Thales + Imperva per una risposta integrata alle nuove minacce e requisiti di compliance nella protezione del nostro patrimonio di dati

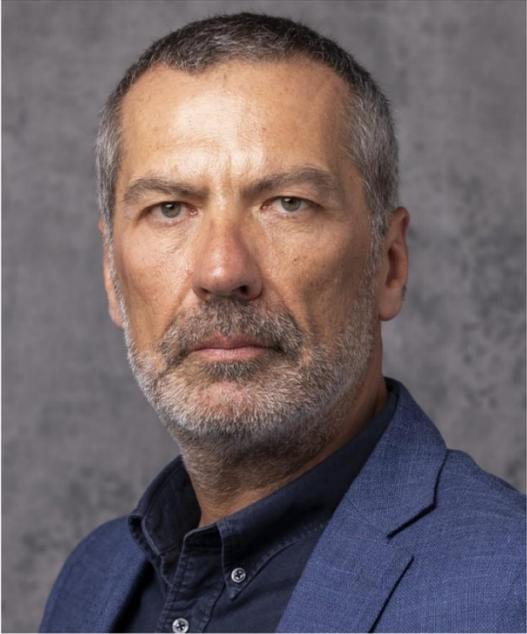**Claudio Squinzi** | Regional Sales Manager - Thales
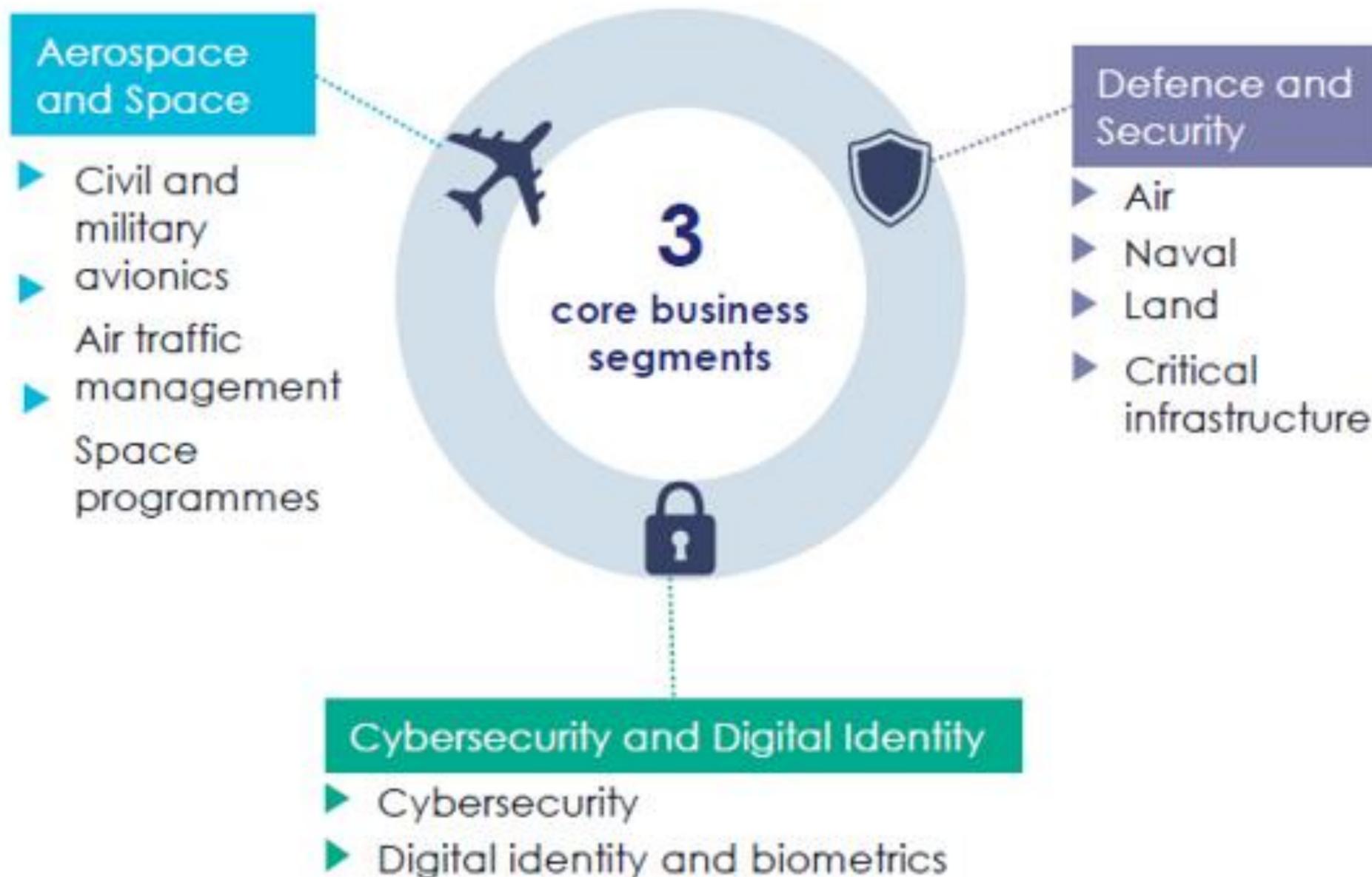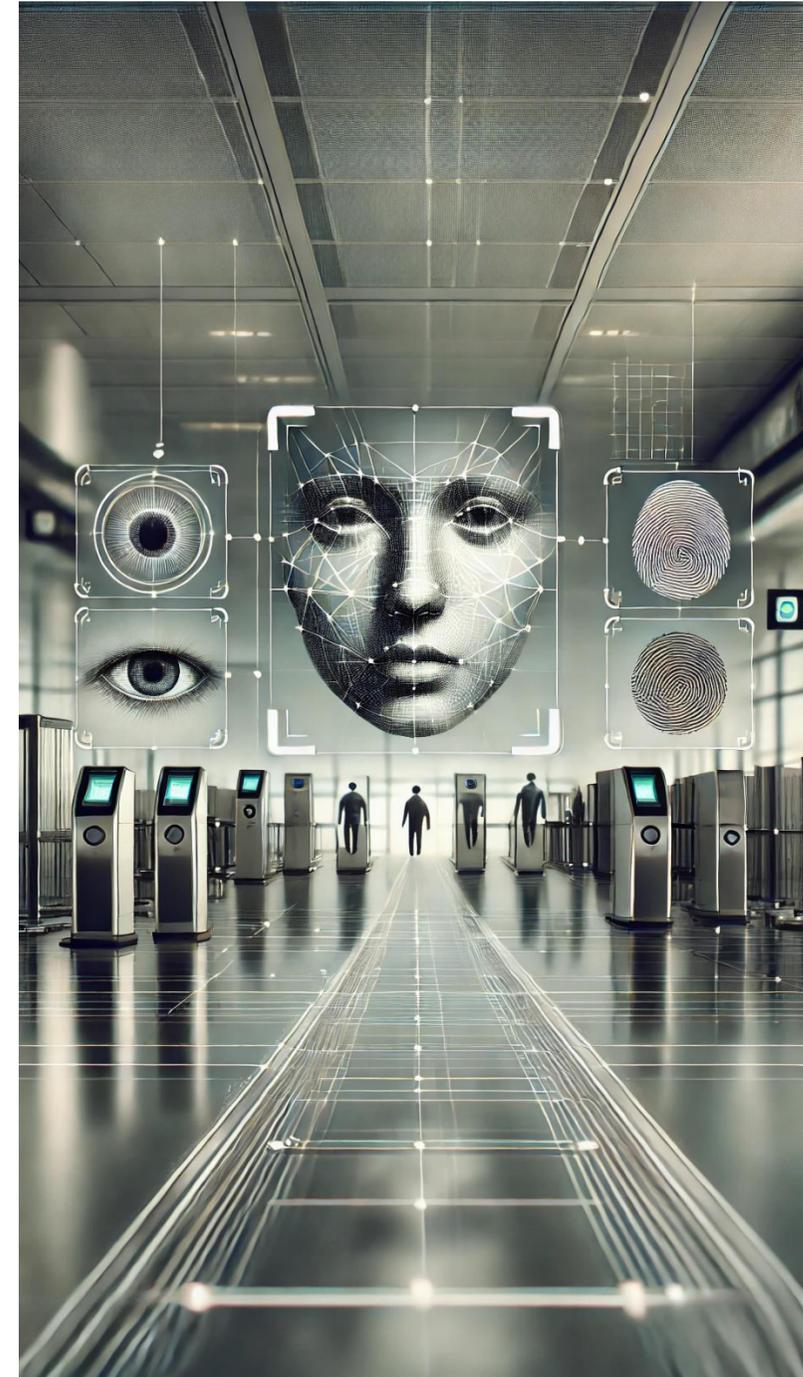
Claudio Squinzi
Regional Sales Manager - Thales

THALES

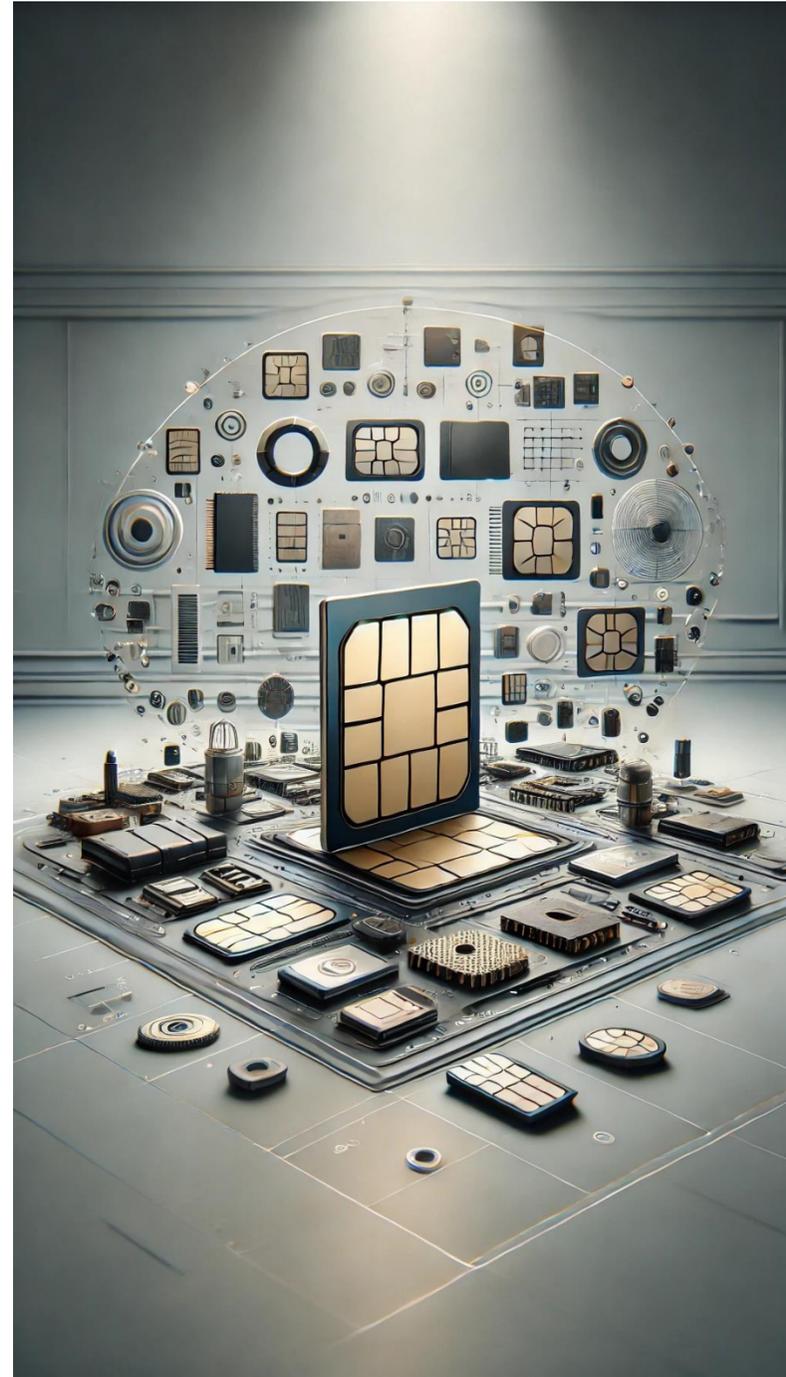# Core business segments

Aerospace and Space
- Civil and military avionics
- Air traffic management
- Space programmes

Defence and Security
- Air
- Naval
- Land
- Critical infrastructure

3 core business segments

Cybersecurity and Digital Identity
- Cybersecurity
- Digital identity and biometrics

THALES

CDI in our everyday life

Cyber Security Products (CSP): a very broad product portfolio

An effective analogy

Cloud shared responsibility

Digital (Data) sovereignty
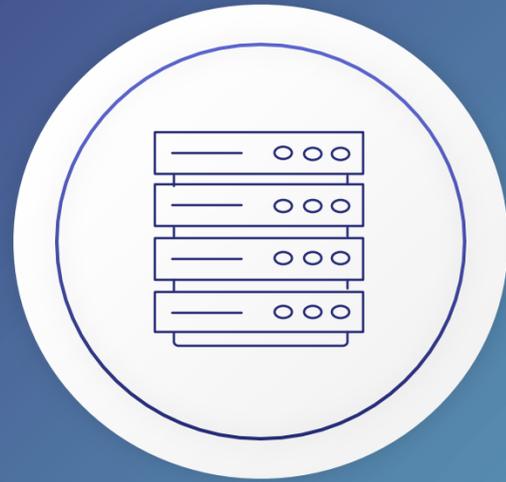
92%
of all the data in the western world is stored on US-owned servers (*)

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

Clusit 25
2000-2025

SECURITY SUMMIT

ASTREA

THALES GROUP LIMITED DISTRIBUTION - SECRET

Options for the cloud

Cloud services qualification

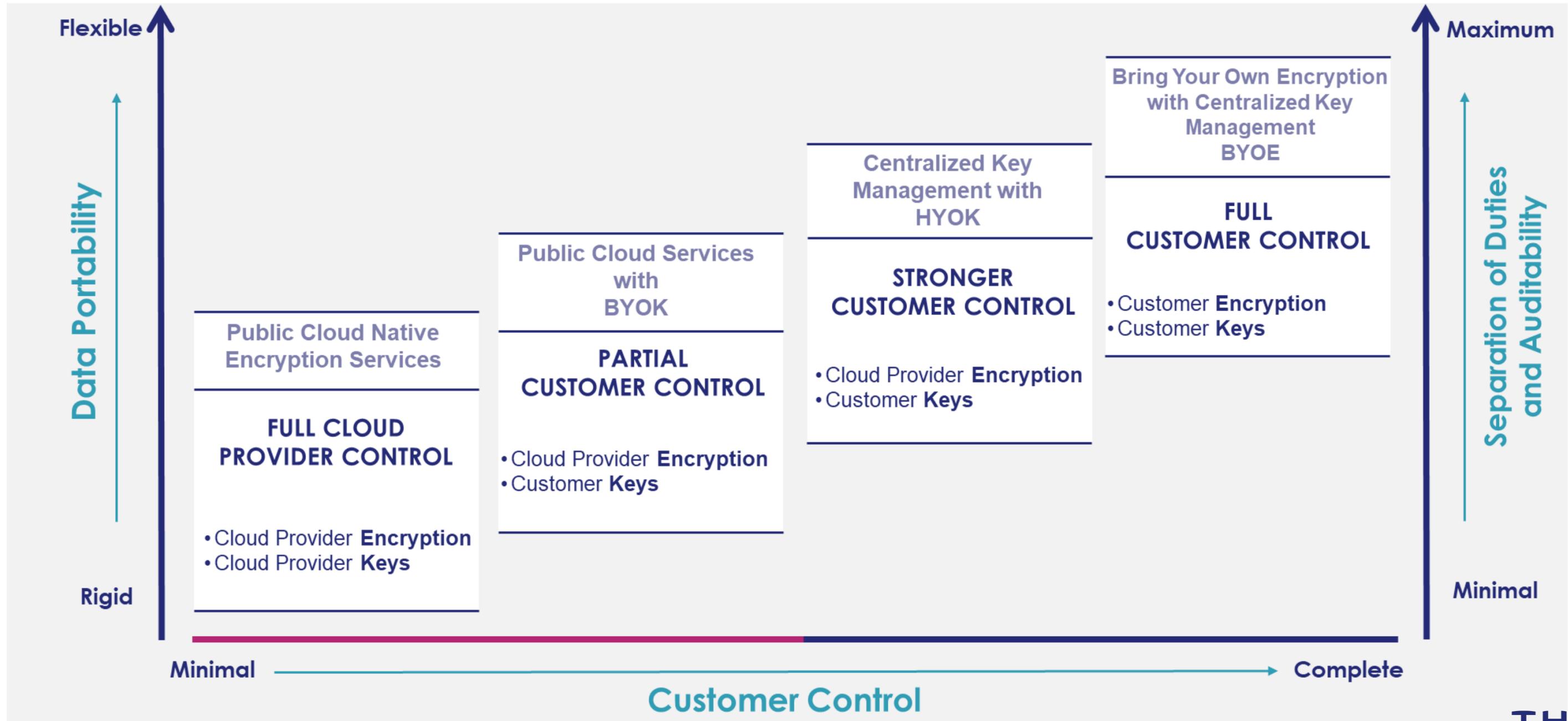| CARATTERISTICHE		CERTIFICAZIONI	REQUISITI CARATTERIZZANTI
QC1	40 Sicurezza 11 Qualità 2 Portabilità 4 Interoperabilità	ISO 27001/17/18* ISO 9001 (Qualità)	• Localizzazione in EU: infrastrutture fisiche e tecnologiche servizio cloud, dati Amministrazioni;
QC2	66 Sicurezza	ISO 27001/17/18* ISO 9001 (Qualità) ISO 20000 (Gestione Servizio) ISO 22301 (Continuità Operativa)	• Importazione delle chiavi di cifratura generate esternamente, BYOK (HSM gestito dall'Amministrazione)
QC3	72 Sicurezza		• Localizzazione in EU: metadati; • Controllo delle attività privilegiate e aggiornamenti hw/sw • Verifica aggiornamenti ambiente di test
QC4		ISO 27001/17/18 CSA STAR* Level 2 ISO 9001 (Gestione Qualità) ISO 20000 (Gestione Servizio) ISO 22301 (Continuità Operativa)	• Gestione delle chiavi autonoma esterna, HYOK (HSM gestito dall'Amministrazione) • Flussi da/verso esterno sono soggetti a procedure di approvazione, monitoraggio e controllo dell'Amministrazione • Metodologie di verifica e controllo del personale sono condivise con l'Amministrazione

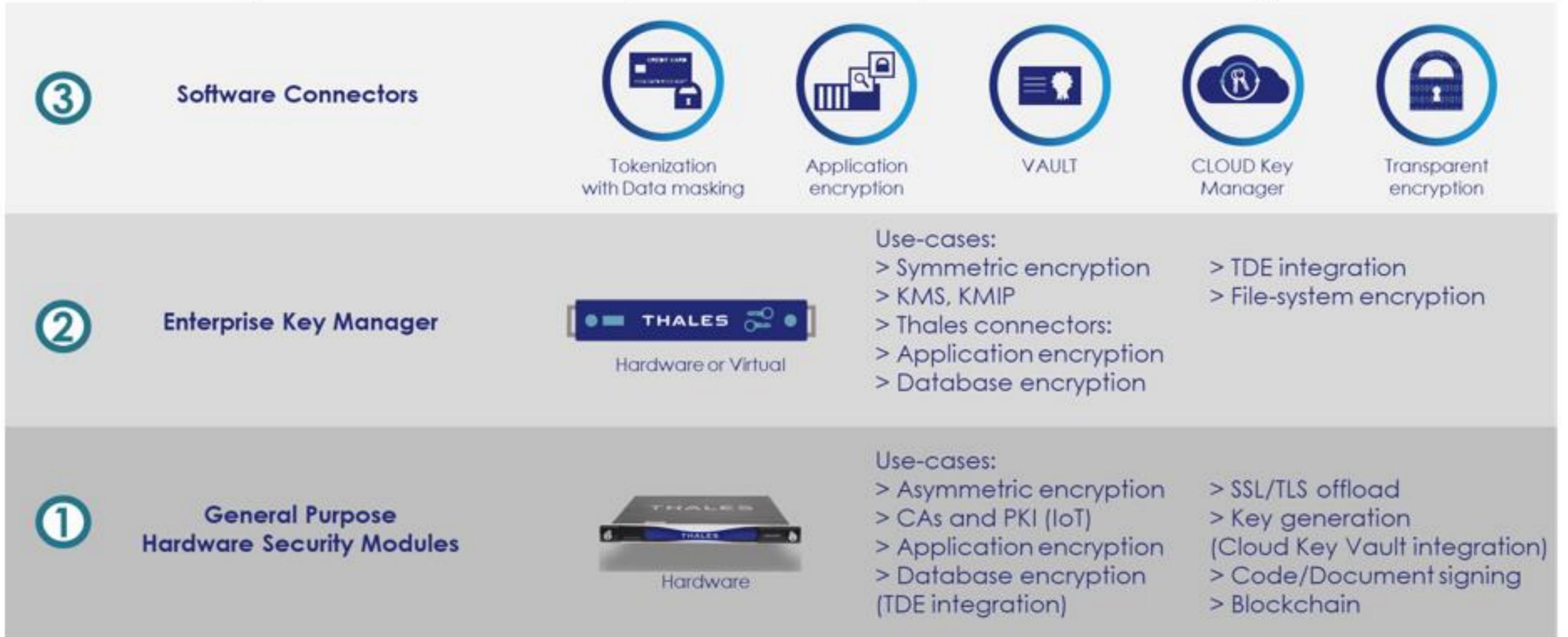ORDINARIO / CRITICO / STRATEGICO
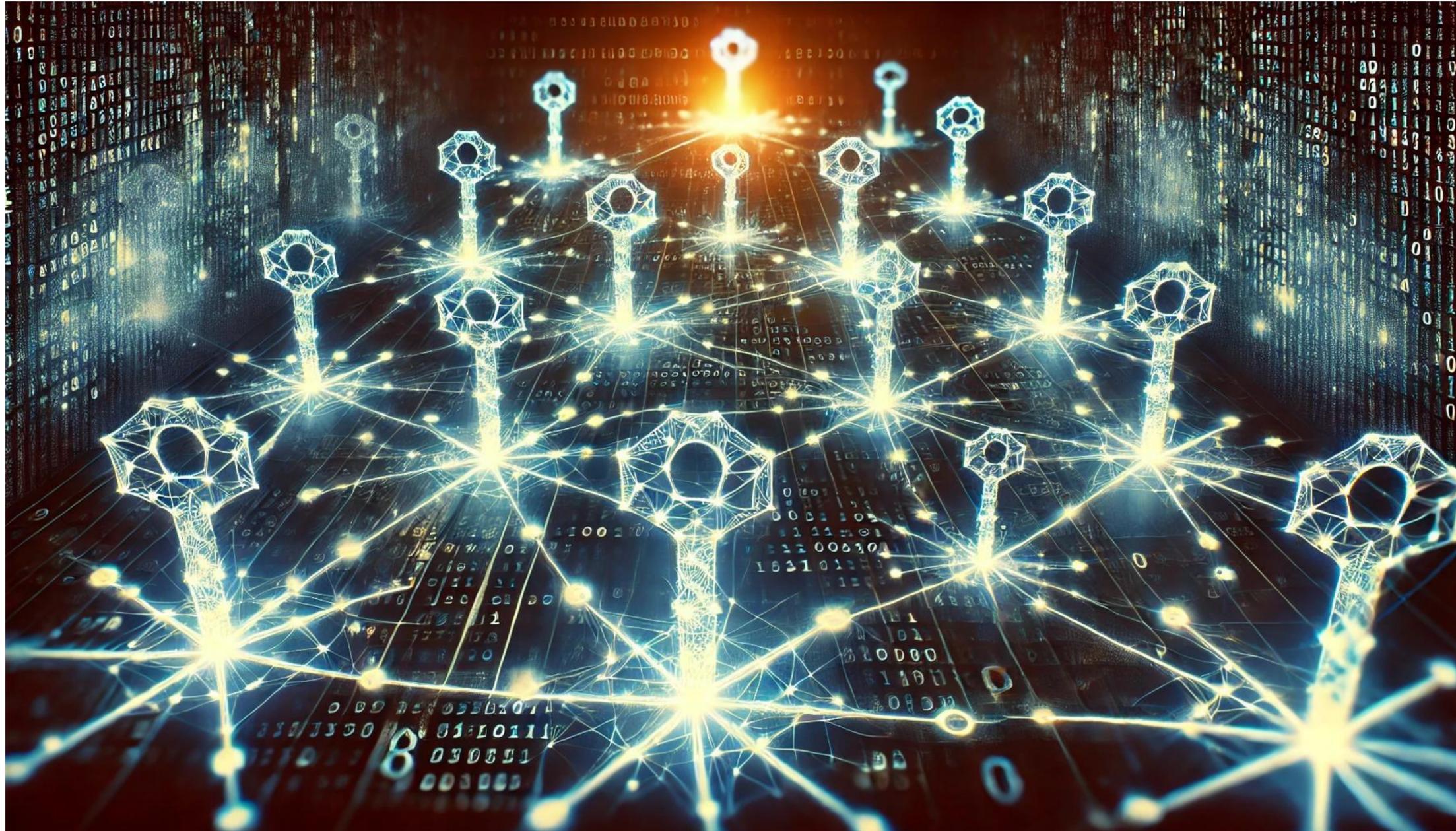
Key Management

DORA

Digital Operational Resilience Act (DORA)

Thales helps organizations comply with DORA by addressing requirements on chapter II for risk management and chapter V on managing third party risk.

Requirements	DORA Articles	Thales Supporting Capabilities
Chapter II: ICT Risk Management		
Identify and classify	8.1	Data Discovery and Classification
Protect data at rest, in use or in transit	9.2	Transparent Encryption, Tokenization, High Speed Encryptors (HSE)
Access management	9.3,b 9.4,c	Identity and Access Management, Consent and Preference Management, Transparent Encryption
Implement multi-factor authentication	9.4	SafeNet Trusted Access
Securely manage cryptographic keys	9.4	Enterprise Key Management, Hardware Security Modules (HSMs)
Monitor and detect anomalous activities	10.1	SafeNet Trusted Access, Transparent Encryption
Chapter V: Managing of ICT Third Party Risk		
Mitigate risks of third-party service providers	28.8	Cloud Key Management, Transparent Encryption

THALES

A three-layered architecture

③ **Software Connectors**	Tokenization with Data masking	Application encryption	VAULT	CLOUD Key Manager	Transparent encryption

② **Enterprise Key Manager**	THALES — 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

Q&A

Contatti:

Claudio Squinzi
Mail: Claudio.squinzi@thalesgroup.com
Mob.: +39 348 851 3843

Vieni a trovarci al nostro stand!