THALES

Data Security Use Case by THALES

ชัชวาล จิตติกุลดิลก

Regional Sales Director

chajchaval.chittikuladilok@thalesgroup.com
+6681-833-2377

GOVERNMENTS

INSTITUTIONS

CITIES

COMPANIES

OPEN

THALES
Building a future we can all trust

From the Bottom of the Oceans… to the Depths of Space & Cyberspace

Digital Identity and Security

Ground Transportation

Defence and Security

Space

Aerospace

OPEN

THALES
Building a future we can all trust

Thales + Imperva secure your most sensitive data **…and all paths to it**

External threats

Application Security

Applications

Control

Data creation   Data in motion   Data at rest   Data in use

Visibility

Internal threats   Identities

Identity & Access Management

THALES
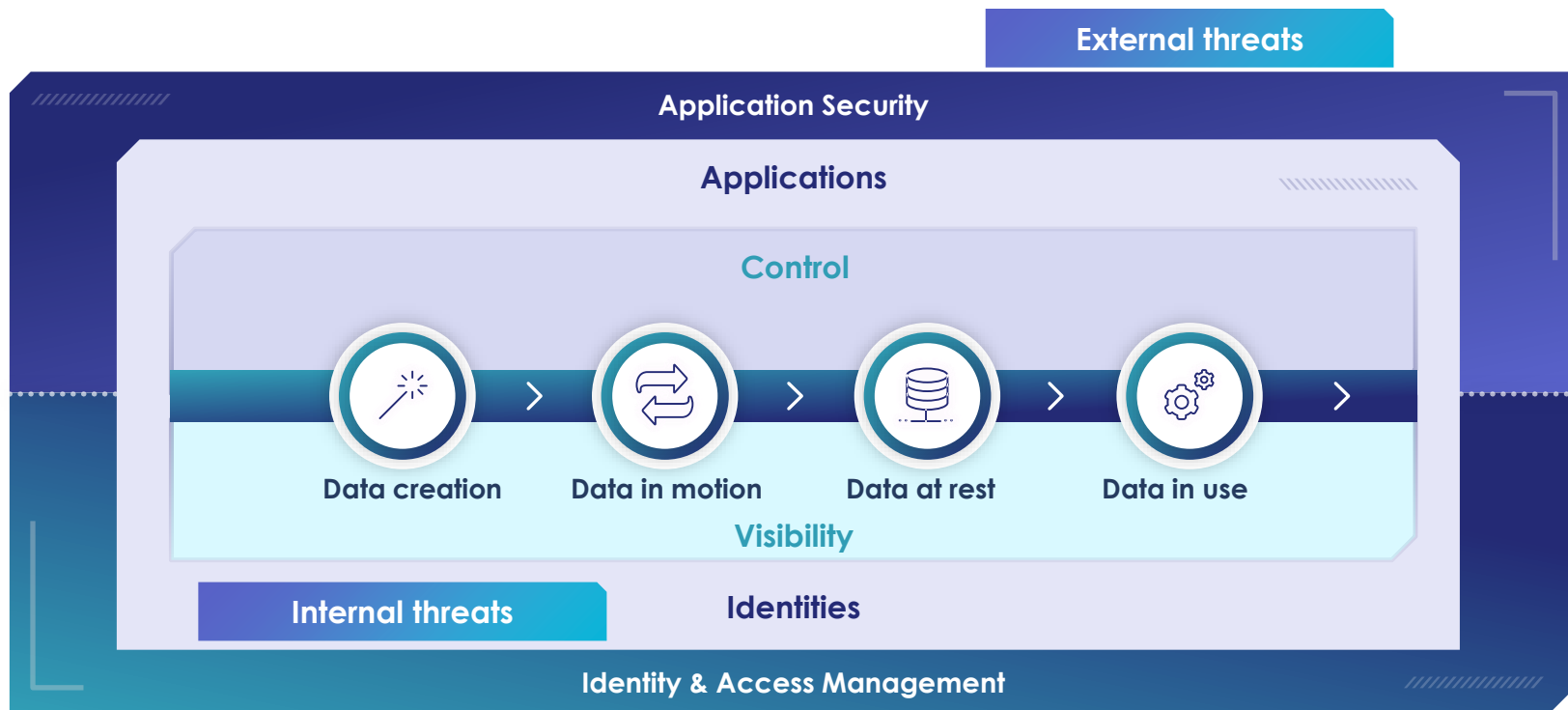
providing a broad range capabilities to **protect what matters most**

Applications

- Web App. Firewall
- DDoS Protection
- Advanced Bot Protection
- API Security

Data

- Encryption
- Tokenization
- Key & Secrets Management
- Hardware Security Modules
- Data Access Monitoring
- Data Discovery & Classification
- Data Governance
- Threat Detection

Identities

- Customer Identity & Access Management
- Workforce Identity & Access Management
- Broad Range of Authenticators

THALES

Government Data Among Top Targets

~18000
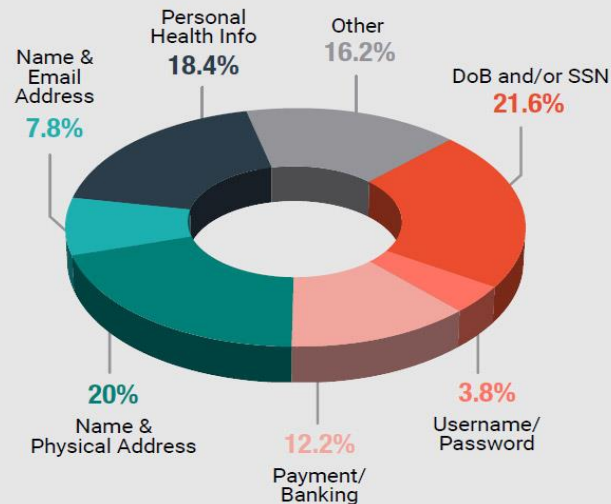**cyber incidents** affected government **agencies across the world** in 2022[7]

178
Total data breaches in Singapore public sector alone in 2021-22[8].

Breach Types
Types of Data Exposed in Every Breach

- Name & Email Address **7.8%**
- Personal Health Info **18.4%**
- Other **16.2%**
- DoB and/or SSN **21.6%**
- Username/ Password **3.8%**
- Payment/ Banking **12.2%**
- Name & Physical Address **20%**

Personally identifiable information (PII) is by far the most common type of breach, representing 97% of all breaches[4]

THALES

APAC regulatory landscape

- Governments strengthening their privacy law frameworks

- Mandatory data breach notification laws

- Greater recognition for the individual's rights to privacy and data sovereignty

- Fines/penalties for contravention

China
The PRC Cybersecurity law & other laws/regulations

South Korea
Personal Information Protection Act

Japan
The Act on the Protection of Personal Information (APPI)

HongKong
Personal data (Privacy) Ordinance

Thailand
PDPA/Official information Act

Singapore
Public Sector Governance Act

Taiwan
Freedom of Government Information Law

Philippines
National Privacy Commission Data Privacy Act

Australia
Information Privacy Act Mix of federal & state/territory legislation

New Zealand
OPC Privacy Act 1993

THALES

Data Security Priorities across governments worldwide

#. **Digital Sovereignty**

Ransomware Attacks

PQC

IoT attacks

Supply Chain Attacks

Advanced Persistent Threats (APTs)

Regulatory Compliances

*The Top 10 Data Security Threats to the Public Sector by SANS

THALES

#. Digital Sovereignty
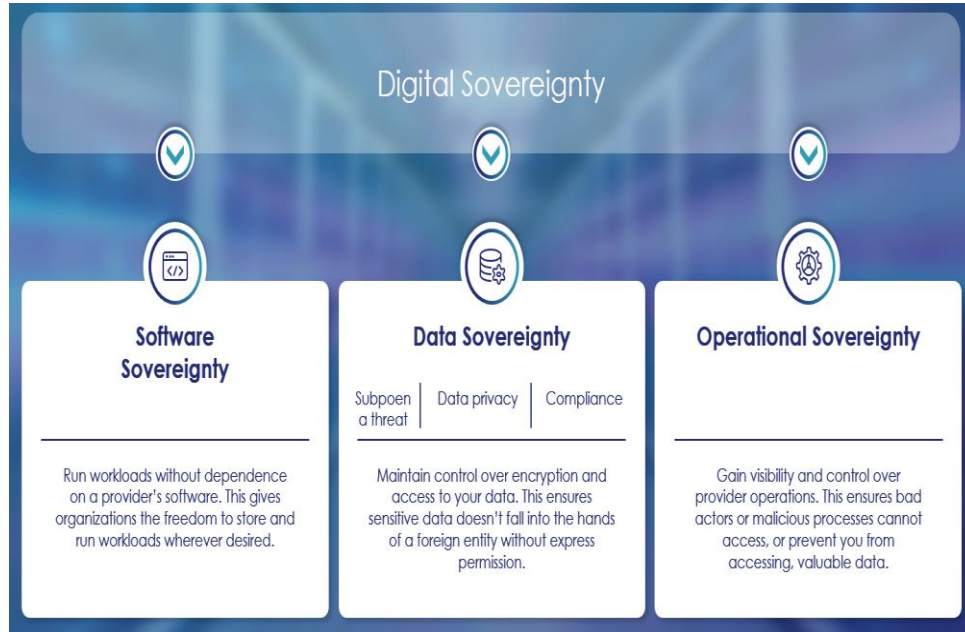
*Sovereign cloud offerings

Data Security Priorities across governments worldwide
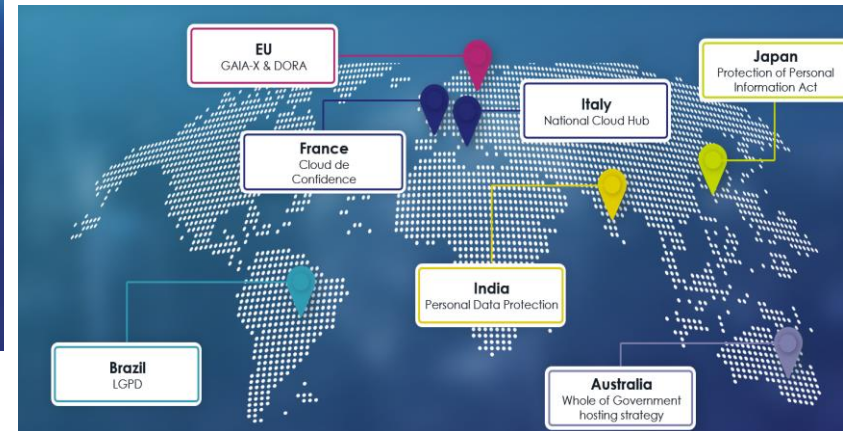
Ransomware Attacks

Australia: The Australian government has developed a National Cyber Security Strategy that includes measures to protect against ransomware attacks.

New Zealand: The New Zealand government has launched a new cybersecurity framework that includes measures to protect against ransomware attacks.

Singapore: The Singapore government has established a National Cybersecurity Agency that is responsible for protecting the country from cyber threats, including ransomware attacks.

Japan: The Japanese government has announced plans to invest $2 billion in cybersecurity over the next five years. This investment will include measures to protect against ransomware attacks.

*The State of Ransomware 2023 by Sophos

Only…

50%

of organisations have a **formal ransomware plan**, compared to **47% in 2022.**

*2023 Thales Data Threat Report

THALES

SG Gov Recommendations for Public Sector

Render data unusable even if exfiltrated from storage
T7: Hashing with salt
T8: Tokenisation
T9: Field-level encryption
P8: Managing keys to these safeguards

Partially hide the full data
T10: Obfuscation/ masking/ removal of entity attributes
T11: Dataset partitioning

Protect the data during distribution
T12: Password protecting and encrypting data files
P9: Securely distribute password out-of-band
T13: Data file integrity verification
P10: Distribute files through appropriate secure channels

*Information from Public Sector Data Security Review Committee Report

THALES

THALES

How Thales solutions can help ?

Thales CPL - Comprehensive Data Security Solutions

Applications Database File Systems Virtual Networks Big Data Containers Public and Private Cloud

IDENTIFY AND CLASSIFY SENSITIVE DATA

Data Discovery and Classification

- Data Discovery
- Data Classification
- Data Mapping

ENCRYPT OR TOKENIZE

Ransomware Protection

Database Protection

Application Data Protection

Tokenization

- Encrypt sensitive **data@rest**, **data-in-motion**
- **Tokenization**, data masking of PII
- Ransomware Protection

CENTRALIZED KEYS AND SECRETS MANAGEMENT

KMIP

Enterprise Key Management

Secrets Management

Multi Cloud

Hardware Security Modules

- Centrally manage **cryptographic keys** and **secrets**
- Root of Trust/Master keys
- Multi Cloud Key Management

Automation & Orchestration

APIs

Reduce silos

Unify policies, processes and operations

Centralize security intelligence

Review and track

THALES

THALES

Case Studies

De-Identifying Sensitive Data to preserve data privacy

Government Agency: Public Healthcare (ASEAN)

Background and Challenge

- Government organizations dealing with humongous volumes of raw & unprocessed data
- Data includes sensitive PII/PHI and other regulated identifiers
- Collected data to be cleansed to enable safe onboarding to commercial cloud and other use cases like data analytics

Solutions & Benefits

- CipherTrust Tokenization
- Identify the sensitive PII and tokenize before dumping the data for analytics
- Tokens preserve format
- High performance Vault-less tokenization
- The same platform can be used for encryption of other sensitive non-PII data

CREDIT CARD
1234 5678 9123 4567
0544-4124-4325-3490

Sensitive Data

CipherTrust Tokenization

4269-8572-9741-2570

Stored Protected Data

THALES
Building a future we can all trust

# Centralized Key Management For Private Cloud

Government Agency: Defense Sector (ASEAN)

Background and Challenge

- Private cloud backed by hyperconverged infrastructure
- Data at rest encryption for storage, virtual machines and datastores
- Need centralized key management system

Solutions & Benefits

- CM +KMIP
- Complete key lifecycle management using Ciphertrust KMS
- Multitenancy support
- Officially certified KMIP integrations by vendors like Vmware, Dell, Hpe etc.
- Highly secure FIPS certified solution
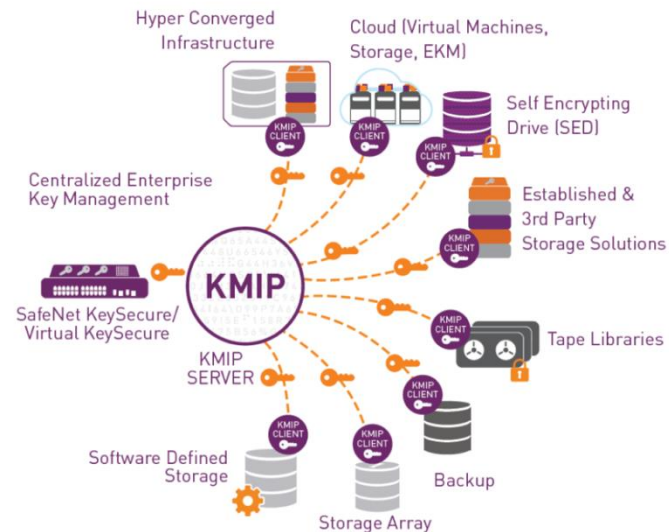
THALES
Building a future we can all trust

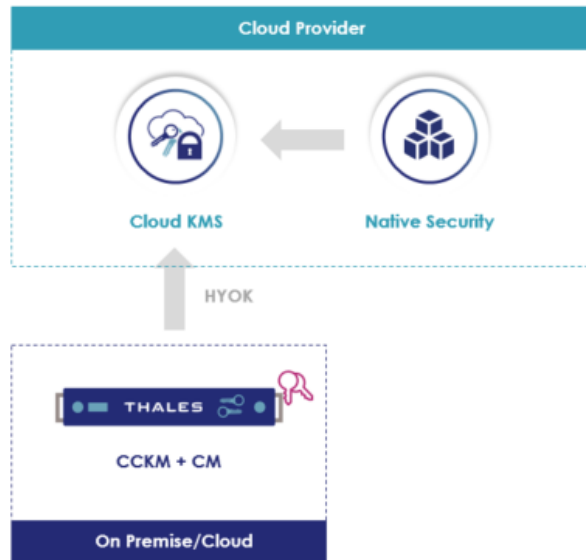# Addressing Data Sovereignty with native cloud controls

Government Agency: ASEAN

Background and Challenge

- Distributed nature of public cloud doesn't guarantee data location
- Most SAAS and PAAS offerings require cloud native encryption mechanisms
- Customer looking for data sovereignty controls in compliance to data localization laws

Solutions & Benefits

- CM +CCKM+ HSM
- Full key ownership and control using HYOK mechanism
- Keys stored outside public cloud at all times in customer controlled environment.
- Natively supported by public cloud platforms like AWS and Google
- Typically doesn't require any changes to underlying applications.

Cloud Provider

Cloud KMS ← Native Security

HYOK

THALES

CCKM + CM

On Premise/Cloud

Google Workspace CSE

aws XKS

THALES
Building a future we can all trust

# Foundational Security for critical cryptographic Keys

Government Agency: (ASEAN)

Background and Challenge

- PKI key protection in tamper resistant hardware
- Key vault for native encryption (TDE) keys
- Certified RNG for high quality cryptographic keys

Solution and Benefits

- Luna network HSM
- establish trust with a FIPS 140-3 L3 and Common Criteria evaluated network HSM
- PQC ready, crypto agile solution
- keys never leave tamper-proof root of trust
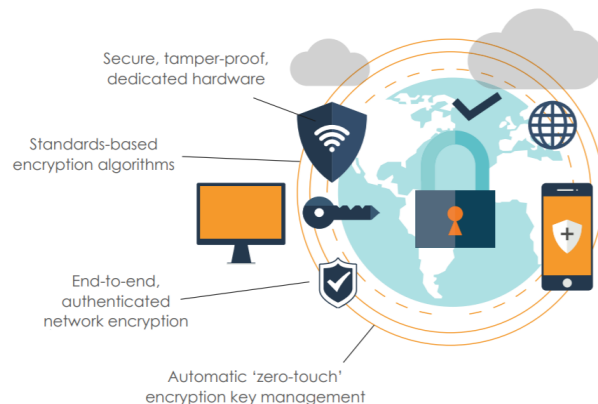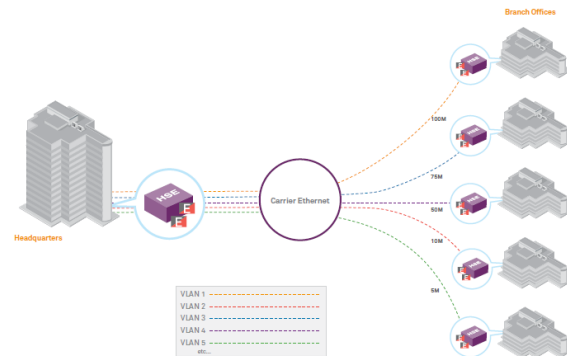- generate unique high entropy keys

THALES
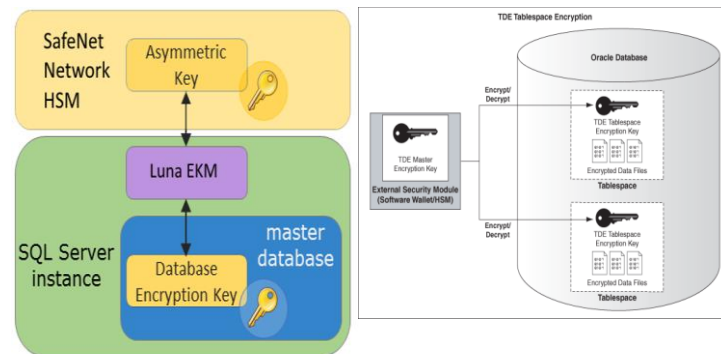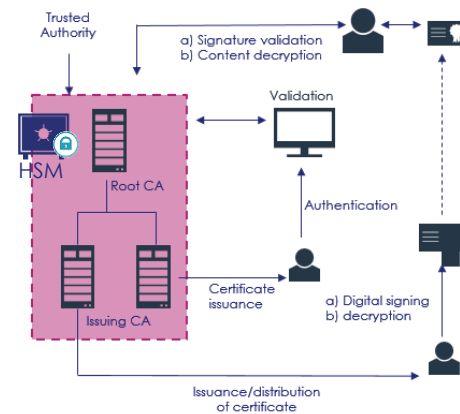
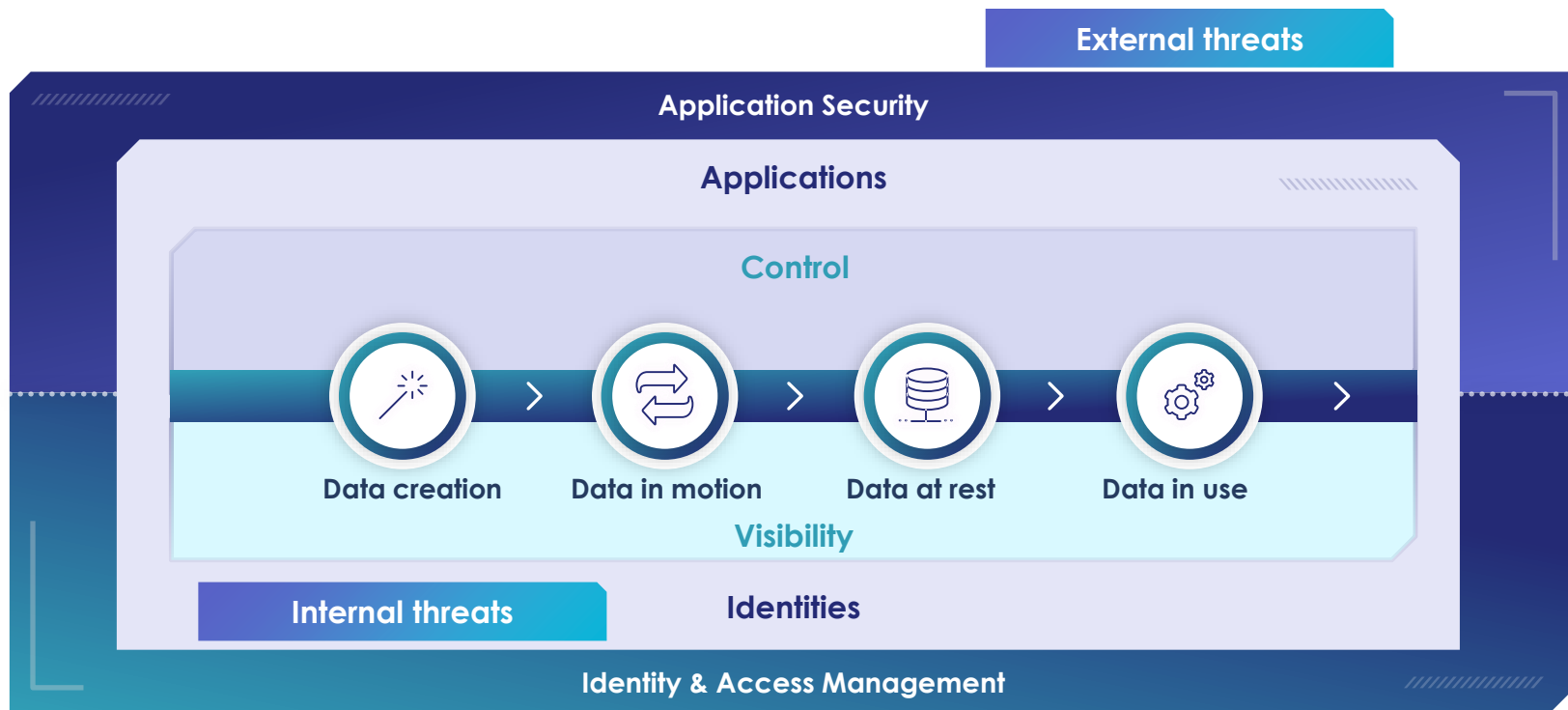## Government Agency: Civil Aviation (ASEAN)

Background and Challenge

- Protection of sensitive operational data sent over high-speed networks between data centers

- Multiple 1G channels, layer 2 network

- Solution to be compatible with current network topology

- Performance and Availability critical

Solutions & Benefits

- CN series hardware encryptors

- True end to end, authenticated encryption

- Microsecond latency, Near-zero overhead

- FIPS 140-2 L3, Common Criteria, NATO, UC APL accredited

- State-of-art automatic, zero-touch key management

- Quantum ready with QKD and QRNG integrations

Secure, tamper-proof, dedicated hardware

Standards-based encryption algorithms

End-to-end, authenticated network encryption

Automatic 'zero-touch' encryption key management

THALES
Building a future we can all trust

Thales + Imperva secure your most sensitive data **...and all paths to it**

External threats

Application Security

Applications

Control

Data creation

Data in motion

Data at rest

Data in use

Visibility

Internal threats

Identities

Identity & Access Management

THALES

Thank you

THALES