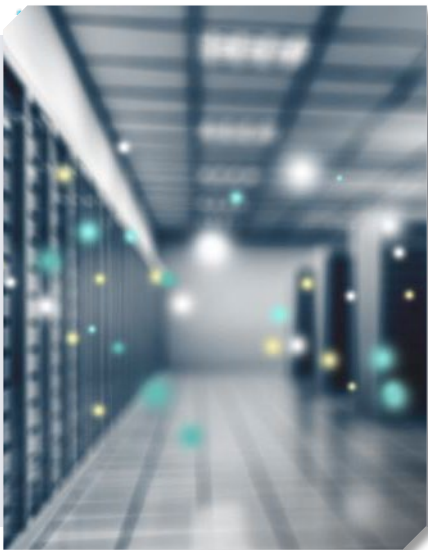


CipherTrust Data Security Platform

Cipher Summit 2025

Thales Trusted Cyber Technologies

Table of Contents



**CipherTrust,
an Overview**



**k160 Mk II
Announcement**



**Multi-Cloud Key
Management**



**Post-Quantum
Cryptography**

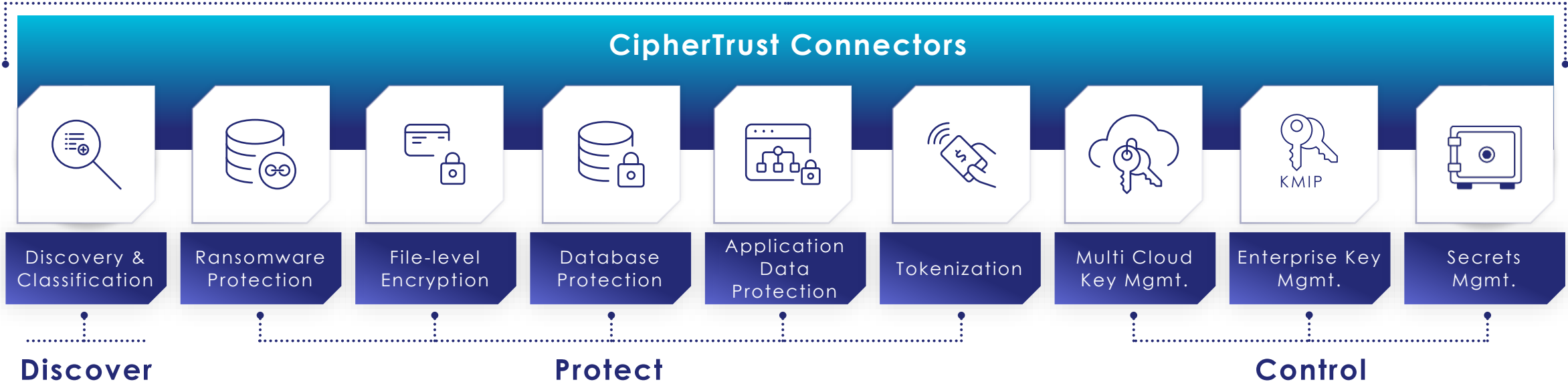


CipherTrust, an Overview

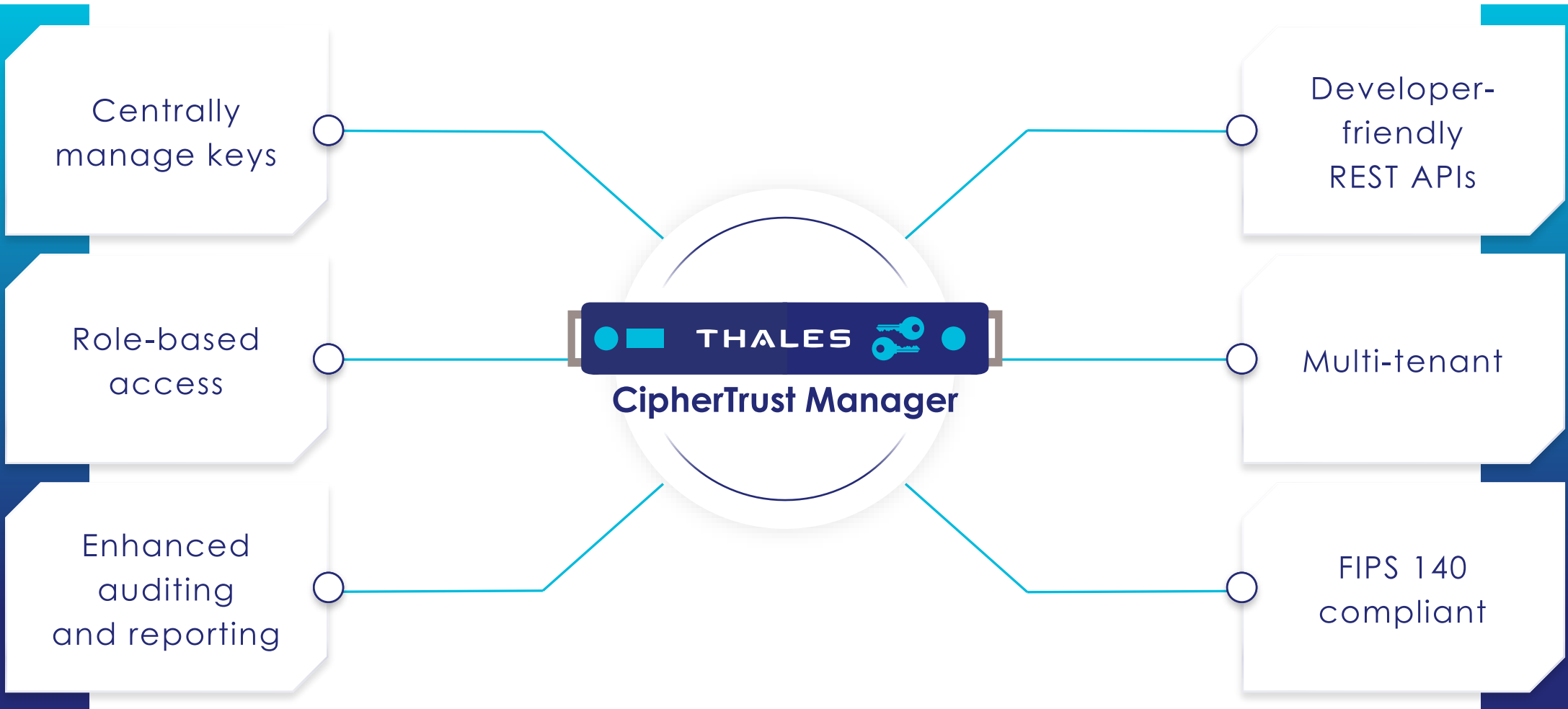
CipherTrust Data Security Platform

CipherTrust Manager

Key Management and Policies




Ciphertrust Manager Centralizes Management Across the Connectors



Ciphertrust Data Security Platform Use Cases

CipherTrust Manager




Discovery & Classification




Data Protection



DevSecOps

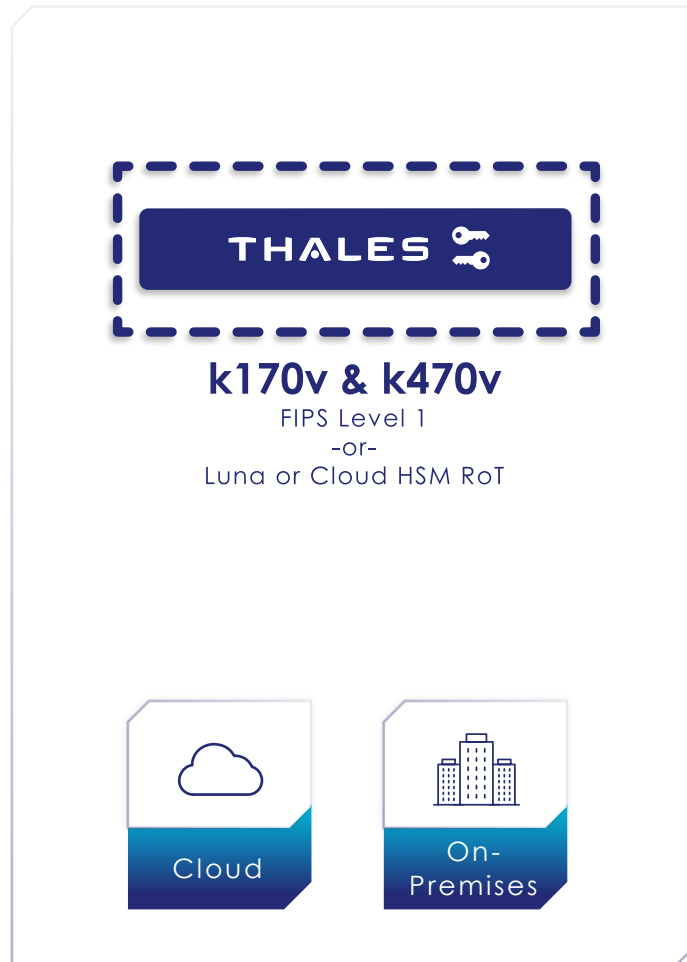


Enterprise Key Mgmt.

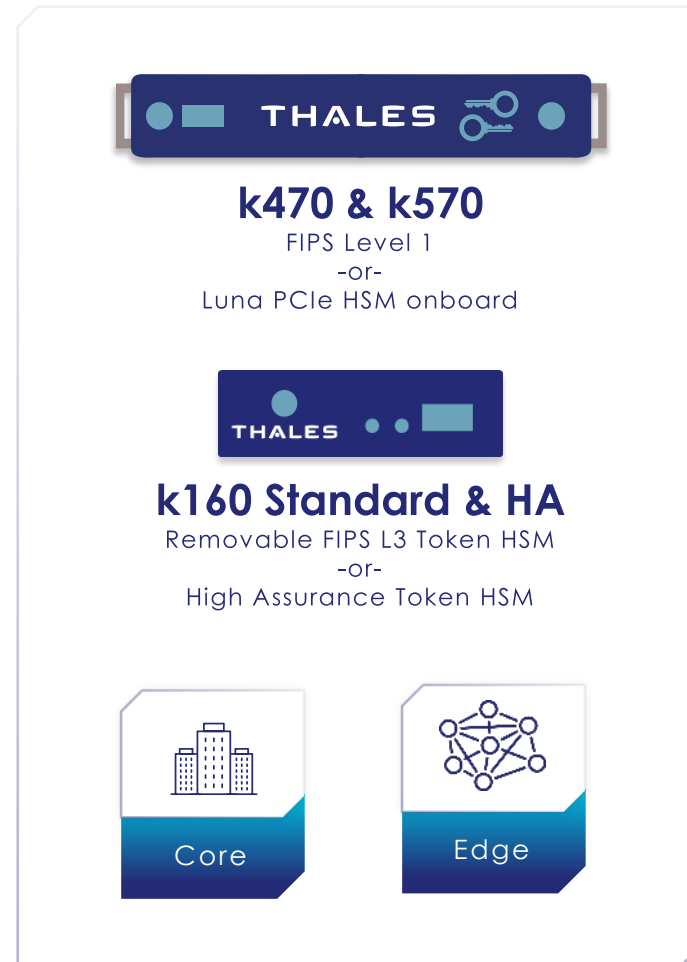


Multi Cloud Key Mgmt.

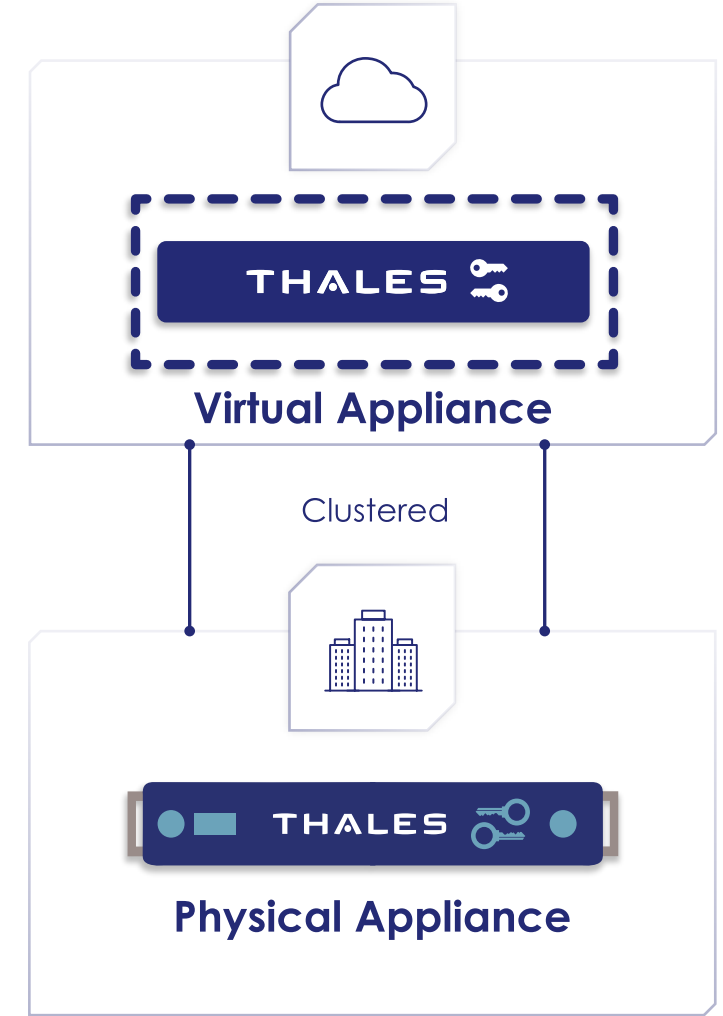
CipherTrust Manager Deployment Options



Virtual



Physical



Hybrid

Hardware Security Module Options

CipherTrust k570

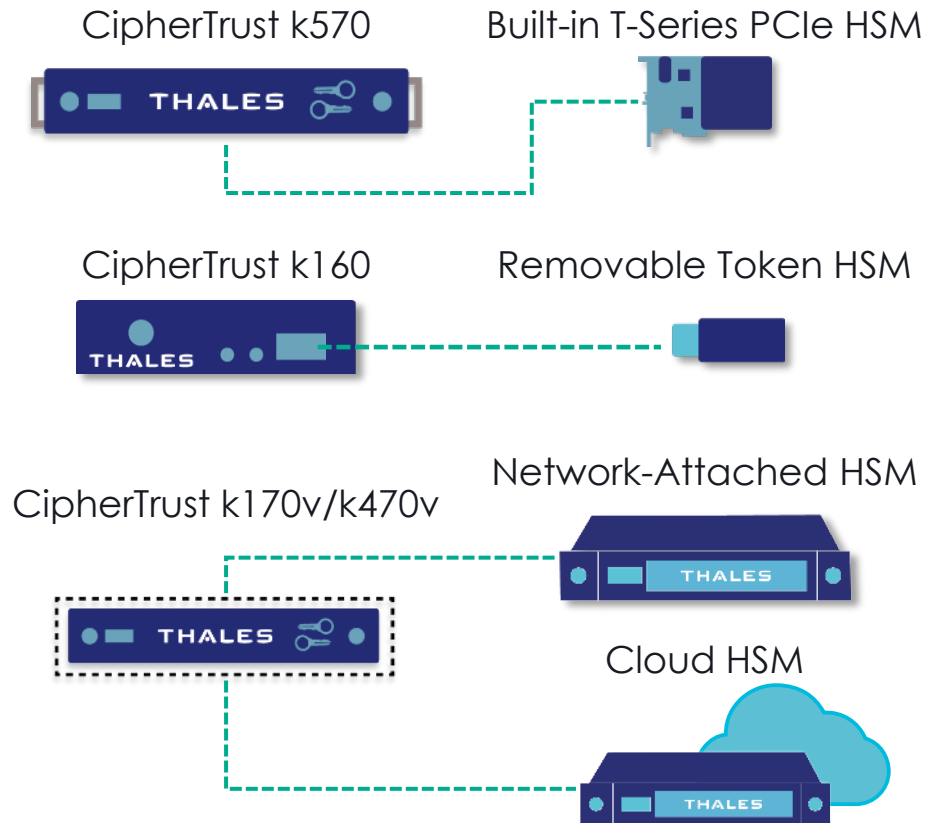
Built-in T-Series PCIe HSM
FIPS 140 Level 3 certified

CipherTrust k160

Removable FIPS-validated or
High Assurance Token HSM

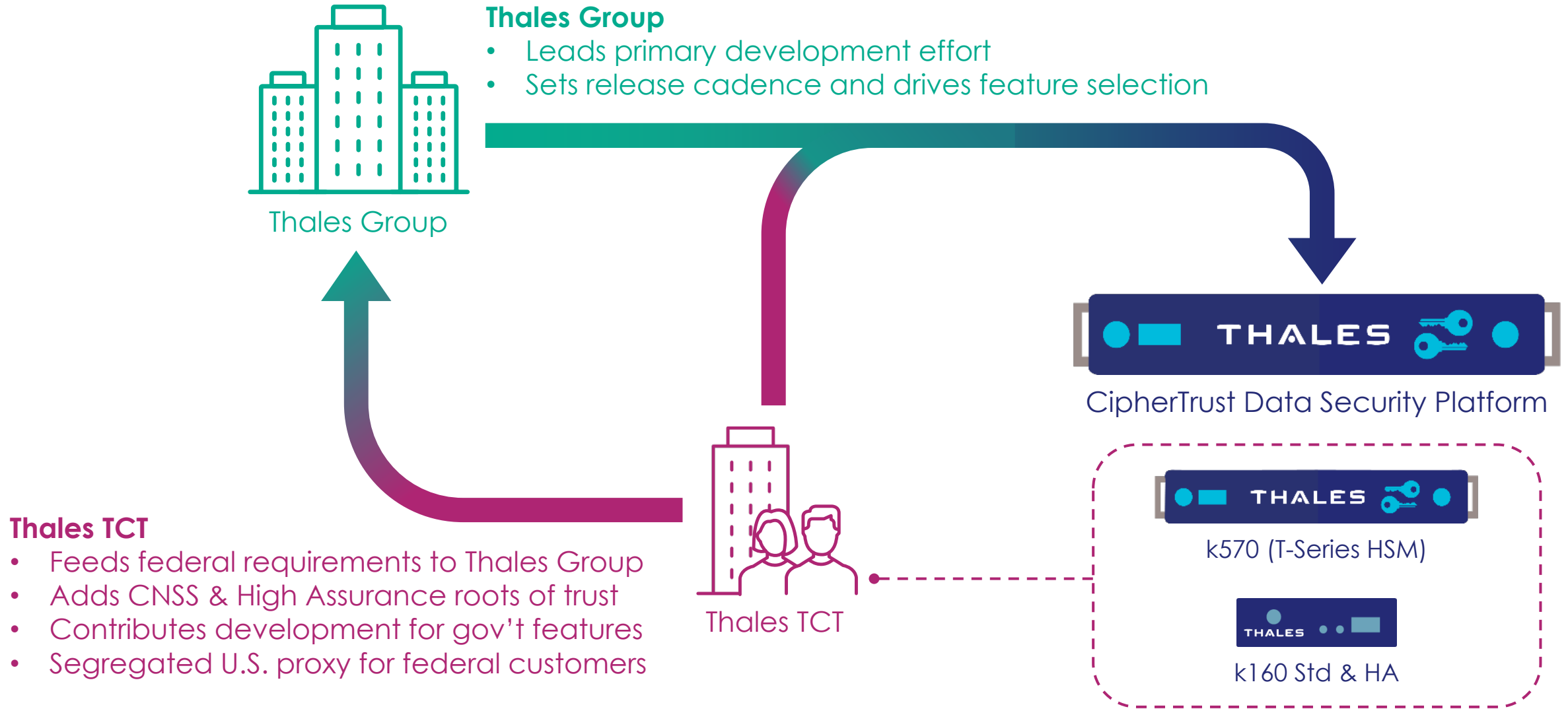
CipherTrust k170v & k470v

Luna T-Series Network HSM
Luna as a Service HSM
AWS/Azure/IBM Cloud HSM



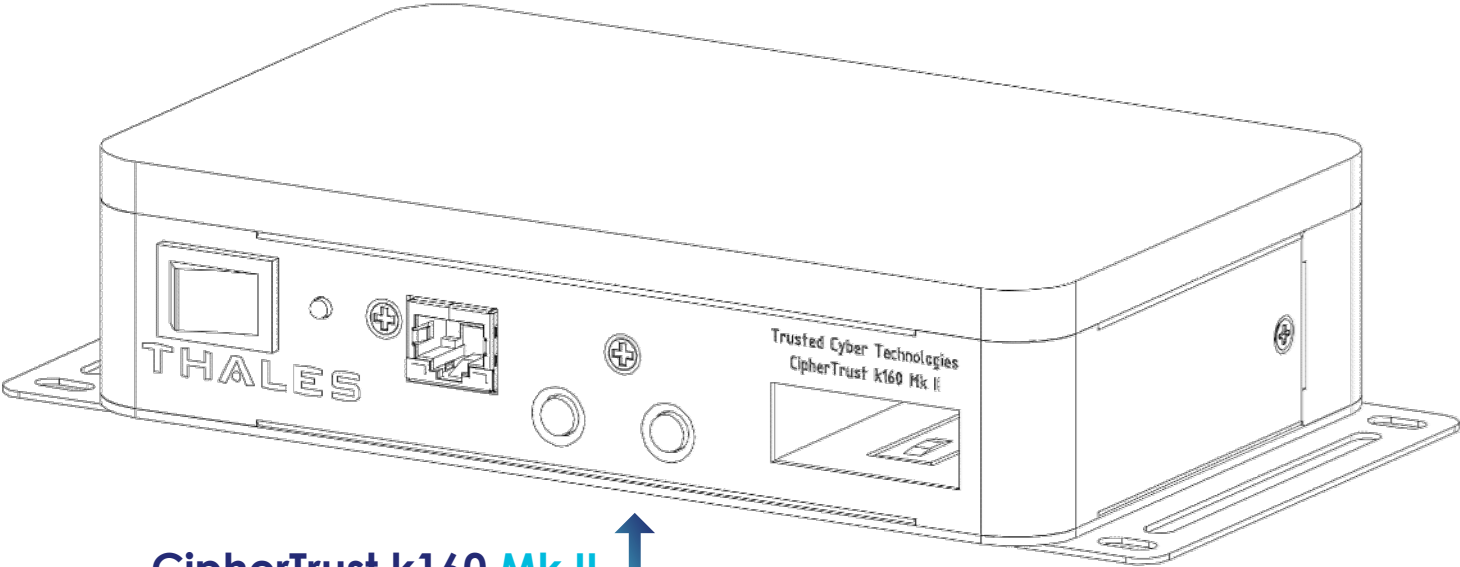
Holds master keys in a FIPS 140 Level 3 or High Assurance crypto module
HSM can be used to provide better key entropy via FIPS-validated RNG or QRNG

CipherTrust Development



CipherTrust k160 Mk II

CipherTrust k160 Evolution



CipherTrust k160 Mk II
Launching: Winter 2025

CipherTrust k160 Mk I
Launched: 06 Sep 2022

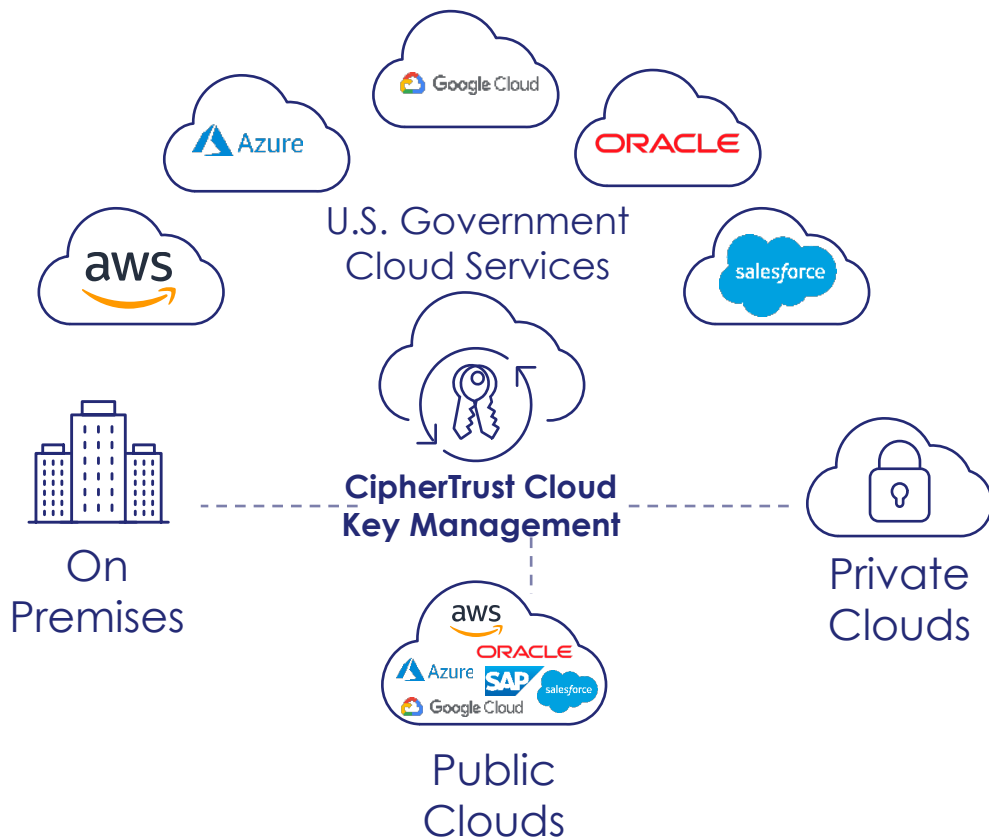


Multi-Cloud Key Management



Take Control of Your Sensitive Data Across Clouds

Mitigate data security and privacy risks with separation of duty between your data and your cloud provider



Centralize multi cloud key management for BYOK, HYOK and cloud native encryption keys across any combination of clouds and on-premises with single UI



Increase efficiency with a single pane of glass view across regions, and automated key lifecycle management with a common set of APIs



Demonstrate compliance with data sovereignty laws and privacy regulations

Control: Zero Trust Governance – Keys and Secrets

Keys (On-prem, Cloud & SaaS)

Key management for enterprise



KMIP: Key management standard for storage and database encryption

Hundreds of integrations



BYOK: You provide your own keys

Providers have limited access for necessary operations



HYOK: Only you hold the keys

Providers cannot access your encrypted data



BYOE: You control encryption and keys entirely

Providers aren't involved in encryption at all

Secrets (API Tokens, Keys & Certificates)

Secrets management for DevSecOps



Short-lived SSH Certificates: Use temporary SSH keys/certificates to simplify secrets management



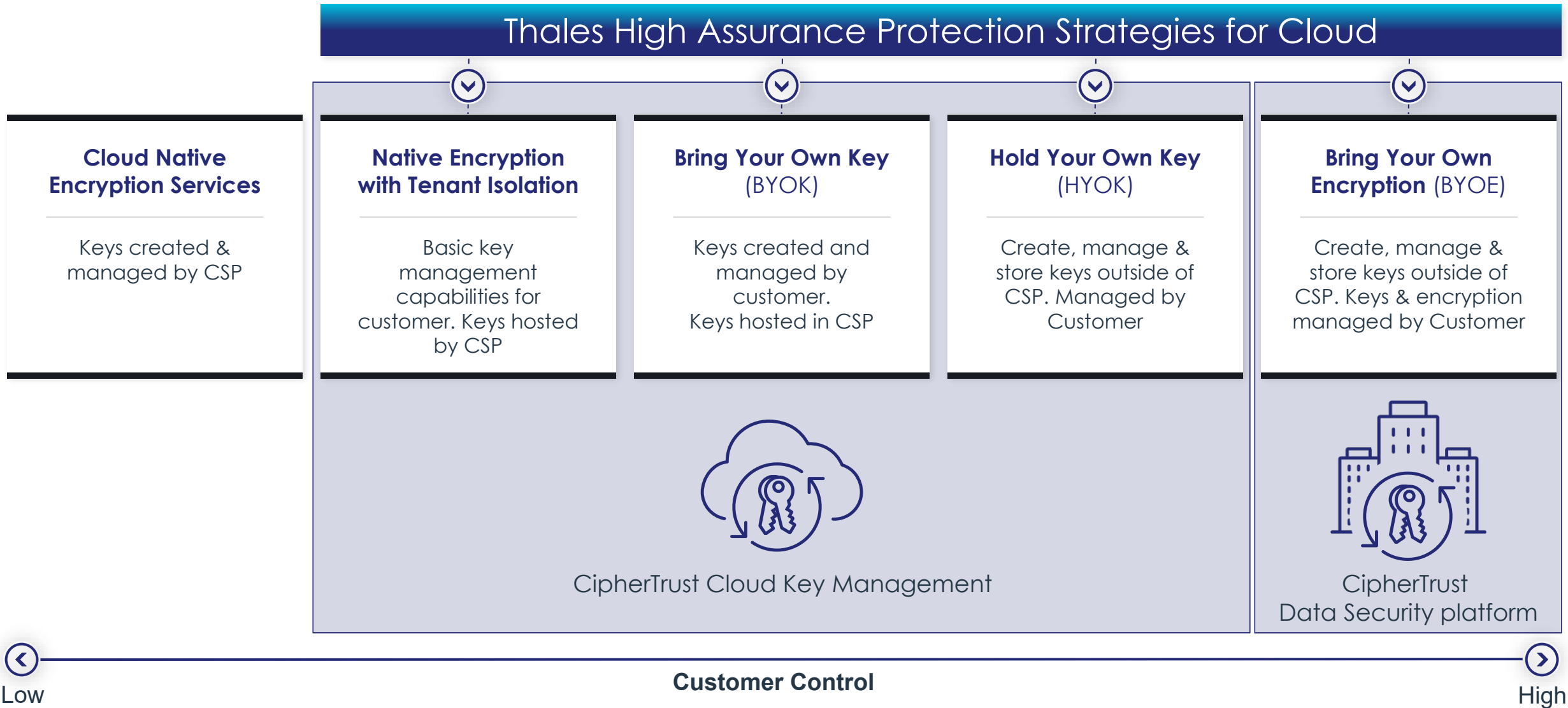
Just-in-Time Credentials: Grant temporary access to eliminate standing privileges



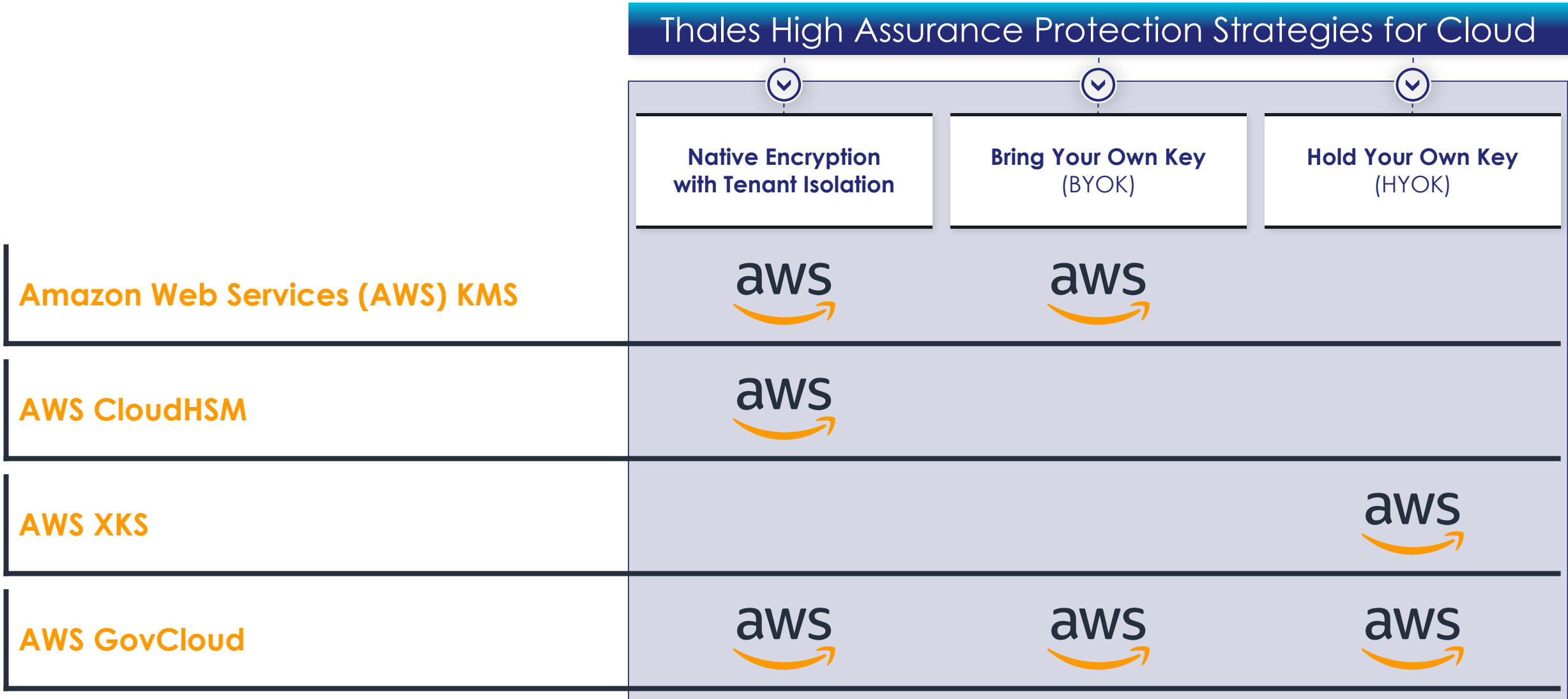
Distributed Fragment Cryptography: Grant temporary access using cryptographic fragments

AWS, Azure, GCP, OCI, OpenStack, VMware, Nutanix, HyperV

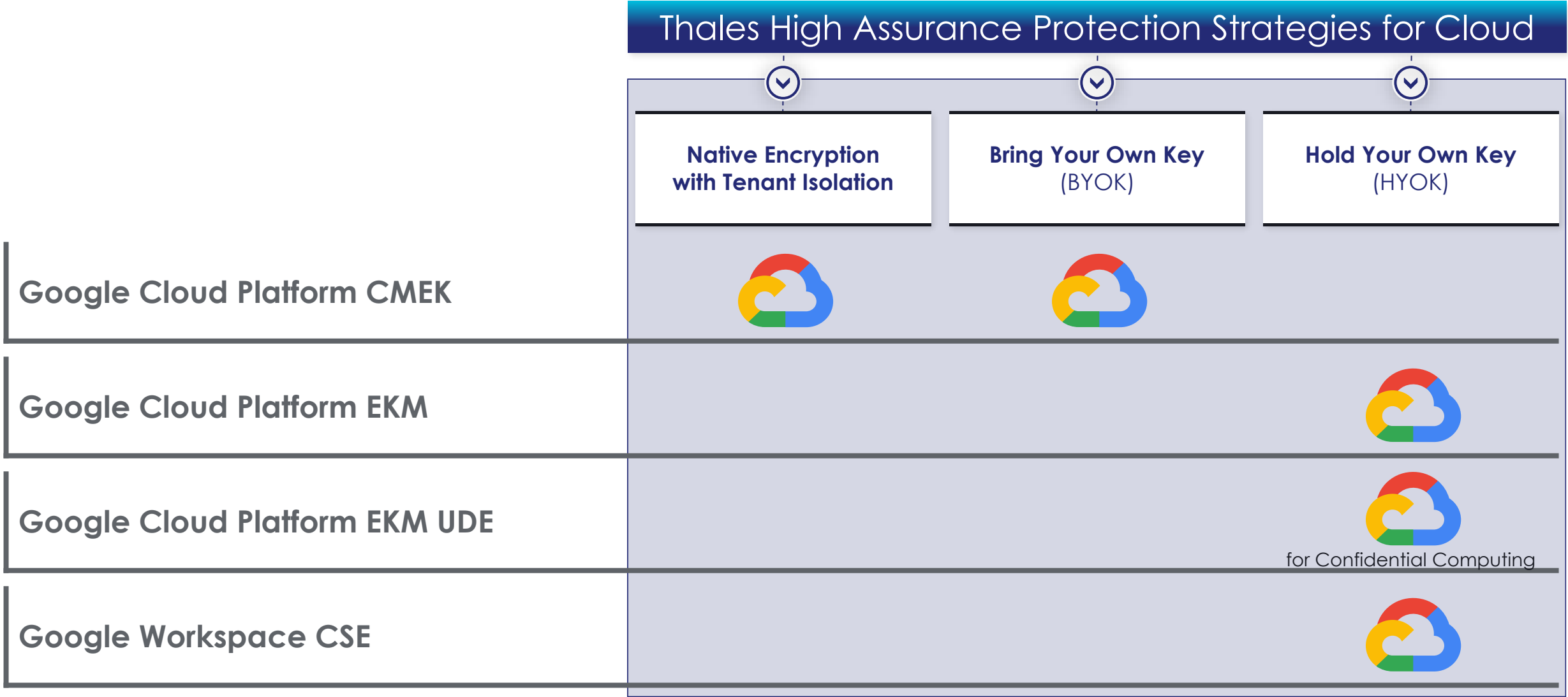
Cloud Encryption Shared Responsibility Spectrum











AWS Key Ownership Models



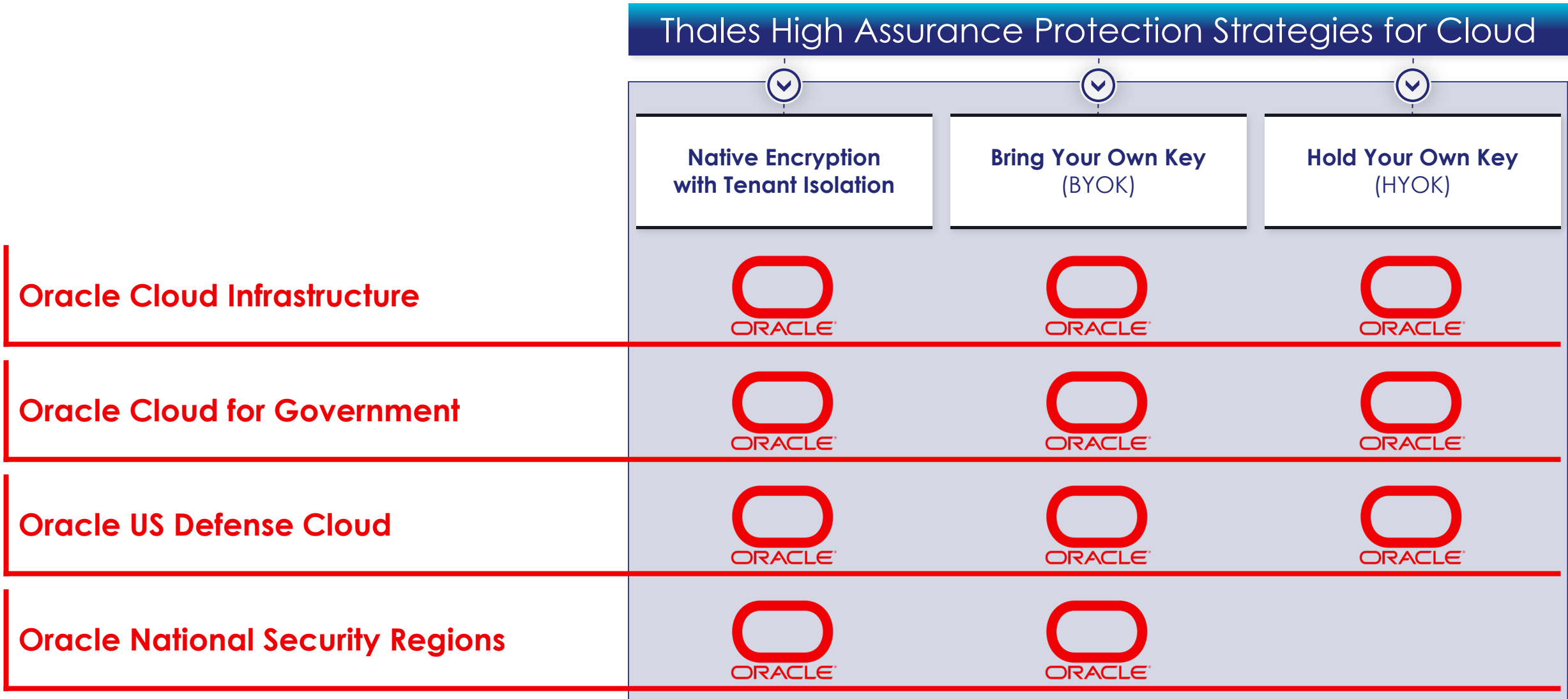
Google Key Ownership Models



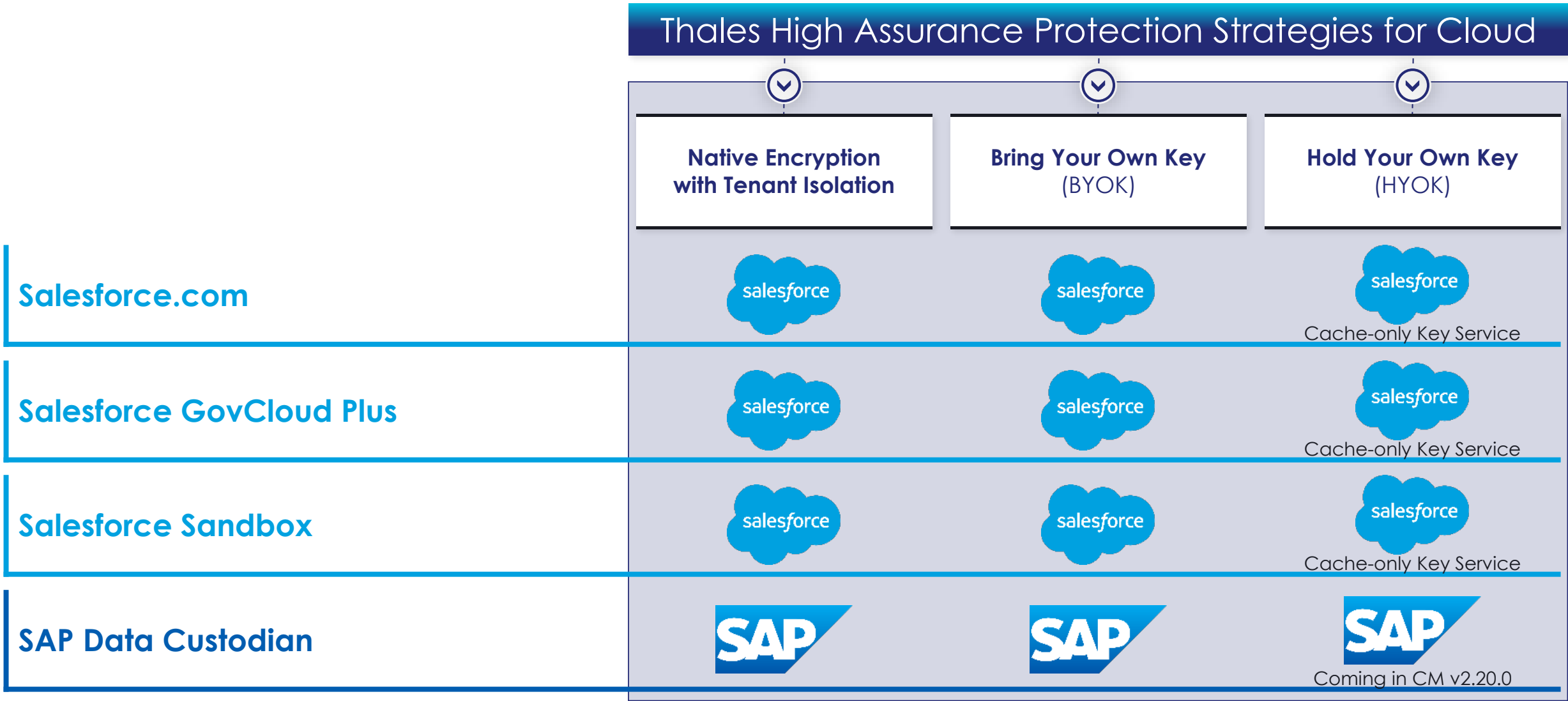
Microsoft Key Ownership Models

Thales High Assurance Protection Strategies for Cloud			
	Native Encryption with Tenant Isolation	Bring Your Own Key (BYOK)	Hold Your Own Key (HYOK)
Microsoft Azure Cloud			
Microsoft Azure GovCloud			
Microsoft Azure Managed HSMs			
Microsoft Office 365			 Double Key Encryption (DKE)

Oracle Key Ownership Models



Salesforce & SAP Key Ownership Models



Post-Quantum Cryptography

NCCoE “Migration to Post-Quantum Cryptography” Project


> NIST’s engagement with the community to address issues related to PQC migration

- Now the largest NCCoE project with >40 collaborators from government, industry and financial sectors

> Thales was a founding participant in June 2022

- Thales HSMs one of six HSM vendors performing PQC interoperability testing (2023)
 - Accelerated Thales TCT T-Series HSM release of pre-standards PQC in July 2023
 - Results published in NIST SP 1800-38 (Draft)

> Adding Thales PQC smartcards to interoperability tests in 2025



MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes. Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning. Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available.
- Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.


BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the project. To learn more, visit the project page: <https://www.nccoe.nist.gov/crypto-ability-considerations-migrating-post-quantum-cryptographic-algorithms>



HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied-crypto-pqc@nist.gov

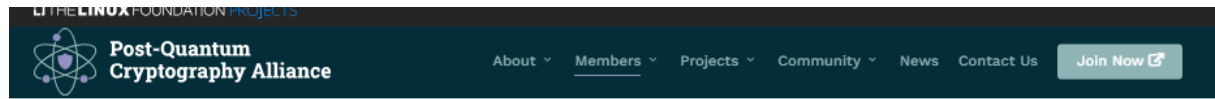
Thales TCT & NSA Sign PQC Cooperative Research and Development Agreement (CRADA)

CRADA for evaluating the NIST selected PQC algorithms when operating on an HSM

CRADA results will be used:

- By Thales TCT to accelerate PQC algorithm deployment
- Assist the Government and other HSM users in understanding the value of using PQC enabled HSMs to mitigate the quantum threat

Premier Member of Post-Quantum Cryptography Alliance



Members

Premier



General



Associate



Post-Quantum Cryptography Alliance

To advance the adoption of post-quantum cryptography, by producing high-assurance software implementations of standardized algorithms, and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.



CipherTrust Manager PQC Phases 2025-2026

Harvest Now, Decrypt Later: Adversaries are Already Collecting Encrypted Data

PHASE 1

- Protect Public Interfaces exchanging confidential information is critical.
 - Examples:
 - Web/REST/UI/KMIP
 - CDSP Connectors
 - Quantum entropy (QRNG) w/Luna HSM
- Protect Management Interfaces exchanging confidential information is critical.
 - Management Interfaces:
 - SSH & SMTP
 - Protect Clustering Protocols as it has sensitive data replication:
 - Public Networks
 - Private Networks

PHASE 2

- Replacing internal asymmetric encryption components on internal and external networks:
 - Data in Motion
 - Encryption of sensitive data between CM and Agents
 - Backup Files
- Replacing internal asymmetric encryption components on private networks:
 - Sensitive internal components

CipherTrust Manager v2.20 Introduces TLS PQC Support – Tech Preview

- **TLS Key Exchange Groups** include a list of the key exchange algorithms that the system offers for the WEB interface during the TLS handshake.
- By default, the following **classic key exchange algorithms** are enabled:
 - 'x25519', 'secp256r1', 'x448', 'secp521r1', 'secp384r1', 'ffdhe2048', 'ffdhe3072', 'ffdhe4096', 'ffdhe6144', and 'ffdhe8192'
- By default, the following **post-quantum key exchange algorithms** are disabled:
 - 'X25519MLKEM768', 'SecP256r1MLKEM768', 'MLKEM1024', and 'MLKEM768'
- **NOTE: CM will prevent users from disabling common EC curves. At least one EC curve will remain enabled. As PQC implementations mature, and support becomes widely available from browsers and HTTPS clients, this limitation will be removed.**
- One of the following curves must stay enabled:
 - 'X25519', 'secp256r1', 'X448', 'secp521r1', 'secp384r1'



Thank you!

Evan Pelecky

Senior Product Manager
Cryptographic Key Management

 **443-484-7076**

 **evan.pelecky@thalestct.com**