Word on the Street: Top 5 Tech Trends

Gina Scinta
Deputy CTO

Thales Trusted Cyber Technologies

Cyber Security Landscape

2024 Data Threat Report - Federal Edition Background

- Report summarizes key findings from the 2024 Thales Data Threat Report (DTR) focused on USFED agencies and organizations
- Examines the differences between USFED survey respondents and global responses across all industry verticals.
- S&P Global Market Intelligence Report commissioned by Thales

Download Report
thalestct.com/dtr

Data Breach Trends and Threats

49%

- About half of USFED agencies have been breached at some point
- Heavy security investments have dropped the percentage of breaches since 2021 from 47% to 13%

40%

- 40% of USFED have experienced a ransomware attack (12 percentage points higher than the global result)
- Planning is still poor, only one in five USFED respondents saying they would follow a formal plan in the event of an attack

27%

- Human error and zero-day/novel/unknown vulnerabilities were tied as the leading causes of cloud-based data breaches at 27%
- Failure to apply MFA to privileged accounts was another major cause, at 20%

Common Root Causes of Cloud-Based Breaches

27%

Human Error

27%

Exploitation of a known vulnerability

20%

Failure to use MFA for privileged user accounts

Enterprise Observations

KEY STATISTIC

In 2024, among USFED respondent agencies and organizations that had failed a compliance audit in the last 12 months, 83% reported at least one breach in their history.

83%

KEY STATISTIC

In contrast, for those USFED agencies and organizations that had not failed a compliance audit, only 32% reported a breach history, and just 3% had a breach in the last 12 months.

32%

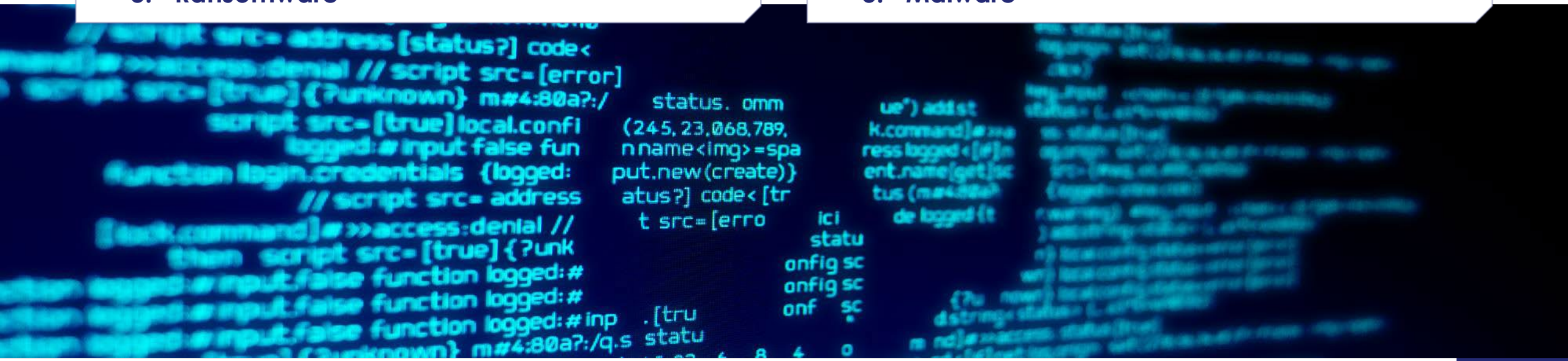
Nine out of 10 USFED respondents (93%) said they were experiencing an increase in attacks

Top 3 Fastest-Growing Threats in 2023

1. Malware
2. Phishing
3. Ransomware

Top 3 Fastest-Growing Threats in 2022

1. Ransomware
2. Phishing/Whaling
3. Malware



Top 5 Tech Trends

01

Quantum Resistant Security

02

Artificial Intelligence (AI)

03

Zero Trust

04

Multi-Cloud Security

05

Edge Security

Quantum-Resistant Cryptography

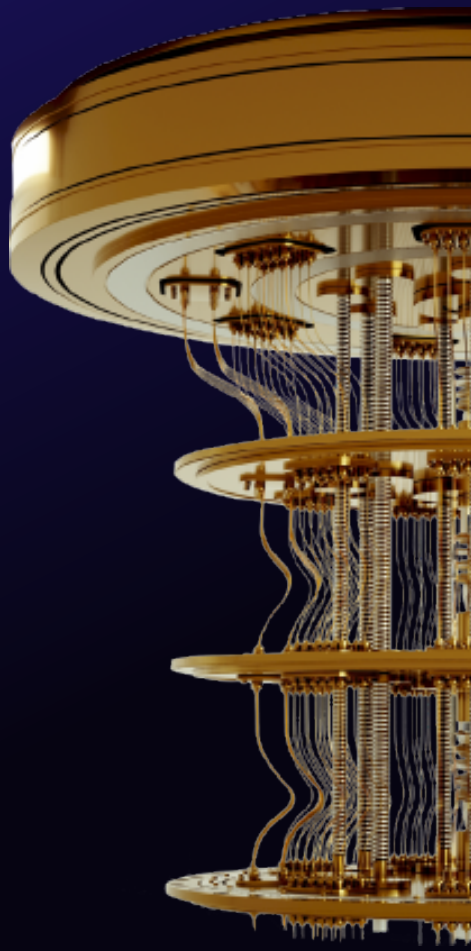
Quantum Computing

62%

of U.S. Federal respondents cite **Harvest Now, Decrypt Later** attacks leading interest in Post Quantum Cryptography (PQC)

Would likely create resilience contingency plans

Would prototype PQC algorithms in the next 18-24 months



USFED agencies are deploying PQC at a similar rate globally. This is likely to increase due to significant focus on PQC driven by the Quantum Computing Cybersecurity Preparedness Act, coupled with pressure on US government agencies to deploy PQC.

Word on the Street: Quantum-Resistant Security

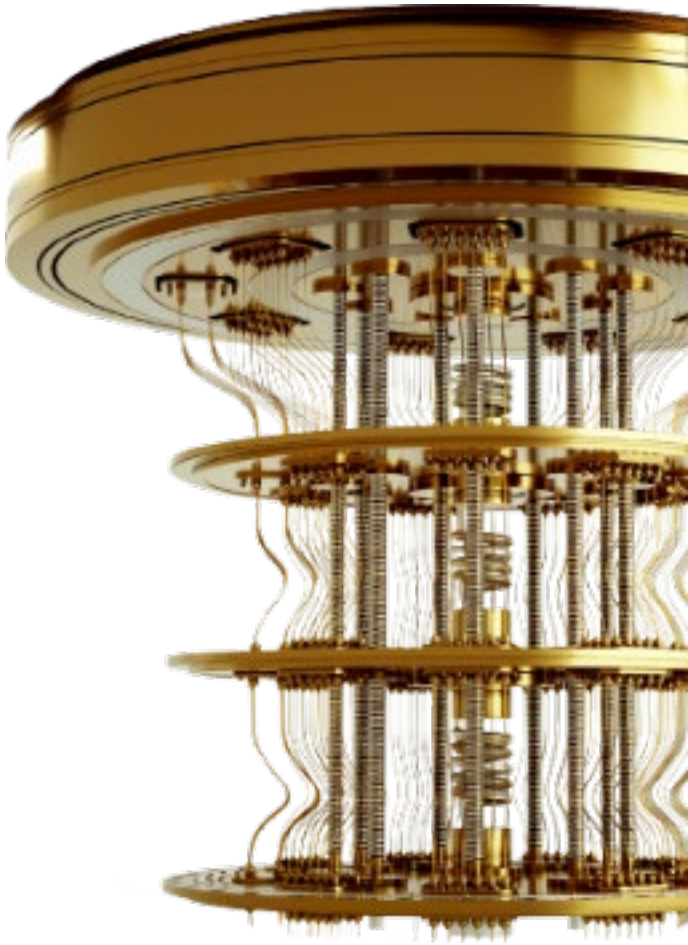
NIST initial standards for PQC algorithms released – give users options

Government tasked with putting PQC migration into FY2026 budget

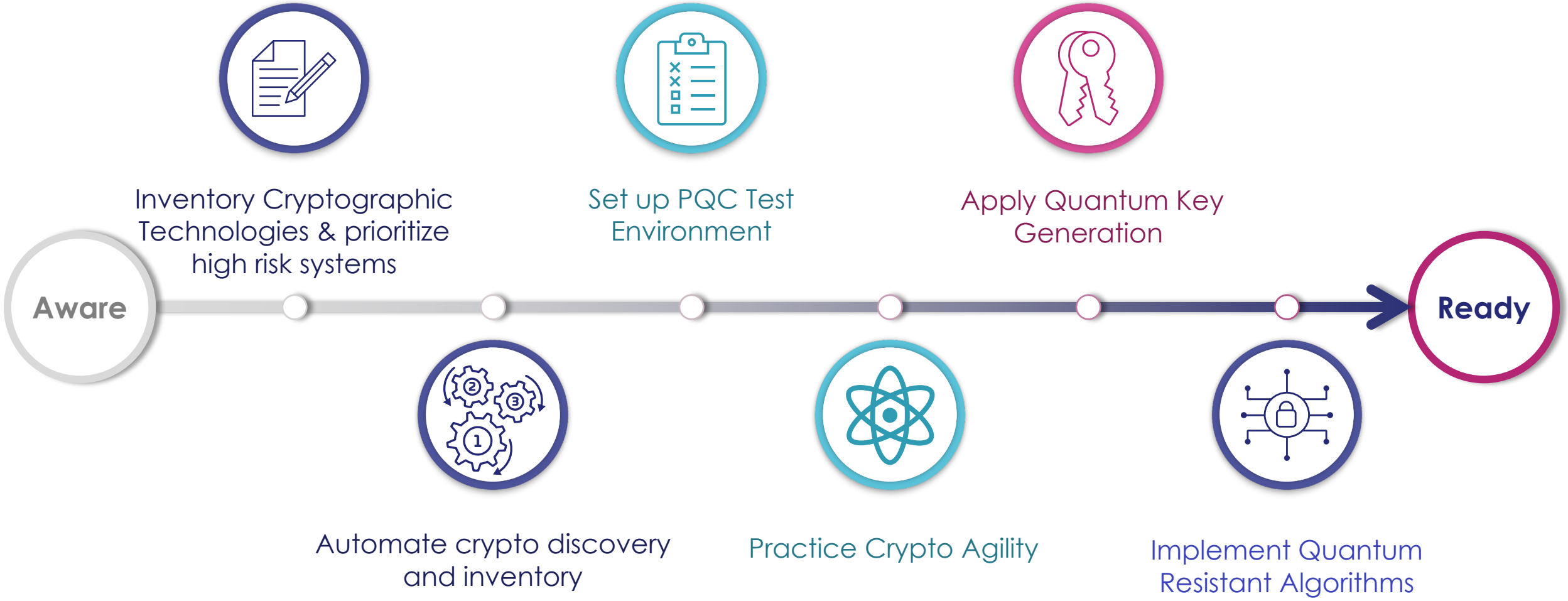
Crypto Agility should be a requirement

NIST draft publication out for review

Following CNSA 2.0 Timeline



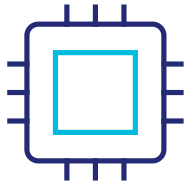
Strategy for Migration to Post-Quantum Crypto



CISA, NSA and NIST Post-Quantum Cryptography Timeline

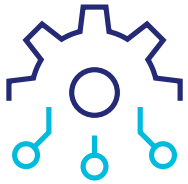
2021-2023

Inventory and prioritize systems



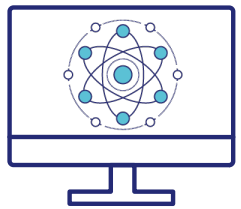
2024

NIST post-quantum cryptography standard published



2024-2030

Transition of systems to NIST post-quantum cryptography standard



2030

Cryptographically relevant quantum computer potentially available

NIST Released First Three Post-Quantum Encryption Standards

Start Getting Used to Names

NIST Released August 13, 2024

ML-KEM

- Formerly CRYSTALS-KYBER
- FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism

ML-DSA

- Formerly CRYSTALS-Dilithium
- FIPS 204 Module-Lattice-Based Digital Signature Standard

SLH-DSA

- Formerly SPHINCS+
- FIPS 205 Stateless Hash-Based Digital Signature Standard

FN-DSA

- Formerly FALCON
- Designed for digital signatures
- Slated draft FIPS late 2024

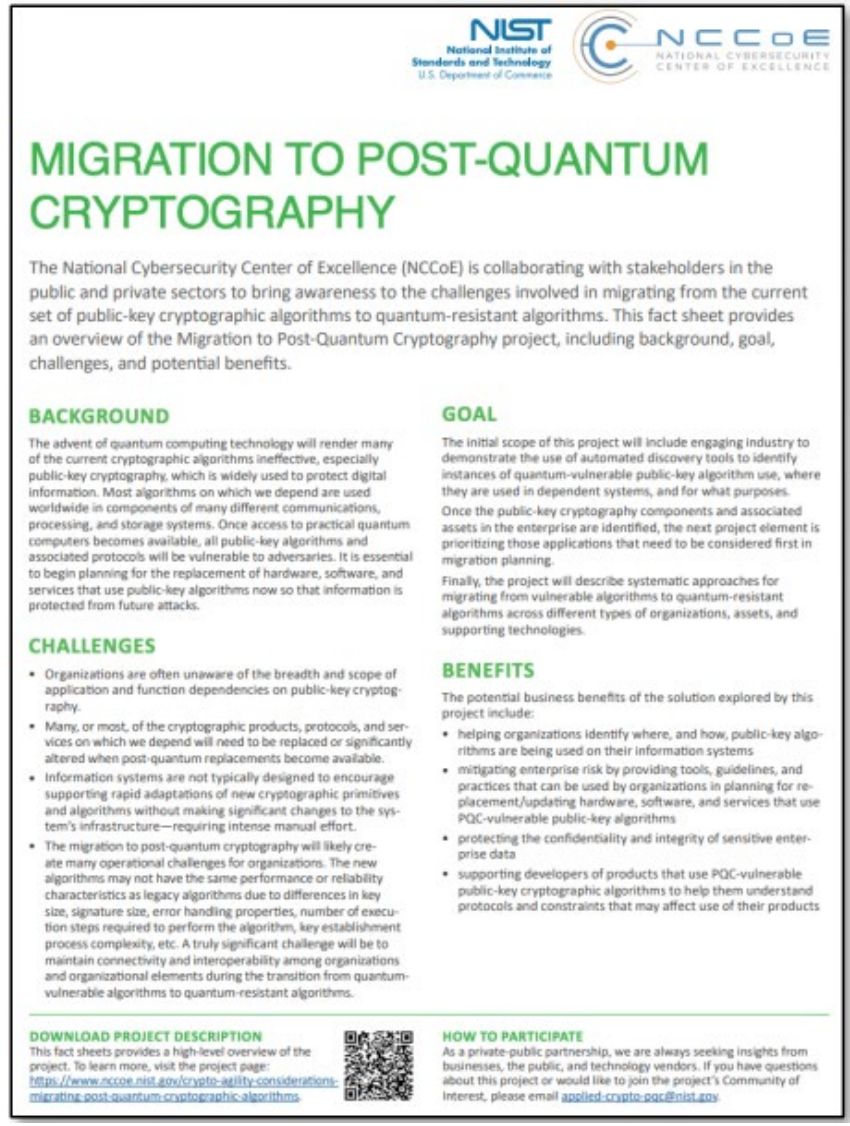
HQC

- Serves as backup for ML-KEM
- NIST plans to issue draft standard 2026
- Final standard expected 2027

Standardization Forthcoming

NCCoE "Migration to Post-Quantum Cryptography" Project

- **NIST's engagement with the community to address issues related to PQC migration**
- **Thales was a founding participant in June 2022**
- **Now the largest NCCoE project with >40 collaborators from government, industry and financial sectors**
- **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**



NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE National Cybersecurity Center of Excellence

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.

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.

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.

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 sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-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 PQC Standards Implementation Timeframe

High Speed Encryption (HSE)

Firmware supports all NIST pre-standard algorithms

PQC Algorithm Standards implemented H2 2025

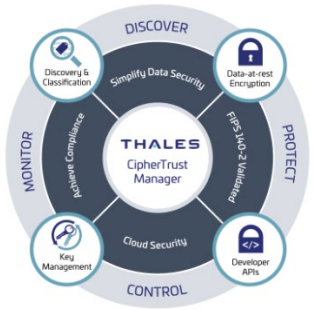
Submitted for Certifications

Luna T-Series HSM

Pre-standards available with Firmware Upgrade

PQC Algorithm Standards implemented H1 2025

Submitted for Certifications



CipherTrust Data Security Platform (CDSP)

Cryptographic Inventory of CipherTrust Data Security Platform

Implement Quantum Safe Communications, Services & Manufacturing 2025/2026

Submitted for Certifications

Identity Access Management (IAM)

Adding PQC capabilities to next generation smartcard platforms

PQC Enabled Smartcards/Tokens Engineering samples in 2026

PQC enabled smartcards/tokens released in 2027. Submitted for Certifications

Artificial Intelligence (AI)

The AI Boom is Underway

31%

of USFED respondent organizations plan to integrate AI into their core products and services in the next 12 months,

- 9 percentage points higher than global respondents.

27%

of USFED organizations are experimenting with AI, compared to 33% of all respondents.

- **This suggests that USFED agencies and organizations are embracing innovations in AI through integration at a much higher rate than the general survey population.**

Word on the Street: Artificial Intelligence (AI)

Safe to Use
Secure from Adversary
Verify/Trust the Results

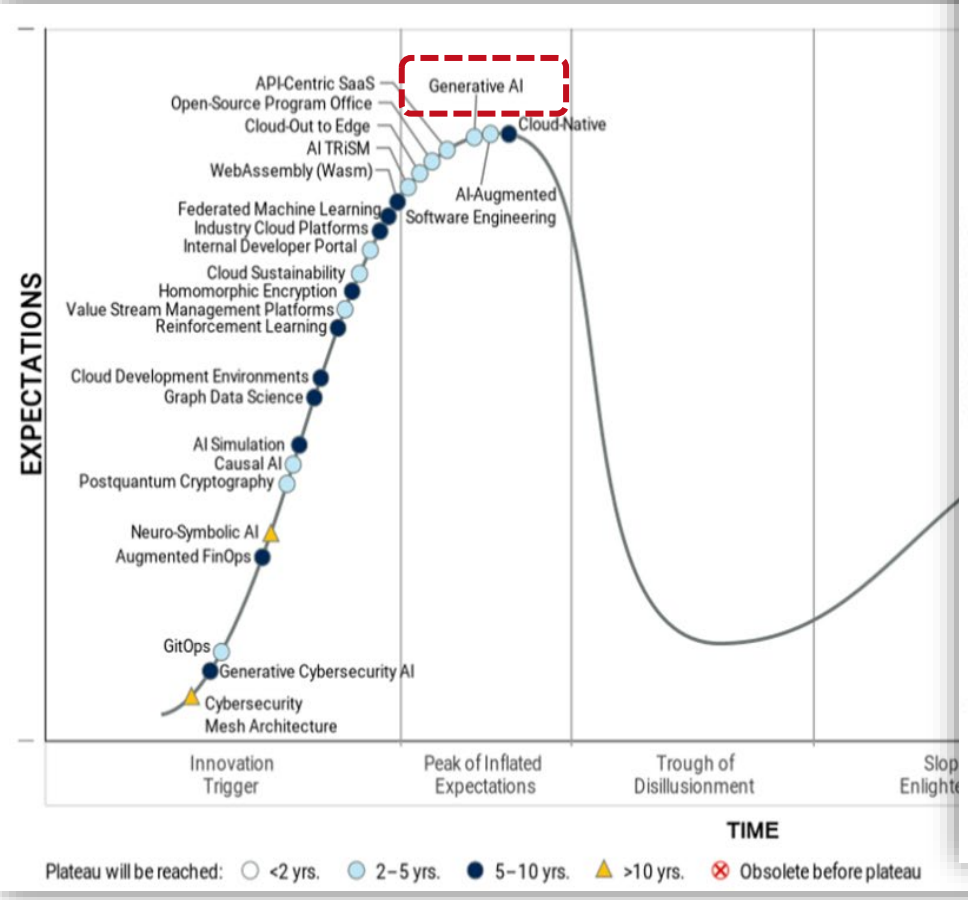
Need to ensure you are protecting data so it can't be poisoned

Need tools to sift thru and automate the discovery of data

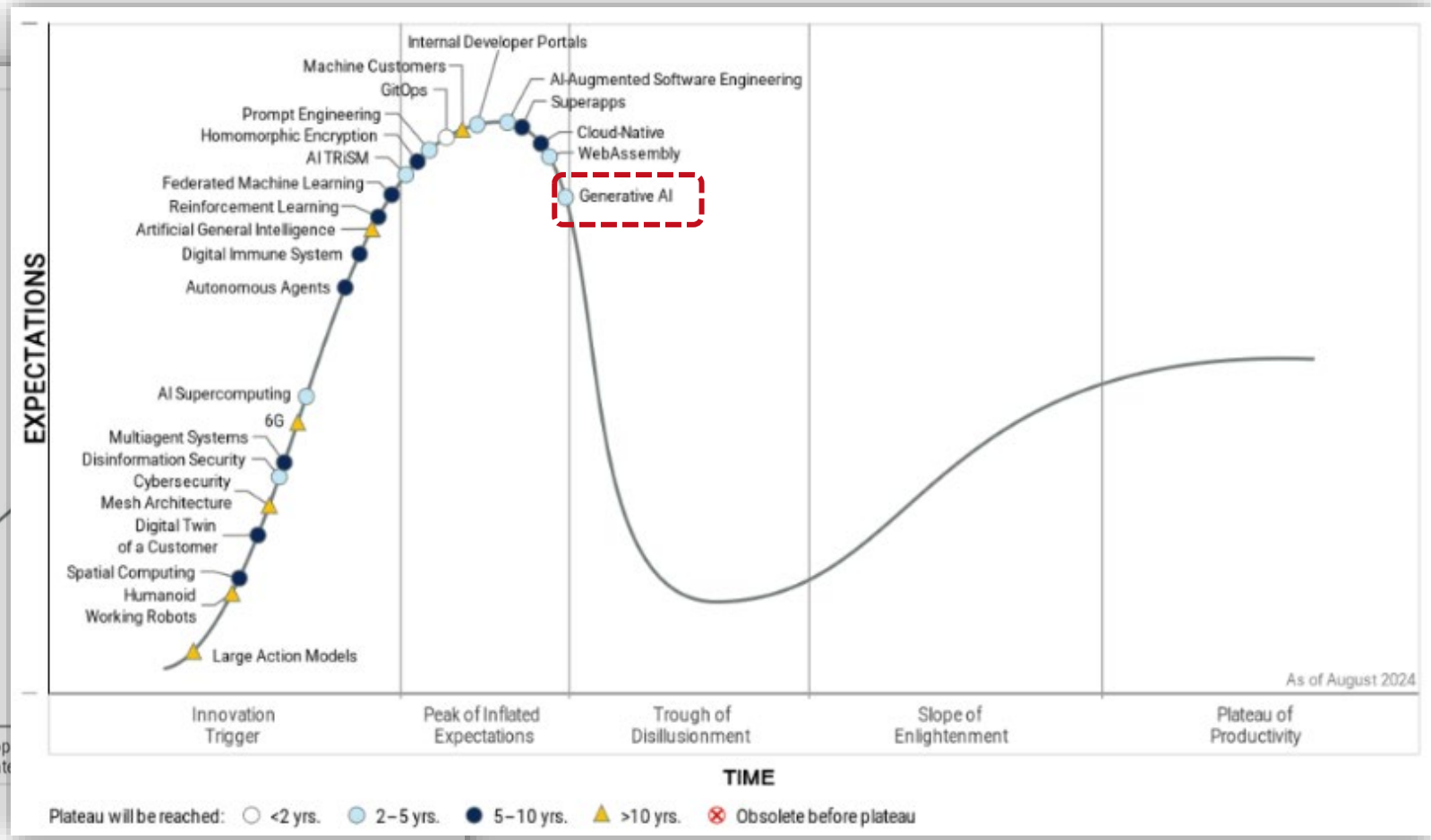
Commerical AI algorithms might not work in government systems, have to modify for more accurate results

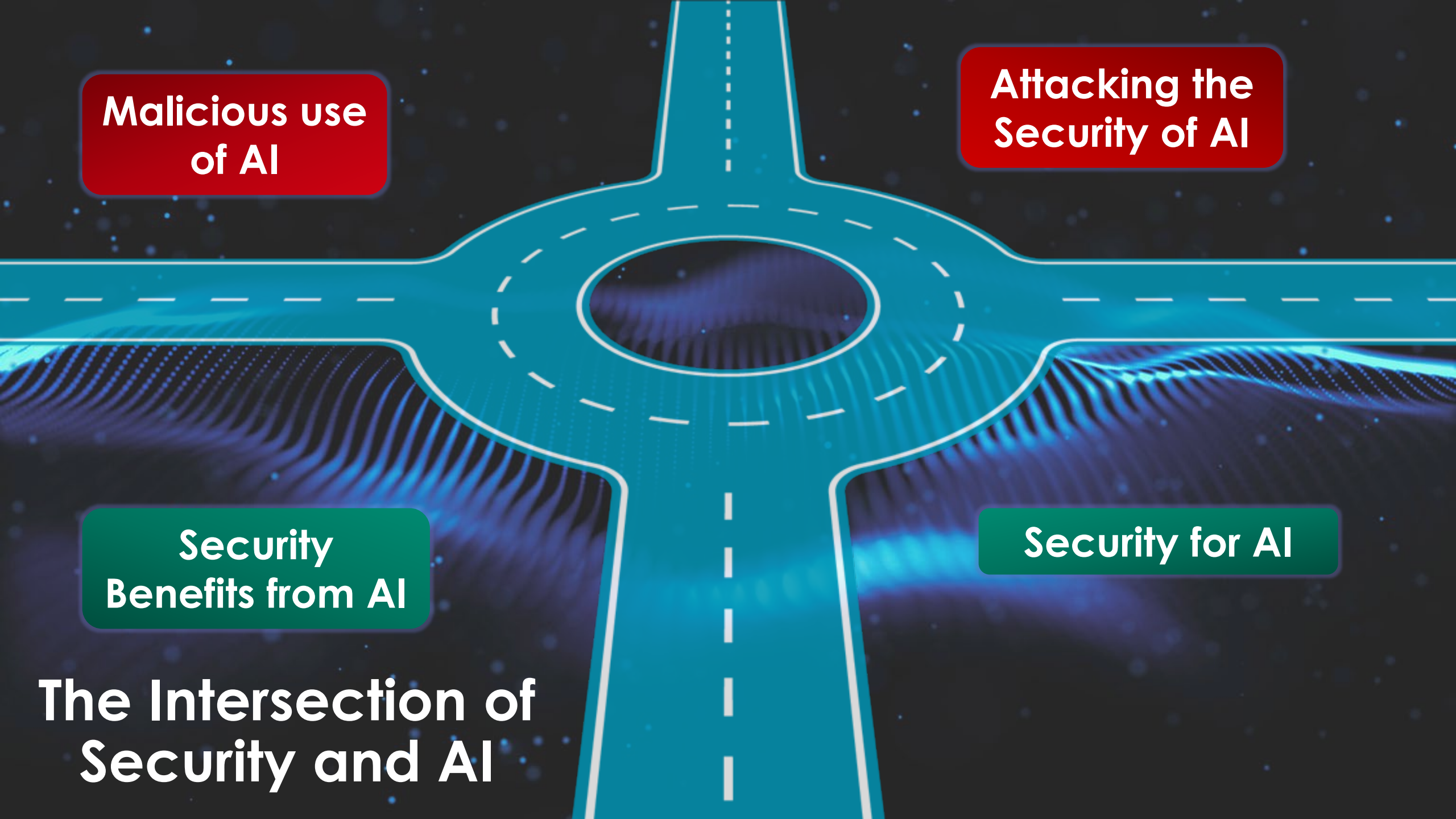
Gartner Hype Cycle for Emerging Technologies

GenAI at Peak of Inflated Expectations
August 2023



GenAI Over the Peak of Inflated Expectations
August 2024




Malicious use of AI
Attacking the Security of AI
Security Benefits from AI
Security for AI
The Intersection of Security and AI

Data Controls and Protection for AI/ML Systems

Discover and classify data.
Prepare data for tokenization and model training.

Monitor all data access.
Full audit of all data access by users and applications.

Behavior Analysis & Anomaly Detection.
Detect data misuse, abuse or breach.

Encryption.
At rest and in transit.
Maintain data integrity and prevent data exposure/theft.

Tokenize/mask data.
Ensure data security and privacy obligations are met.

Authentication & Access Control.
Enforce strong authentication and access control.

Thales Products Address OWASP Top Machine Learning Security Issues

Data Poisoning Attack	Model Inversion	Model Theft	Output Integrity Attack	Model Poisoning
Secure data storage Data separation Access control	Access control Input validation Regular monitoring	Encryption Access control Monitor and audit	Cryptography Secure communications Input validation	Model design Cryptography Access control
CipherTrust Identity Access Management	Identity Access Management Imperva	CipherTrust Identity Access Management Imperva	CipherTrust HSM Imperva	CipherTrust Identity Access Management Imperva

High Speed Network Encryption

Zero Trust

Identity Complexities and Compromise

16% of all external access to USFED IT systems and resources comes from "customers"

Of those that cite external identity as a security concern, 64% say that achieving security consistency across workforce and non-workforce identities is one of the top challenges

Word on the Street: Zero Trust

ZT is a journey and every agency has a different journey. It's a cultural shift.

Looking to use AI LLM tools to help tag the data

Data pillar is the most challenging due to the volume of data and level of detail involved with tagging the data.

DoD Controls:

91 Target ZT by FY27

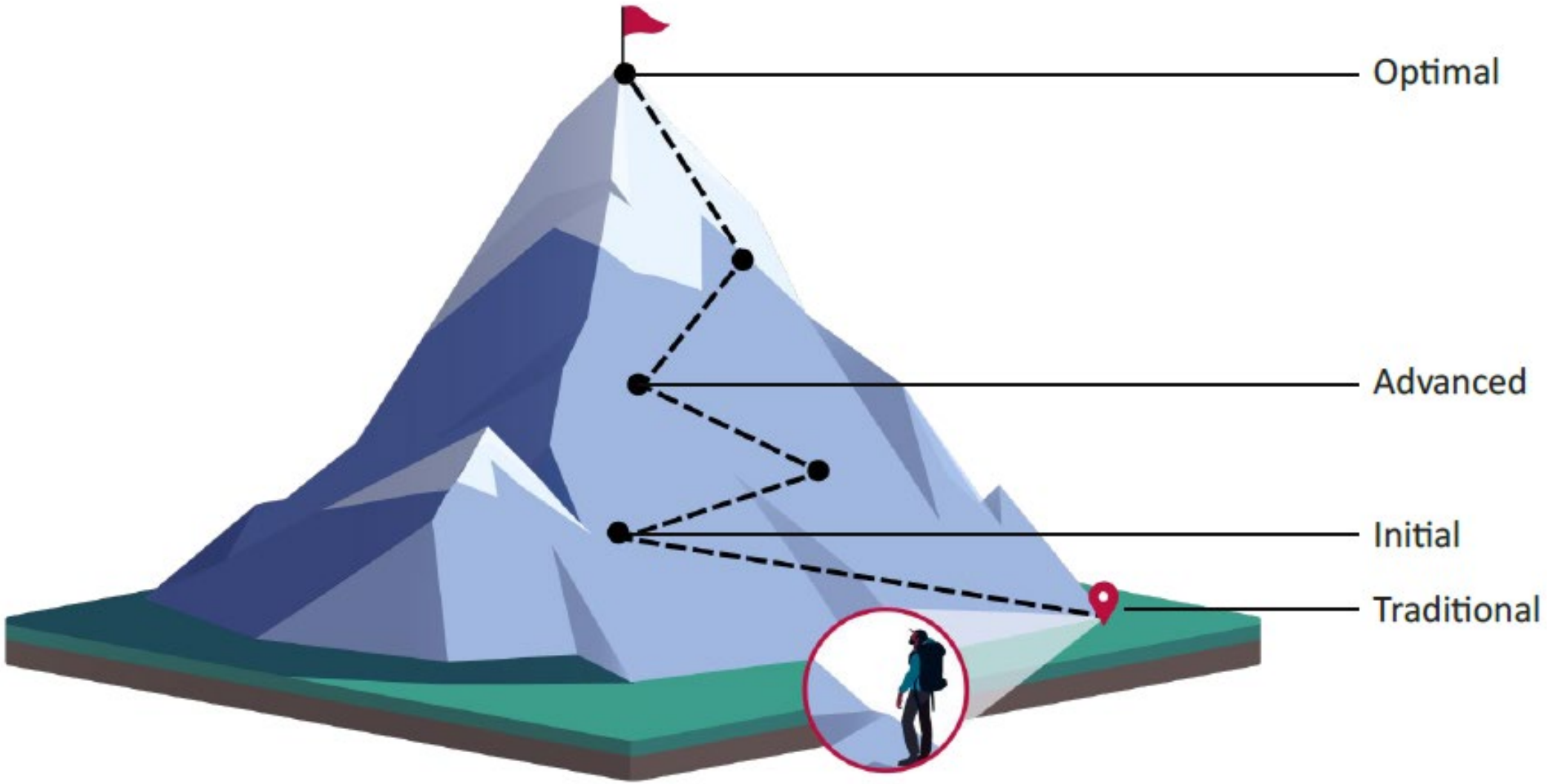
- Dell Fort Zero

151 Advanced ZT

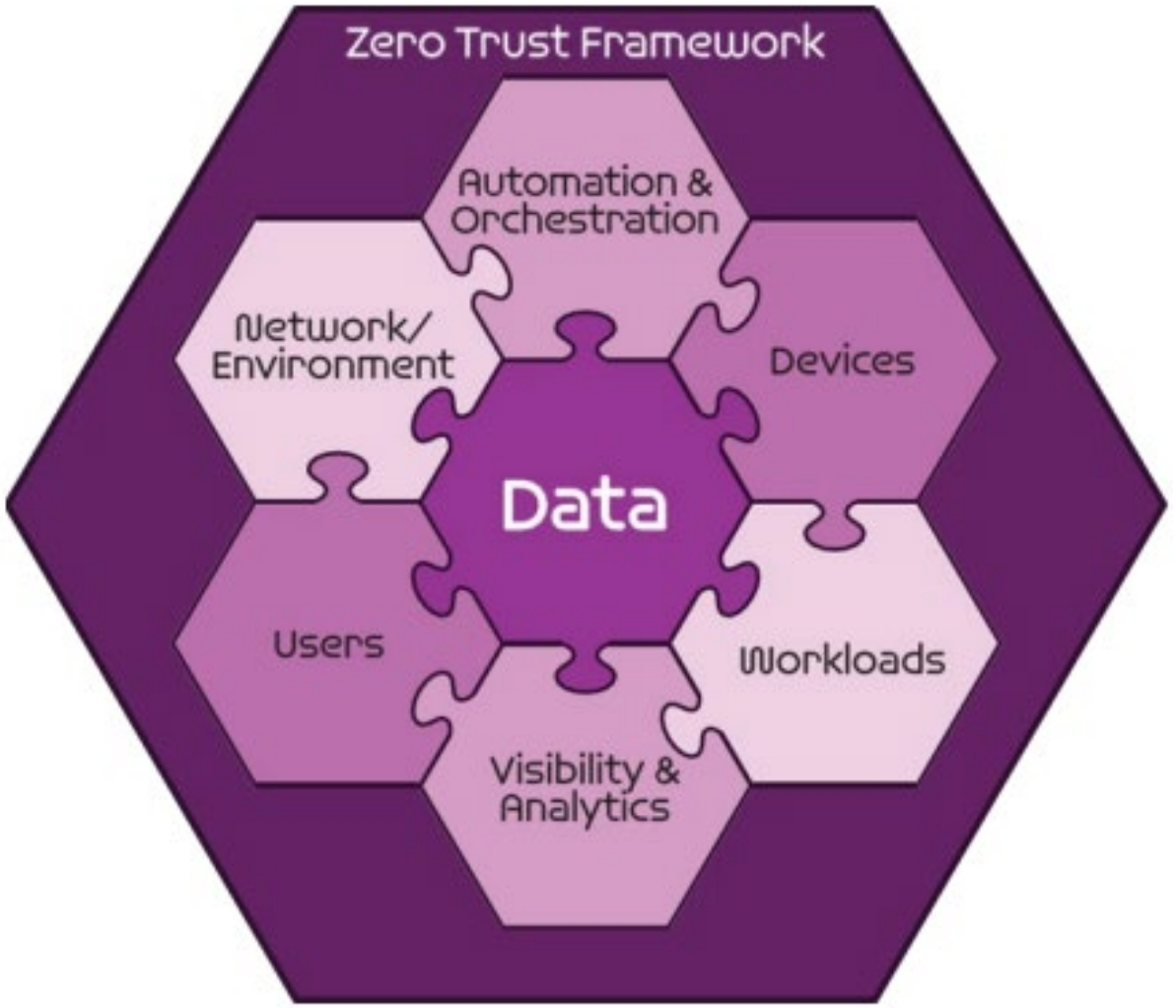
- US Navy Flankspeed
- Thunderdome

NIST Zero Trust Architecture (NIST SP 800-207)

CISA Zero Trust Maturity Journey



DoD Zero Trust Framework – Zero Trust Pillars



Thales TCT Data Protection Portfolio

Data at Rest

- **Risk Assessment & Mitigation** — Suspicious Behavior & Anomalies
- **Data Discovery & Classification** — Sensitive Data
- **Tokenization Data Masking** — PCI, PHI
- **File/DB Encryption** — Sensitive Data

Cloud Control

- **Application Level Encryption** — PII
- **Cloud Security** — BYOK HYOK BYOE

Protecting/Managing High Value Keys

- **Public Key Infra (PKI)** — For Enterprise & IoT
- **Digital Signing & Time Stamping** — Docs or Apps
- **TLS/SSL Private Key Protection** — SSL Load Balancers/ Content Inspection
- **Robot Process Automation** — Credential Data Protection

Data in Transit

- **High Speed Encryption (Layers 2, 3, 4)** — Core-Cloud-Edge
- **Application Security** — Web Apps & API
- **Secure File Transfer & Collaboration** — Inside & Outside of the Enterprise
- **Secure File Gateway** — Email and Web Apps

Imperva Data Security Fabric

Risk Assessment & Compliance

- Data Risk Analytics
- Data Activity Monitoring
- Data Risk Management
- Data Retention & Archive

Discovery

Data Discovery & Classification (CipherTrust or Imperva)

CipherTrust Data Security Platform

Encryption

- Encryption & Access Control
- Database Protection
- App. Data Protection
- Ransomware Protection
- Tokenization

THALES

Key Management

Core – Cloud - Edge

General Purpose HSM

Luna T-Series HSM

Luna as a Service

Luna Credential System

Luna Credential HSM

Network Encryption

THALES

High Speed Encryption

App Security

Imperva Web Application Firewall

End-to-End Encryption

SureDrop

Content Security

Email

Web Apps

Votiro

Identity & Access Management

Access Management

- SafeNet Authentication Service (SAS PCE)
- SafeNet Trusted Access (STA)

Phishing-Resistant MFA

- Certificate-based PKI Authentication
- FIDO Devices
- FIDO/PKI Fusion Devices

OTP & Other MFA

- 3rd Party
- Voice
- Pattern-Based
- Email
- Password
- OTP Push
- Kerberos
- Biometric
- SMS
- Number Matching

High Assurance MFA

- HA Certificate-based Smartcards & Tokens

Multi-Cloud Security

Operational complexity remains a security concern

41% of USFED respondents report that their organization **uses five or more key management systems**, down considerably from 2022 (58%)

The average number of SaaS apps reported in use by USFED has risen from 20 in 2022 to **84 in 2024**.

These results reflect a dramatic increase in cloud utilization by the U.S. government, likely driven by significant increases in the quantity of FedRAMP marketplace-certified vendors (at the time of this writing):

- **337 classified as FedRAMP-authorized**
- **116 more in process**

This also illustrates encouraging trends in reducing hybrid cloud complexity.

Cloud Key Management

25%

Of USFED respondents depend on **cloud providers to control the encryption keys** for more than half of their applications

20%

For those keys specifically under their control, **20%** of USFED respondents have chosen the **bring your own key (BYOK) approach**, a figure that has increased 6 percentage points since 2022 (14%).

Word on the Street: Multi-Cloud Security

There is no such thing as "lift and shift"!

Each app is their own "snowflake" so look at each one differently

Leverage 'aaS' where possible

SaaS, PaaS, IaaS in that order

DLA closed all their data centers 5 years ago

USAF:

70-80% of apps moved to the cloud

Cloud Security Alliance Best Practice on Cloud Encryption Keys

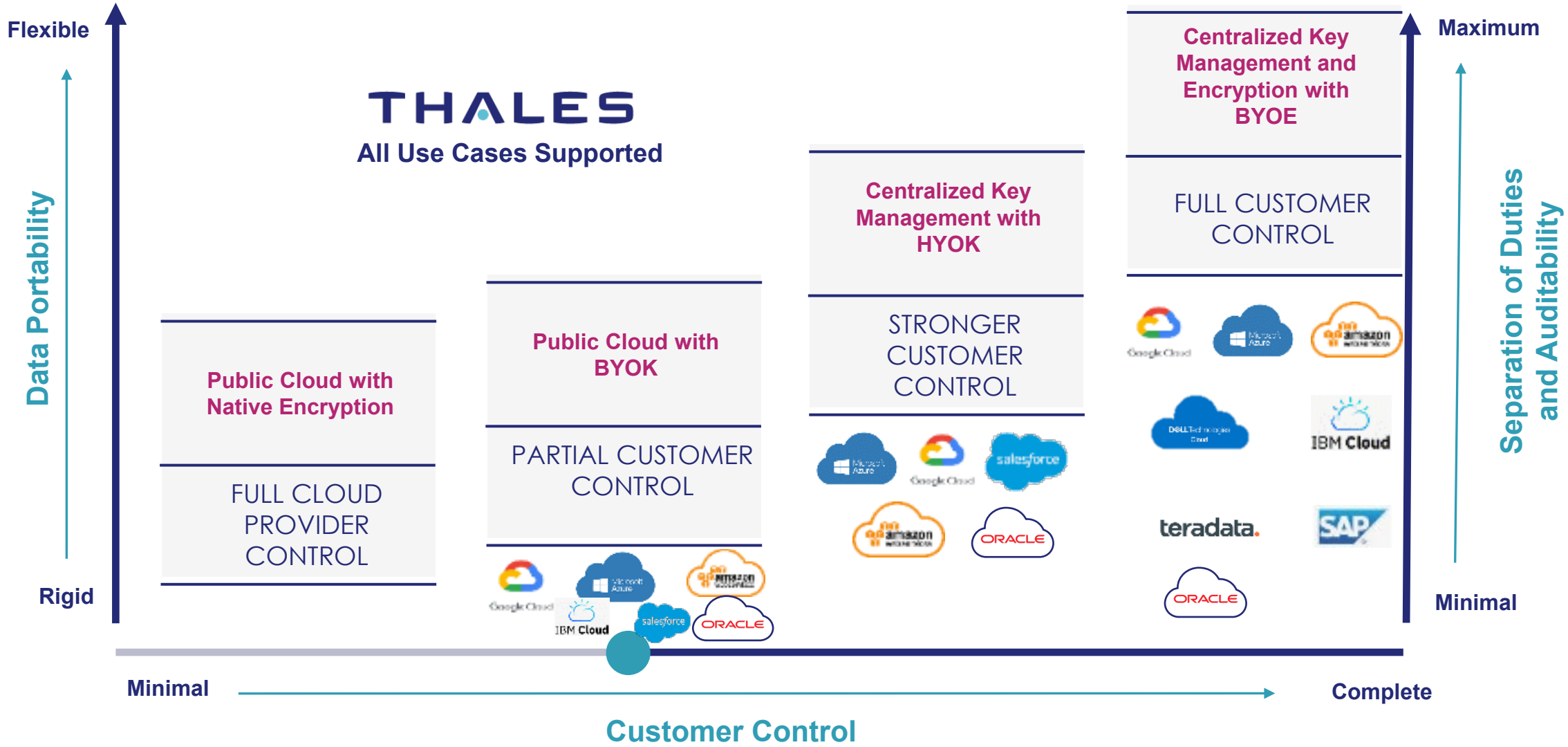
cloud security alliance®

‘[Encryption] Keys shall not be stored in the cloud but maintained by the cloud consumer or trusted key management provider.’

– EKM-04

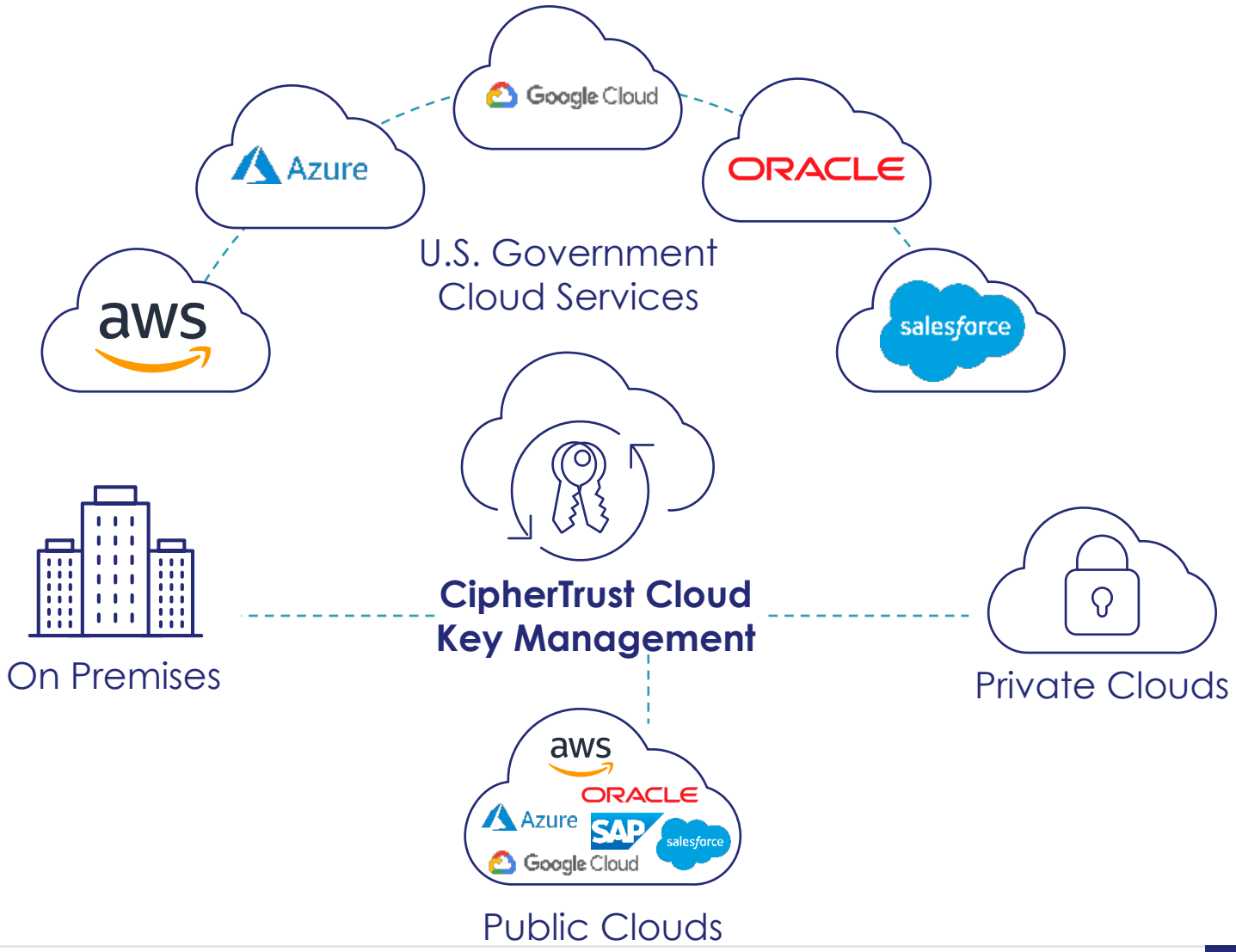
THALES

Risk Maxims to Consider in Hybrid Cloud



Multi and Hybrid-cloud Support with Thales

Amazon Web Services (AWS) KMS	Native	BYOK	
AWS CloudHSM	Native		
AWS XKS			HYOK
AWS GovCloud	Native	BYOK	
Google Cloud Platform CMEK	Native	BYOK	HYOK
Google Cloud Platform EKM			HYOK
Google Cloud Platform EKM UDE			HYOK -CC*
Google Workspace CSE			HYOK
IBM Cloud HPCS	Native	BYOK	
IBM Cloud Key Protect	Native	BYOK	
Microsoft Azure Cloud	Native	BYOK	
Microsoft Azure GovCloud	Native	BYOK	
Microsoft Azure Managed HSMs	Native	BYOK	
Microsoft Office 365		BYOK	
Oracle Cloud Infrastructure	Native	BYOK	HYOK
Oracle Cloud for Government	Native	BYOK	HYOK
Oracle US Defense Cloud	Native	BYOK	HYOK
Oracle National Security Regions	Native	BYOK	
Salesforce.com	Native	BYOK	HYOK**
Salesforce GovCloud Plus	Native	BYOK	HYOK**
Salesforce Sandbox	Native	BYOK	HYOK**
SAP Data Custodian	Native	BYOK	



Edge Security

Word on the Street: Edge Security

Won't have SME's so edge solutions need to be easy to use and manage

Have to have cloud at the edge

Engineer to the tactical edge

Has to be scalable and resilient

Has to work on a bad day same way it works on a good day!

Security Challenges at the Edge

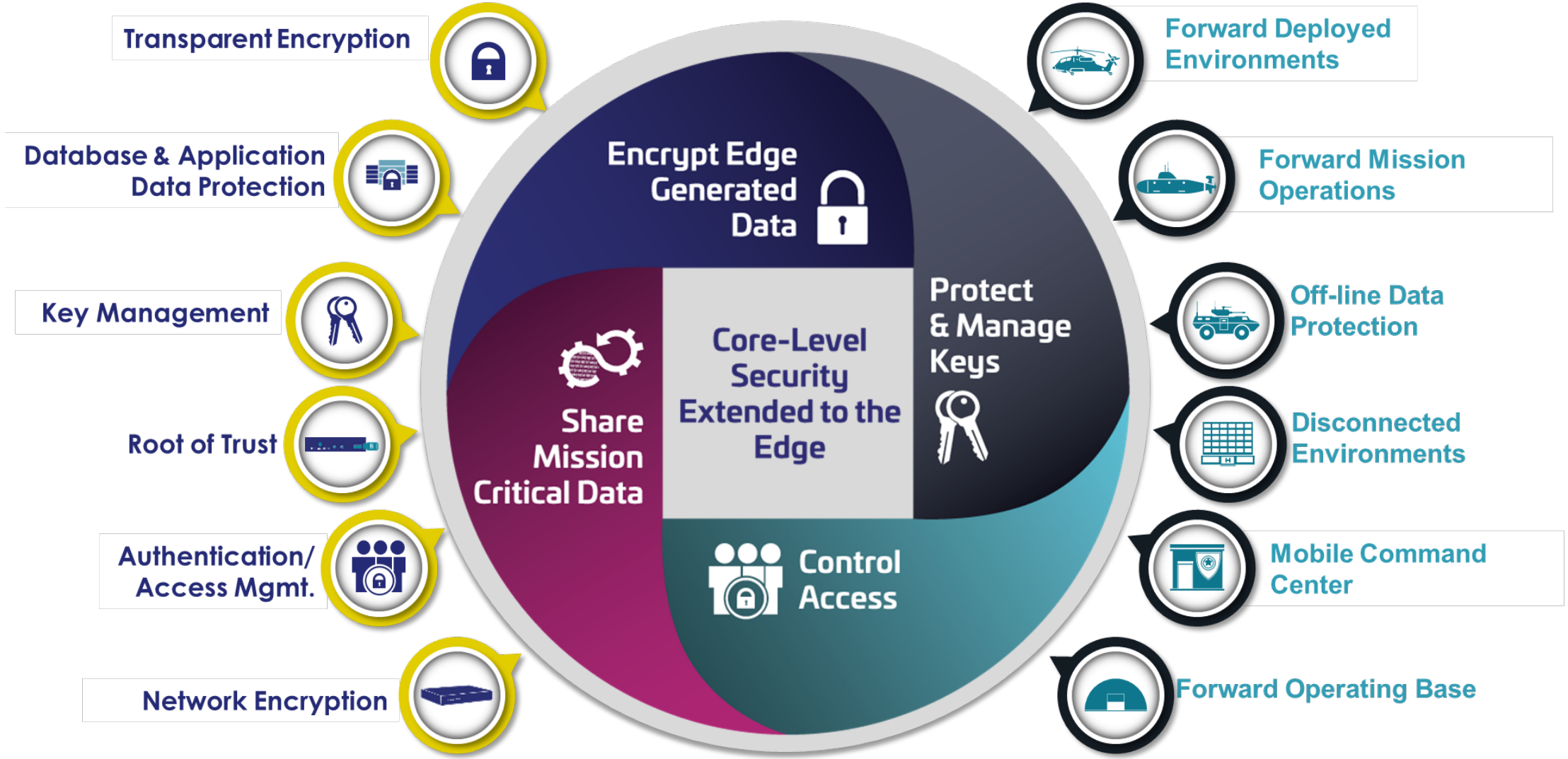
Environmental

- Harsh Environmental Conditions
- Size, Weight and Power (SWaP) Constraints
- Loss of Equipment Control
- Bandwidth Limitations

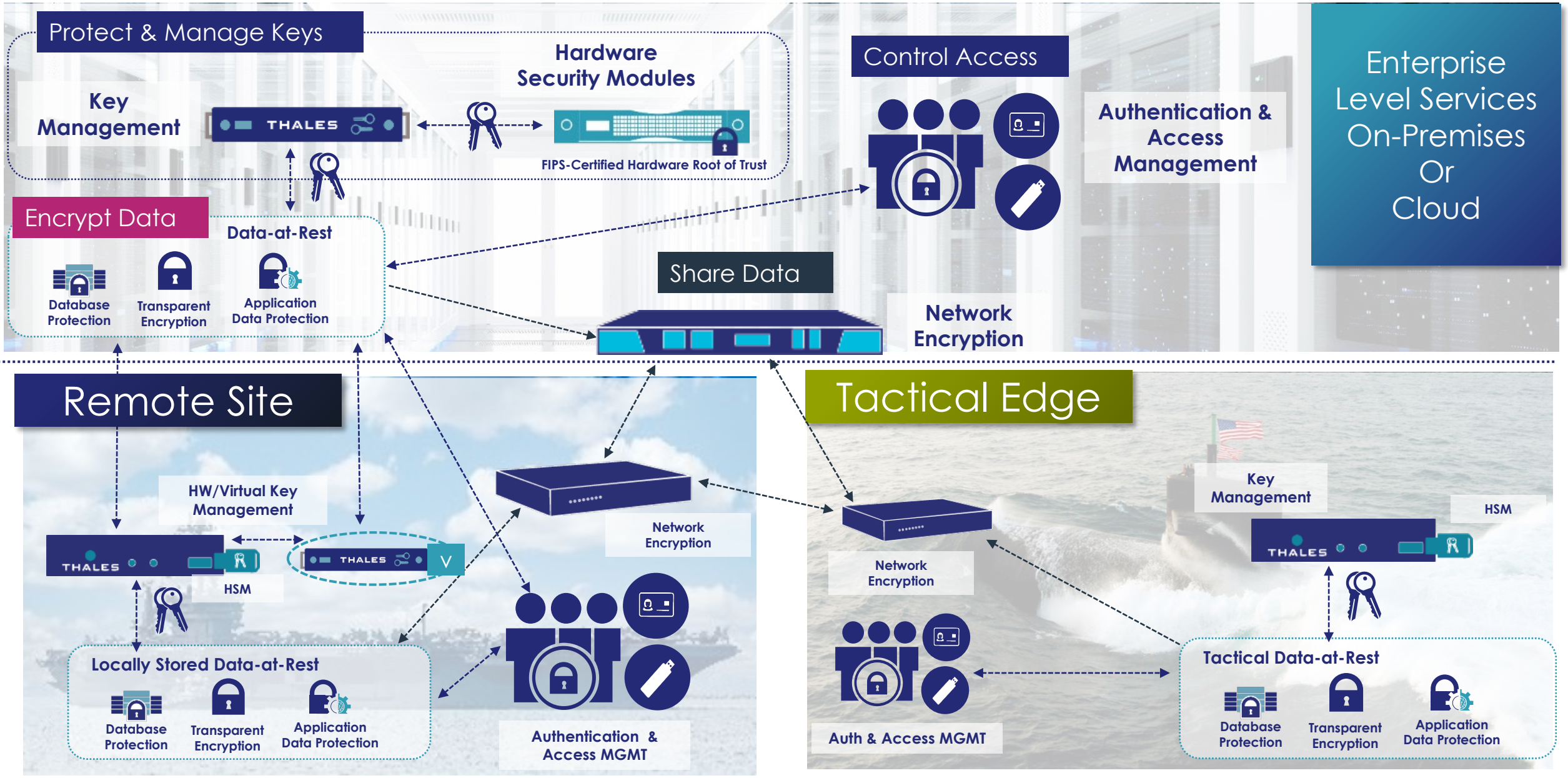
Operational

- Training Deficiencies/Limited SMEs
- Equipment Manageability (Logging, Auditing, Monitoring, Configurations, Policies)
- Data Transfer Between Enterprise and the Edge

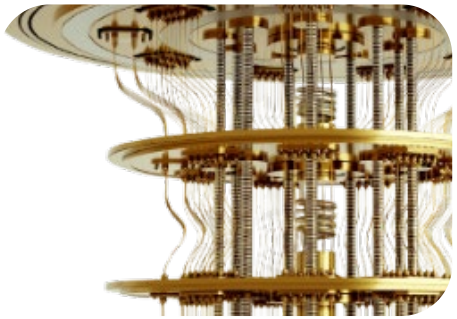
Rightsizing Data Protection for the Edge



Cloud-to-Edge Security



Summary of Top 5 Trends for 2025



Quantum-Resistant Security

Start Now!

Automate discovery and crypto inventory

Set up PQC Test Environment

Leverage Crypto Agility

Implement Quantum Resistant Algorithms

Artificial Intelligence (AI)

Safe to Use

Secure from Adversary

Verify/Trust the Results

Protect Data from Poisoning

Zero Trust

Zero Trust is a journey and every agencies journey is different

Data pillar most challenging due to shear volume of data

Multi-Cloud Security

No such thing as "lift and shift"!

Leverage 'aaS' where possible

Edge Security

Solutions need to be easy, no SME's at the edge

Has to scale and be resilient

Has to work on a bad day same as good day

Top 5 Trends Throughout the Day

Top 5 Trend	Quantum-Resistant Security	AI	Zero Trust	Multi-Cloud Security	Edge Security
Session					
Fireside Chat: Best Practices for Implementing Quantum-Resistant Security (Keynote Session)			B		
A Guide to BYOK, HYOK and BYOE with CipherTrust Data Security Platform (Thales TCT)					
Data Risk Intelligence to Redefine Data Risk Visibility and Proactive Risk Mitigation (Thales TCT)			I		
Building a Root of Trust to Secure the Most Sensitive Data with Hardware Security Modules (Thales TCT)					
FIDO Applicability to US Federal - Improved Security through Improved Management Capabilities (Thales TCT)			N		
Browser Security: The Missing Layer in our Security Strategy (Menlo Security)					
Cryptographic Blind Spots: AI's Fastest Way In (SandboxAQ)			G		
Beyond Theory: Real-World Encryption for Modern Networks (Senetas)					
Zero Trust: Top 5 Best Practices (Thales TCT)			O		

THALES
Building a future we can all trust

Questions

Gina Scinta

Deputy CTO, Thales TCT

Gina.Scinta@thalestct.com