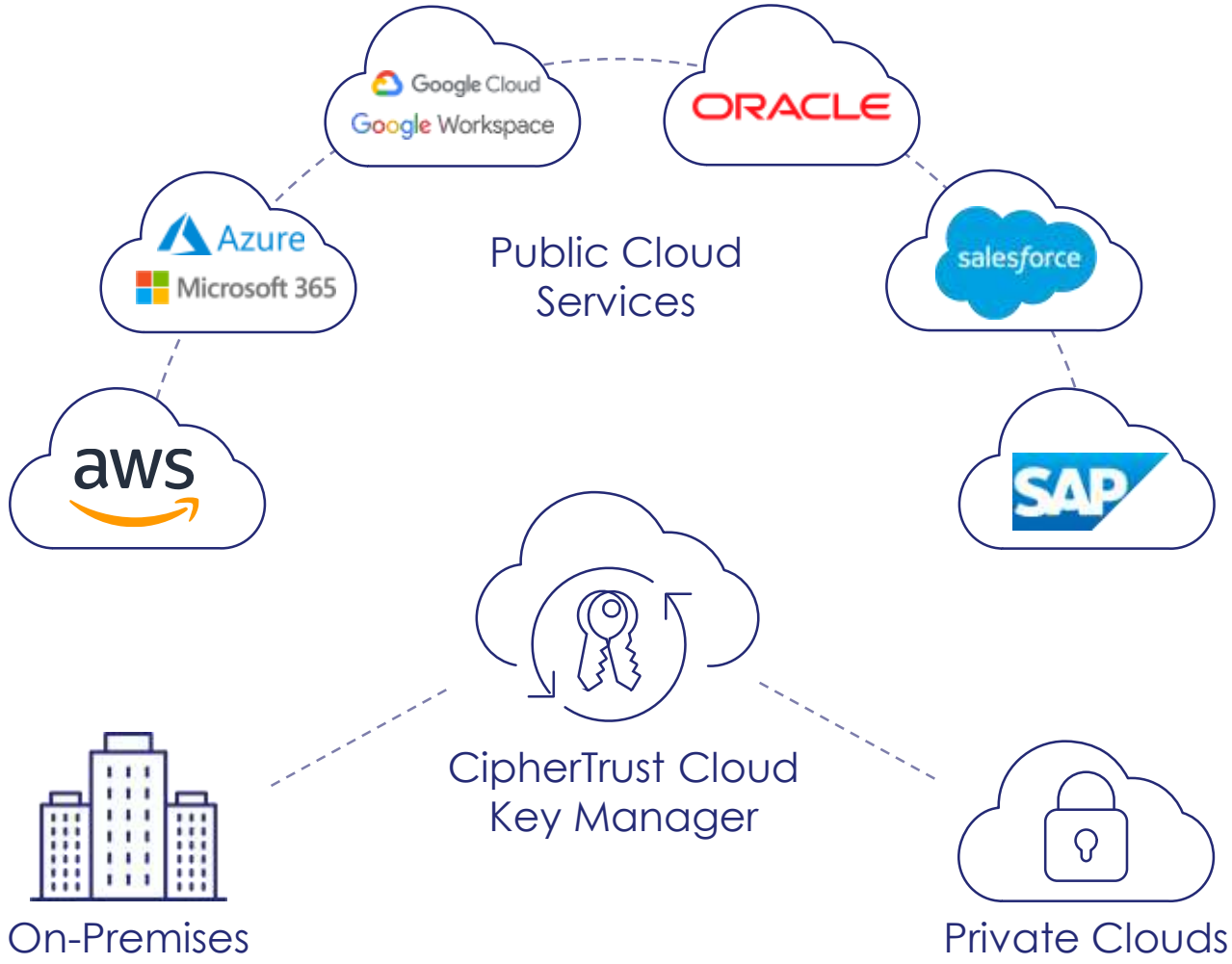
CipherTrust Cloud Key Manager – Cloud Support

IaaS and PaaS

- Amazon Web Services
  - AWS XKS
  - AWS CloudHSM
  - AWS GovCloud
  - AWS China
- Google Cloud CMEK
- Google Cloud EKM
- Google Cloud EKM-UDE
- Google Workspace CSE
  - Drive, Meet, Calendar & Gmail
- Microsoft Azure
  - Microsoft Azure GovCloud
  - Microsoft Azure Stack
  - Microsoft Azure Managed HSM
  - Microsoft China
- Microsoft 365
- Oracle Cloud Infrastructure
- SAP Data Custodian

SaaS

- Salesforce/Sandbox



THALES

Why Security and Compliance Make Digital Sovereignty Important

With encryption, it's all about the keys.

Who do you trust to store and manage them?

Data Sovereignty

You Keep all control over encryption and access to your data

- Subpoena Threat
- Data Privacy
- GDPR

Operational Sovereignty

You have visibility and control over provider operations

- CSP Engineer
- Privileged User
- Ransomware

Software Sovereignty

You can run workloads without dependence on provider's software

- Resilience
- Hybrid Multicloud
- Single Pane Glass

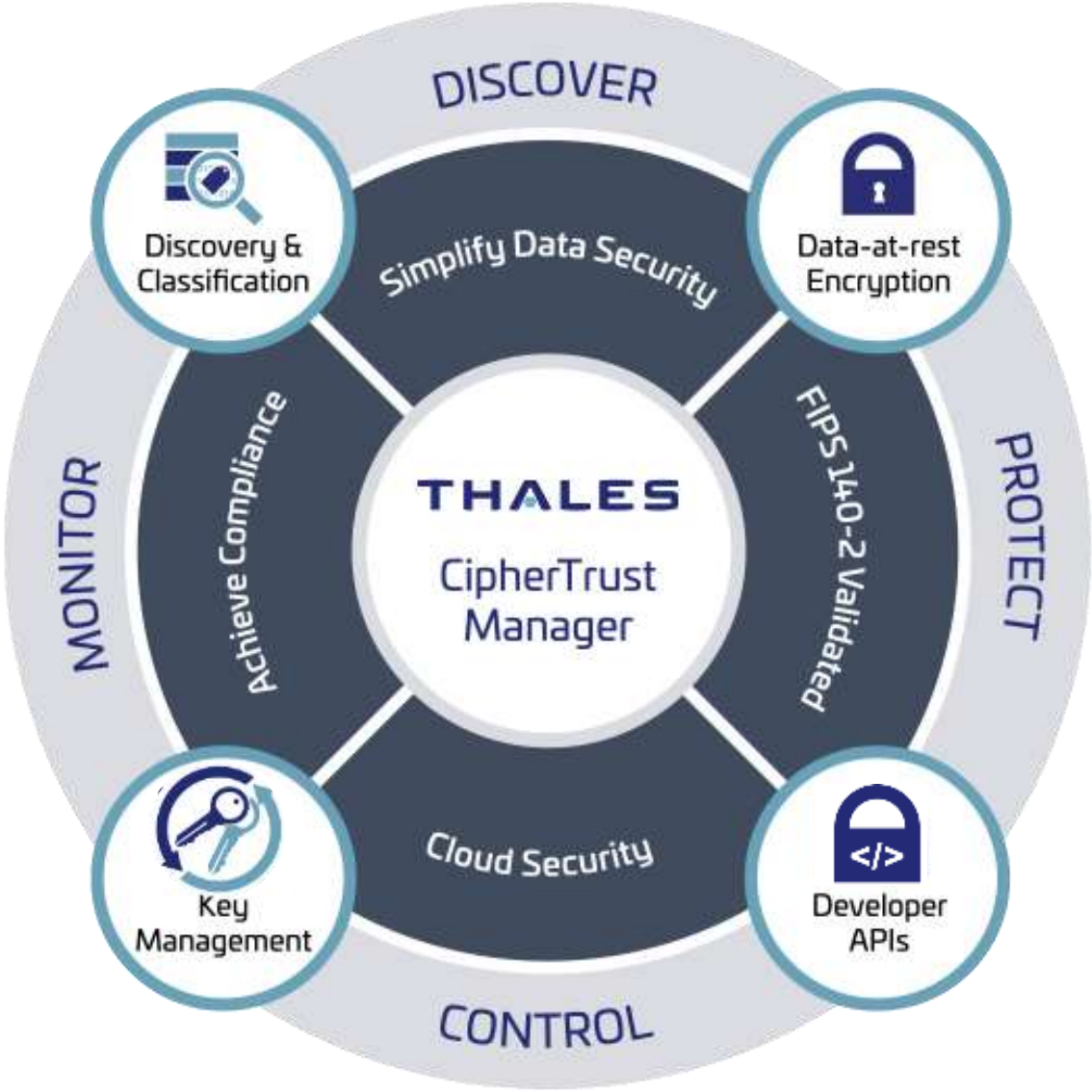
THALES

CipherTrust Data Security Platform

Simplify Data Security

Accelerate Time to Compliance

Achieve Multicloud Security



THALES

THALES

Thank you

Simone Mola
simone.mola@thalesgroup.com
mob. +39 335 1699061