THALES
Building a future we can all trust

Top 5 Ways to Comply with the National Security Memo on Improving Cybersecurity of National Security Systems

Gina Scinta
Deputy CTO

Thales Cyber Technologies

Thales Trusted Cyber Technologies: Who We Are

Trusted, U.S. Provider of Cybersecurity Solutions Dedicated to U.S. Federal Government






Corporate Snapshot

- Business Area of Thales Defense & Security Inc.
- U.S. Support | Cleared Employees | U.S. Manufacturing
- Protect the government's most vital data from the core to the cloud to the edge
- Maintain required U.S. Federal Government approvals and certifications to develop, support and sell products to government clients
  - Proxy Agreement with DCSA for Foreign Ownership, Control and Influence (FOCI)
  - National Security Agreement with the Committee on Foreign Investment in the United States (CFIUS).
- Trusted U.S. Source of Supply of Key Technologies for the Federal Government

THALES
Building a future we can all trust

Cyber Security Landscape

Thales Cyber Technologies

The Reality of Data Breaches

Newsweek

SolarWinds Breach Potentially Gave Hackers 'God Access': Ex–White House Official

The SolarWinds breach potentially gave hackers "God access" or a "God door" to computer systems using the companies OrionIT software, ...

The Washington Post

Analysis | The Cybersecurity 202: Combating ransomware's a top priority for the Senate Homeland Security Committee

The efforts reflect a growing appetite across Congress to tackle big cyber problems.

SC Magazine

IT leaders report lack of visibility into supply chain, widespread ...

Other supply chain attacks followed the SolarWinds announcement, ... followed by an attack on JBS, which disrupted global meat production.

ZDNet

DHS releases new mandatory cybersecurity rules for pipelines after Colonial ransomware attack

Colonial Pipeline and many other pipeline operators ignored cybersecurity reviews by the TSA before the ransomware attack that sparked ...

CNET

Data breaches break record in 2021

According to the Identity Theft Resource Center's 2021 Data Breach Report, there were 1,862 data breaches last year, surpassing both 2020's...

CBS News

How U.S. cyber policy changed after SolarWinds

This happened regularly with SolarWinds Orion software. There was no reason to suspect anything was wrong with the update.

CNET

White House to beef up cyberdefenses for National Security Agency, Defense Department

Following an executive order signed last May, the new National Security Memorandum is intended to boost cybersecurity measures at the...

ZDNet

White House creates board to review cybersecurity incidents, members to start with Log4J

The board was part of the executive order that President Joe Biden signed last year. Experts have long urged the federal government to...

Fox Business

IBM: Cost of data breaches hit 17-year high

The Conversation

What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake

Log4Shell, an internet vulnerability that affects millions of computers, involves an obscure but nearly ubiquitous piece of software, Log4j.

The New York Times

Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business

A cyberattack on the world's largest meat processor forced the shutdown of nine beef plants in the United States on Tuesday, according to ...

Security Magazine

Data breaches from insiders can cost as much as 20% of ...

Data breaches from insiders can cost as much as 20% of annual revenue ... As companies emerge from the pandemic, and 40% of employees are planning ...

20%
– Annual revenue cost of data breach from insiders.

ClearanceJobs

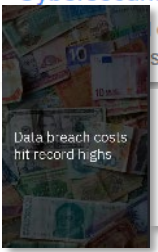
Once More Unto the Breach: DoD Data Disclosed in DISA ...

During the May to July 2019 timeframe, some of your personal information, including your social security number, may have been compromised ...

USA TODAY

What you need to know about the FireEye hack: Cybersecurity attack against US government

cybersecurity attack targeting major branches of the U.S. s put an untold number of Americans at risk of ...



TechNewsWorld

Data Breaches Affected Nearly 6 Billion Accounts in 2021

While the number of breaches and stolen records is on the rise, there's an

ZDNet

SBA reveals potential data breach impacting 8,000 emergency business loan applicants

SBA reveals potential data breach impacting 8,000 emergency business loan applicants. A US Senator says that the White House has "got to get ...

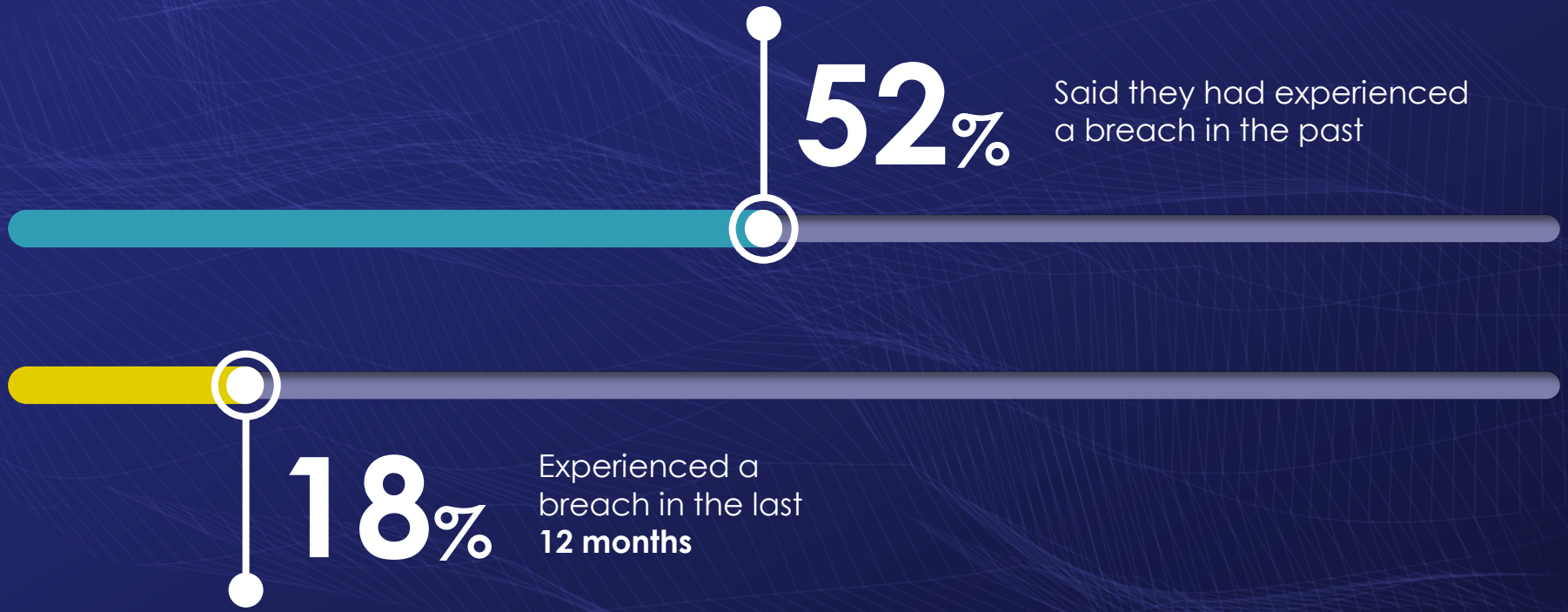
Fierce Healthcare

Healthcare data breaches hit all-time high in 2021, impacting ...

Last year, 493 providers reported a data breach, down by about 4% from 515 in 2020. Hacking/IT incidents continue to be the most common cause of

Phishing, Ransomware Driving Wave of Data Breaches

Data Breaches and Security Threats



Data Breaches and Security Threats

56% of global respondents identified **malware** as the most **common cause** of **increased** attacks

53%

2nd - Ransomware

40%

3rd - Phishing/ Whaling

37%

4th - Denial of Service

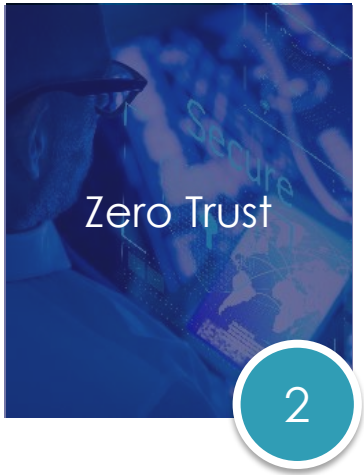
28%

5th - Brand Impersonation

National Security Memo on Improving Cybersecurity of National Security Systems

Top 5 Ways to Comply with the Cyber National Security Memo for NSS

Jan 19, 2022 Memo Requires National Security Systems to Employ Cybersecurity Measures that are Equivalent to or Exceed those required in EO 14028



THALES

THALES

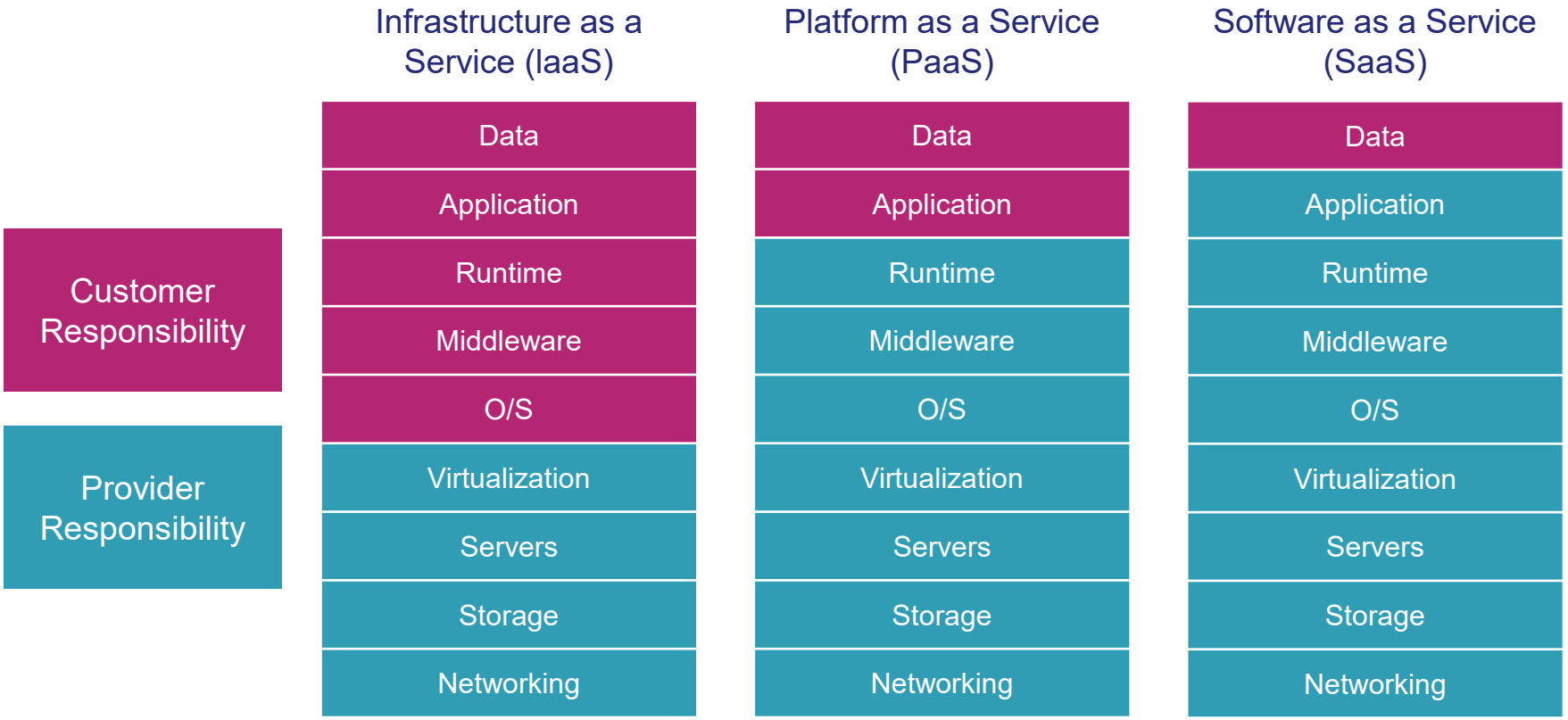
Cloud Security

Section 1 (b) (i), (v)

"…minimum security standards and controls related to cloud migration and operations for NSS,…"

"Develop a framework to coordinate and collaborate on cybersecurity and incident response activities related to NSS commercial cloud technologies"

Shared Responsibility Model for the Security Architect



THALES

Protecting Data in the Cloud

Complementing Public Cloud with Operational Efficiency, Competing with Data Security Vendors with Platform

Highly Sensitive Data → Protect Effectively → Bring Your Own Encryption

Sensitive Data → Native Cloud Encryption → With → Bring Your Own Key

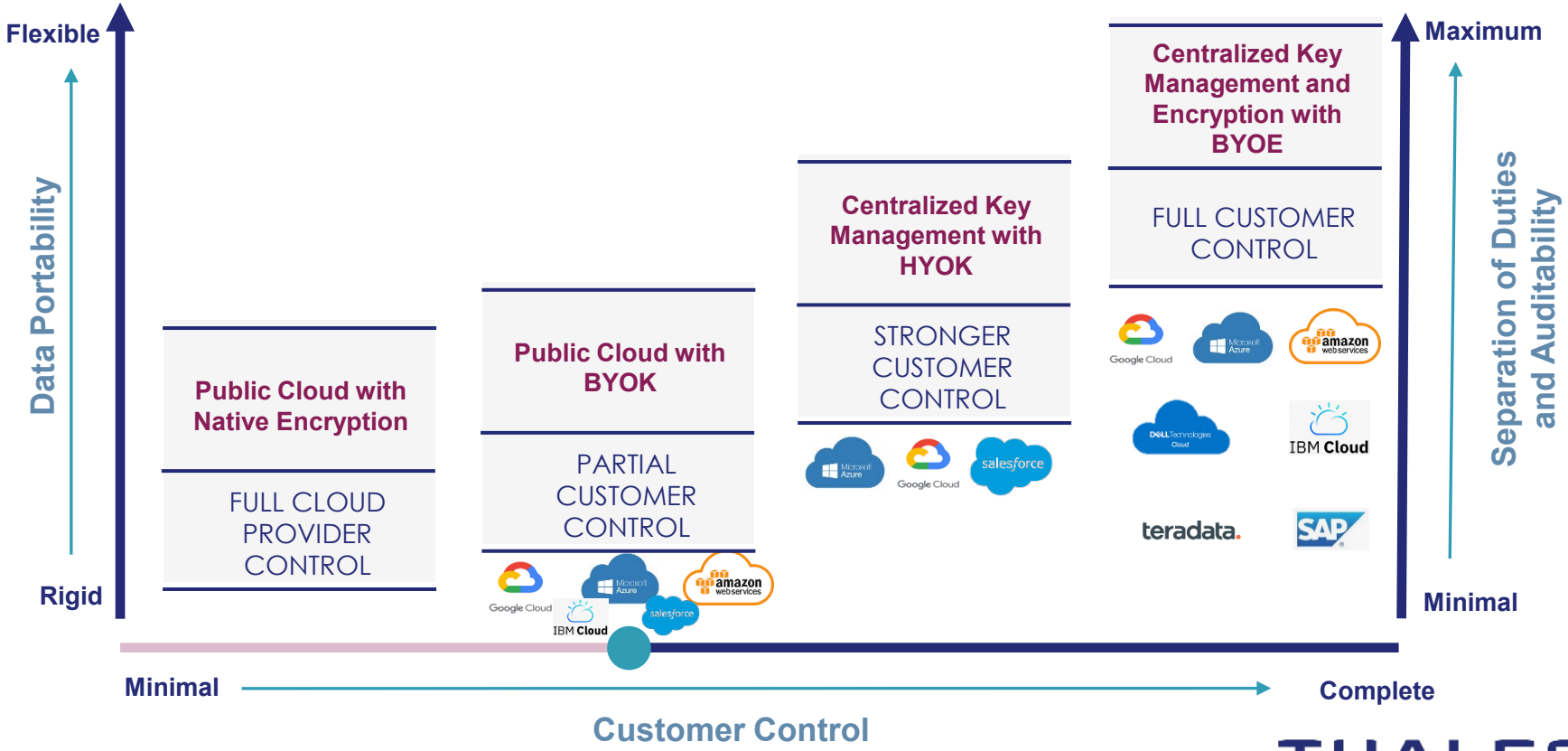
Shared Responsibility Model

IaaS	PaaS	SaaS
Data	Data	Data
Application	Application	Application
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking

Customer Responsibility | Provider Responsibility

THALES

Risk Maxims to Consider in Hybrid Cloud



THALES

Data at Rest Encryption Choices

Cloud Native Encryption

Pluses

- Easy
- Low direct costs

Minuses

- Cloud provider sources, holds the keys
- Generally identical to *full disk encryption*, serving OS clear data
- Very high "indirect" costs

Bring Your Own Encryption

Pluses

- Multi-cloud mobility
- OS-level access controls
- Advanced capabilities
- Low "indirect" costs

Minuses

- Can seem complex
- BYOE for PaaS requires developer assistance
- Medium direct costs

THALES

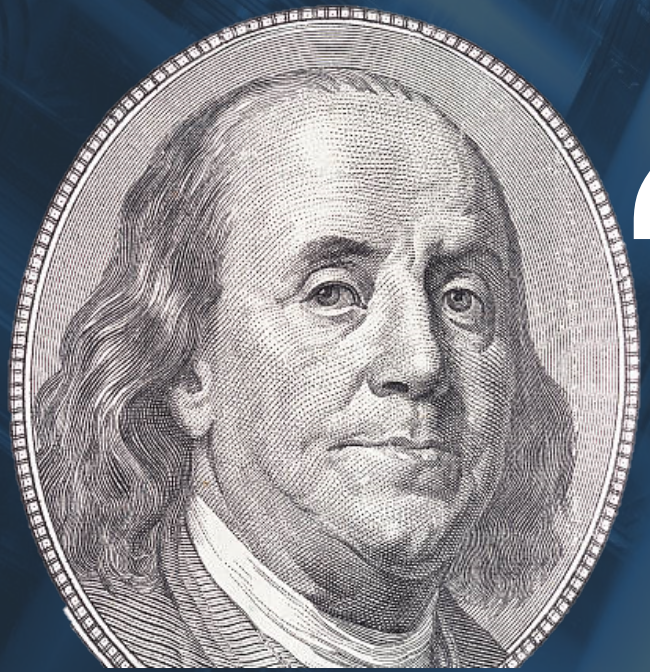
Adopting a Zero Trust Architecture

Section 1 (b) (ii) (A) & (B)

"…prioritize resources for the adoption of Zero Trust Architecture"

"Develop a plan to implement Zero Trust Architecture, which shall incorporate as appropriate:

- NIST Special Publication 800-207
- CNSS instructions on Zero Trust Reference Architectures



“Three can keep a secret, if two of them are dead”

Benjamin Franklin

Who We Can't Trust

"Nobody"

THALES

Zero Trust – There is No "Safe" Network

- The enterprise **security perimeter is no longer a physical location**; it is a set of access points dispersed in and delivered from the cloud
- **Identities are at the core of access decisions**, not the data center.
- The **identity of the user/device/service** provides key context for the application of access policies
- **Zero trust access rules** are as granular as possible to **enforce least privileges** required to perform the action

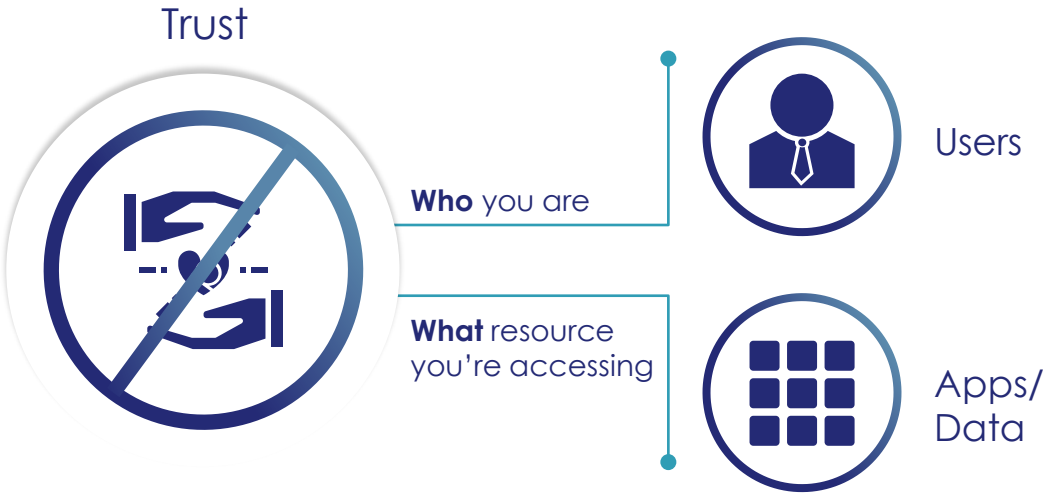
When there is no defined security perimeter, secure access decisions must be centered on the identity of the entity at the access point

Zero Trust
NOT NEW – Coined in 1994

THALES

Principle of Zero Trust Security

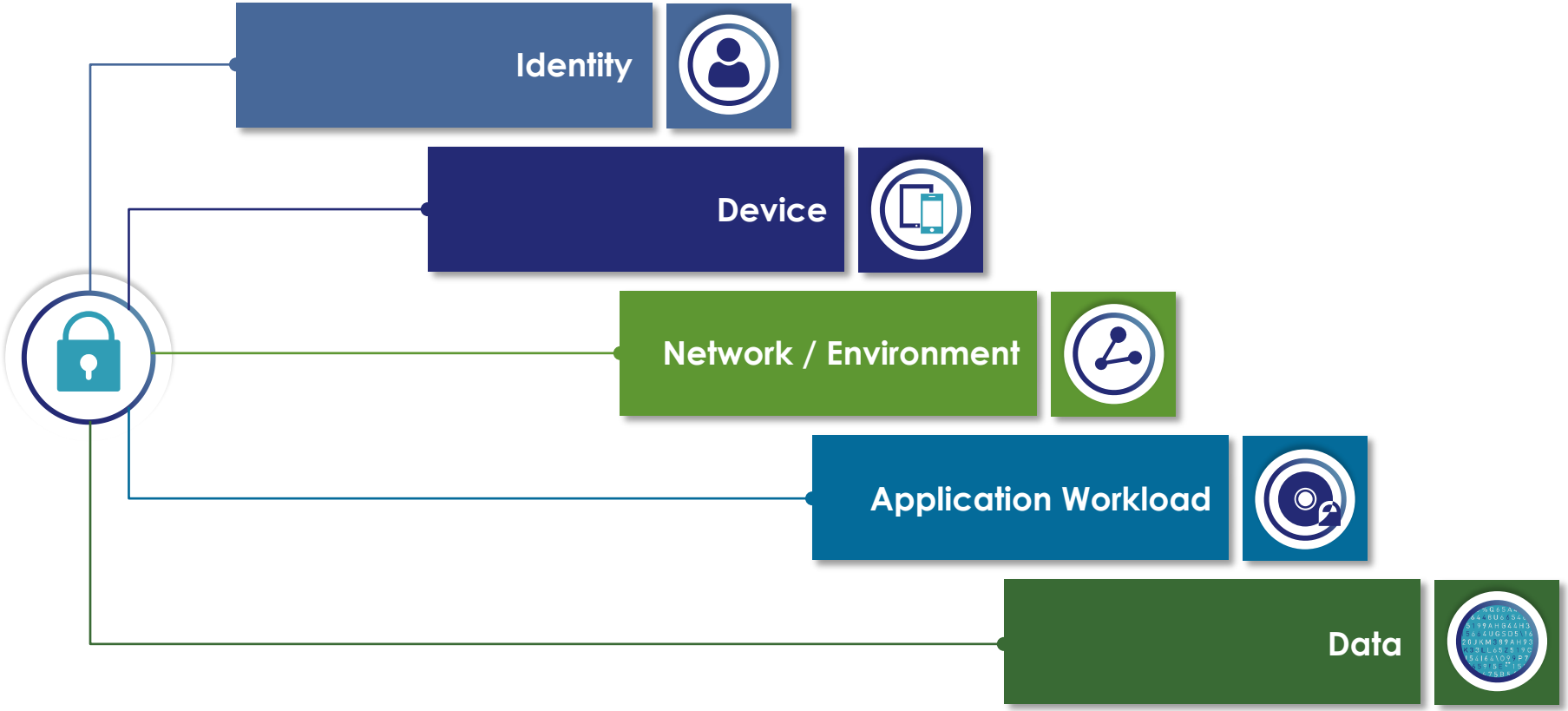
Zero Trust Principle: All transactions within the enterprises are **untrusted** (default deny) and access/transactions are based on…



…and not **where** you are → **Never Trust – Always Verify**

THALES

Foundational Pillars of Zero Trust



CISA Zero Trust Maturity Model

THALES

Zero Trust Foundation Activities

Robust Identity processes

Phishing proof MFA

SSO/Federated Identity across multiple apps

Leverage Privileged Access Management

Positive, accurate inventory of all devices

End point security for all devices/nodes

Detection and response for all endpoints

Network encryption

Encryption of all DNS and HTTPS endpoint traffic

Develop network segmentation

Develop Encrypted Email capability

Enable and enforce secure coding practices

Leverage DevSecOps as a development paradigm

Bake in security to applications during development cycle

Perform routine and open application vulnerability assessments

Develop a Zero Trust data strategy enforcing least privilege

Ensure compliance with data discovery

Leverage data at rest encryption with granular, policy based configuration

Track and review all access

THALES

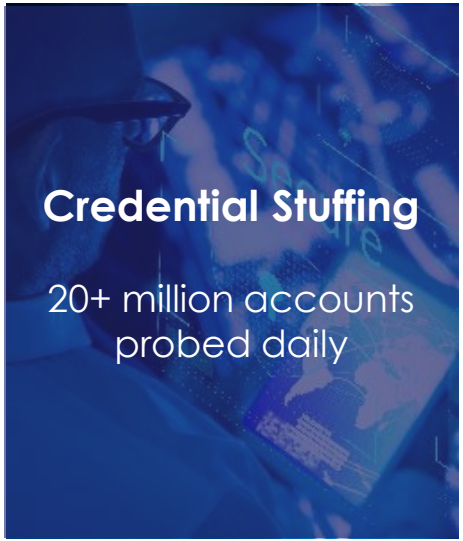
THALES
Building a future we can all trust

Implement Multifactor Authentication

Section 1 (b) (iii)

"Agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit."

What Types of Attacks Use Compromised Credentials



The consequences of data breaches can be catastrophic

- Stolen credentials for sale online, starting at $16! (source ZDNet)
- The average total cost incurred from a data breach is $3.86m! (source Ponemon Institute 2021)

Identity Access Management

Policy-based access

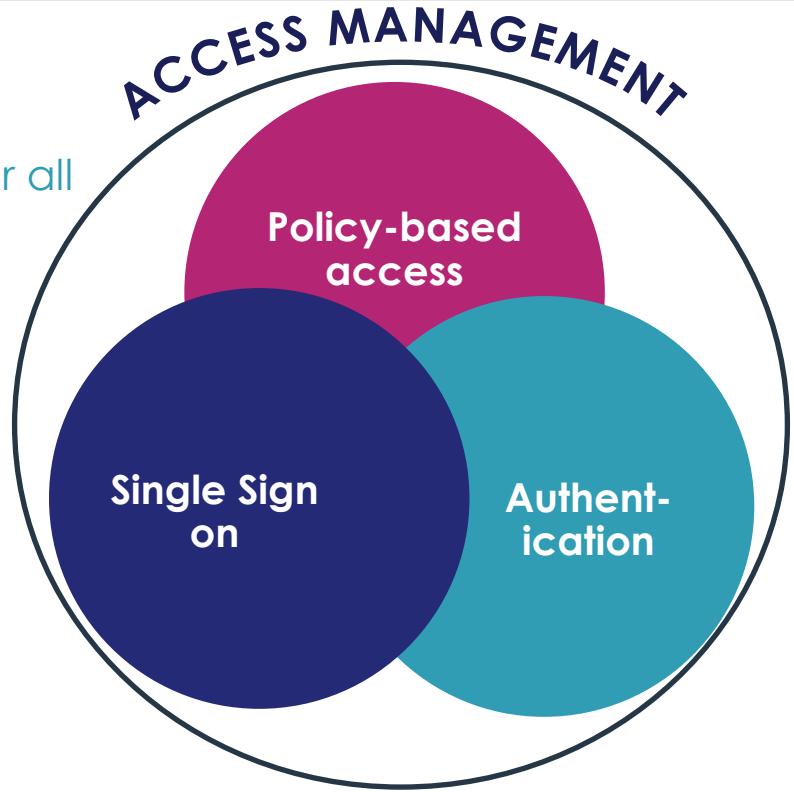
Optimize convenience and access security for all apps and services

Authentication

Prevent data breaches by applying the right level of security for your on-prem and cloud apps

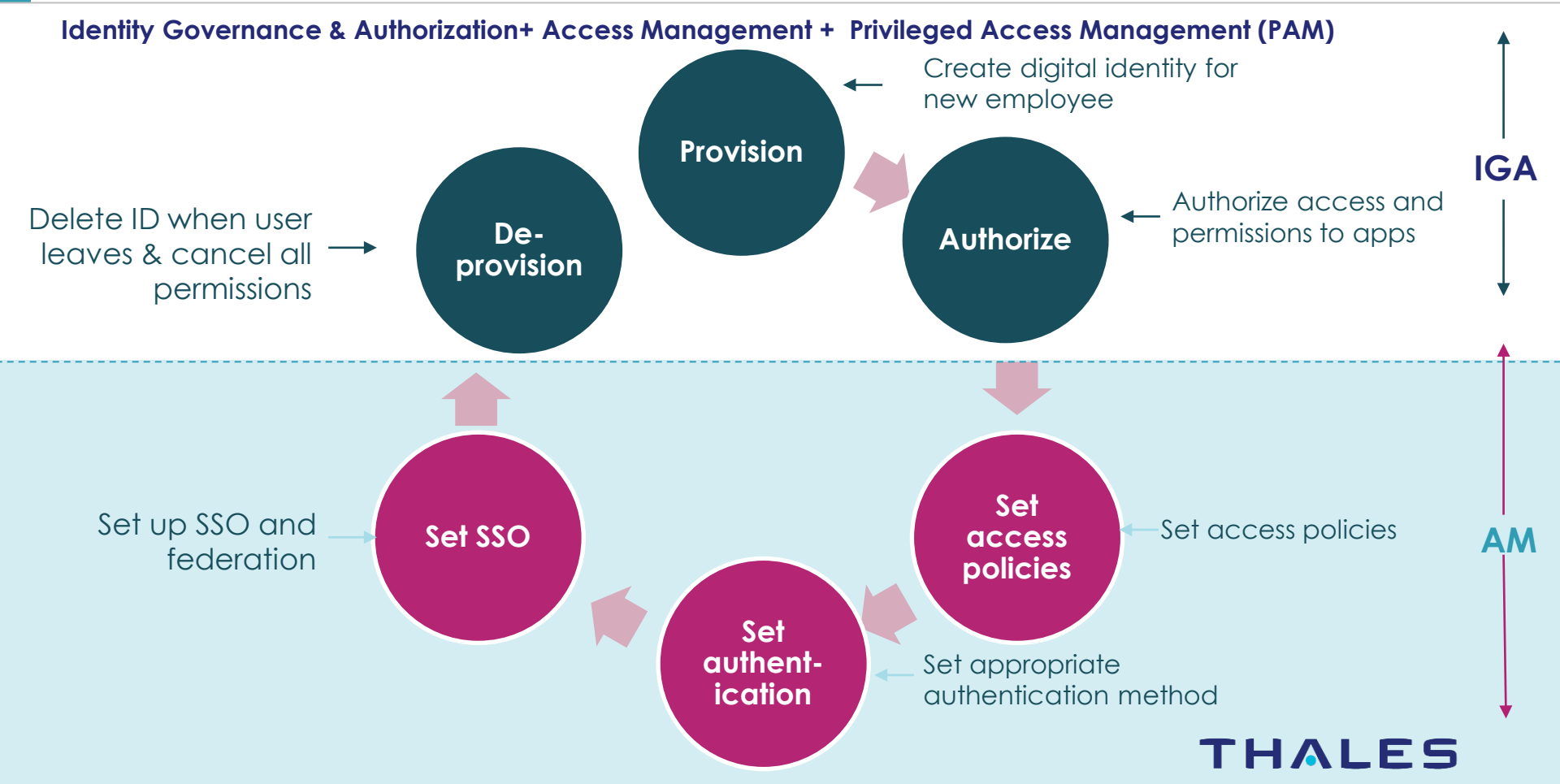
Smart Single Sign On

Make it easy and secure for users to log into apps



THALES

Identity and Access Management



THALES

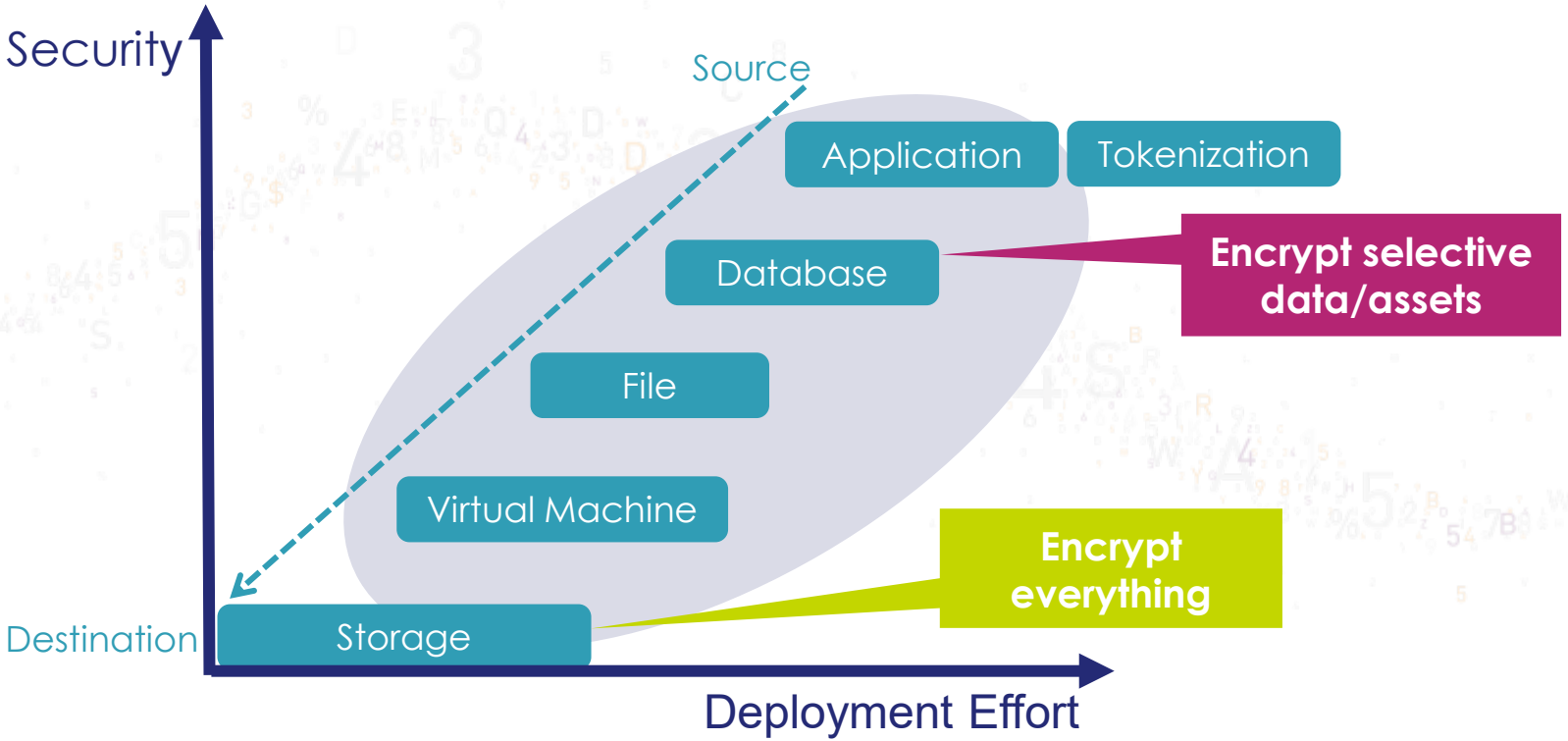
THALES
Building a future we can all trust

Data-at-Rest & in-Transit Encryption

Section 1 (b) (iii)

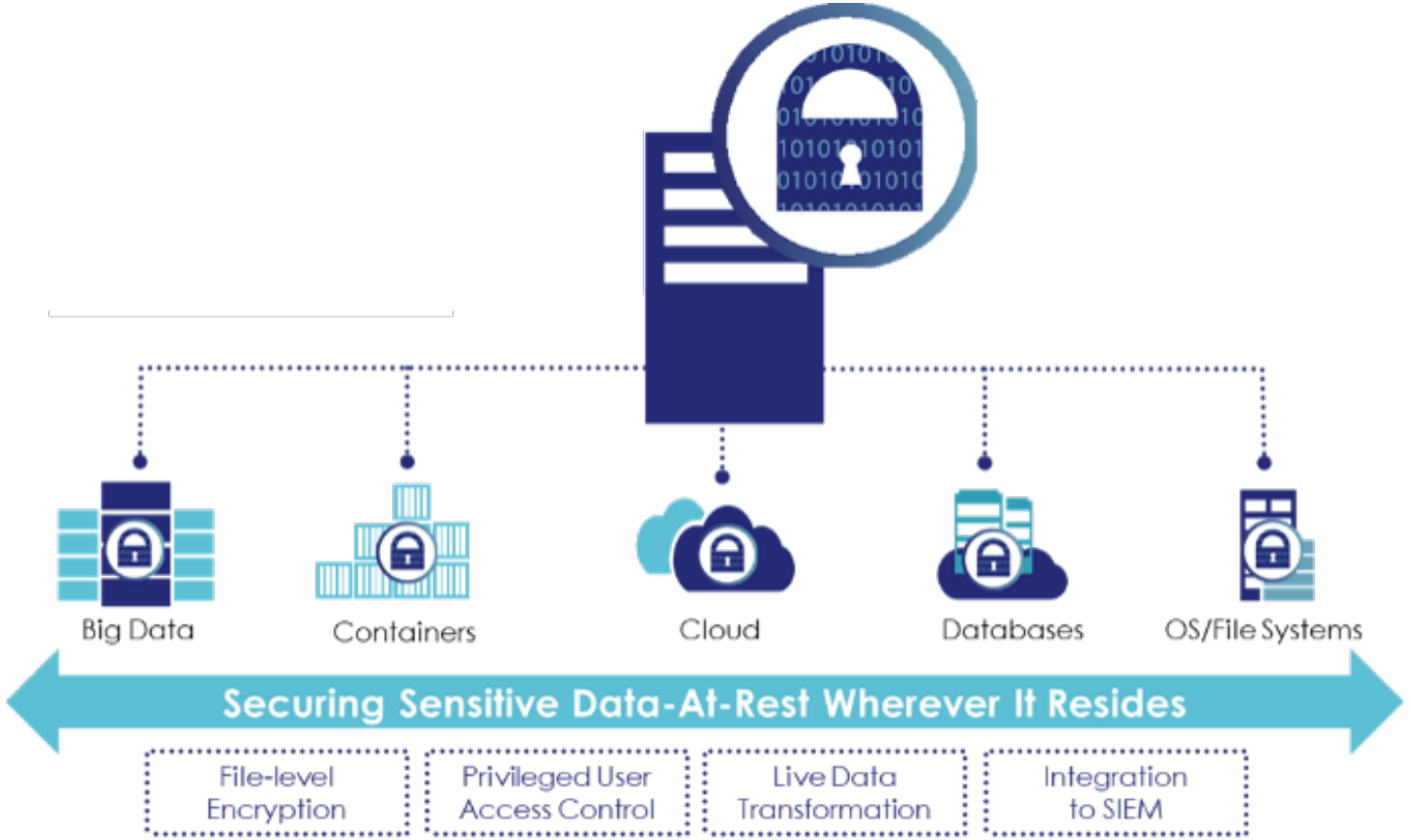
"Agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit."

Data at Rest Encryption: Where to Encrypt?



THALES

Data at Rest Encryption with Access Control



THALES

Modern Networks: Encryption Challenges

Latency

Applications have different sensitivities to latency

Transparency

Support encryption over any kind of access or transport network

Applicability

Apply encryption at customer premises, data center or public cloud

Cost

Cost per encrypted bit and initial cost are important

Compatibility

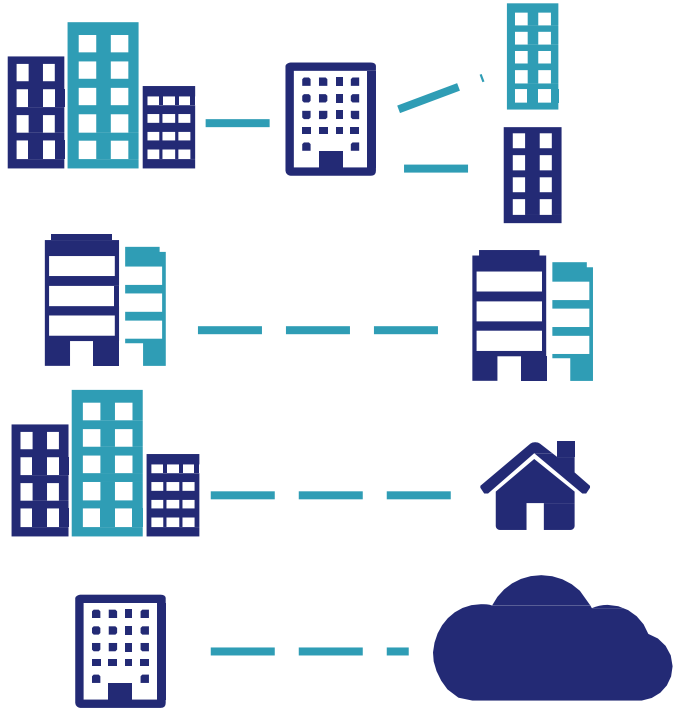
Support services at the layer where they perform best

Efficiency

Encryption has an impact on resource and network utilization

Your Data, Video and Voice is on the Move

- From site to site, or multiple sites
- From Data center to data center, for backup and disaster recovery
- To the last mile, curb, cabinet
- On-premises, up to the cloud



THALES

THALES

Quantum Resistant Cryptography

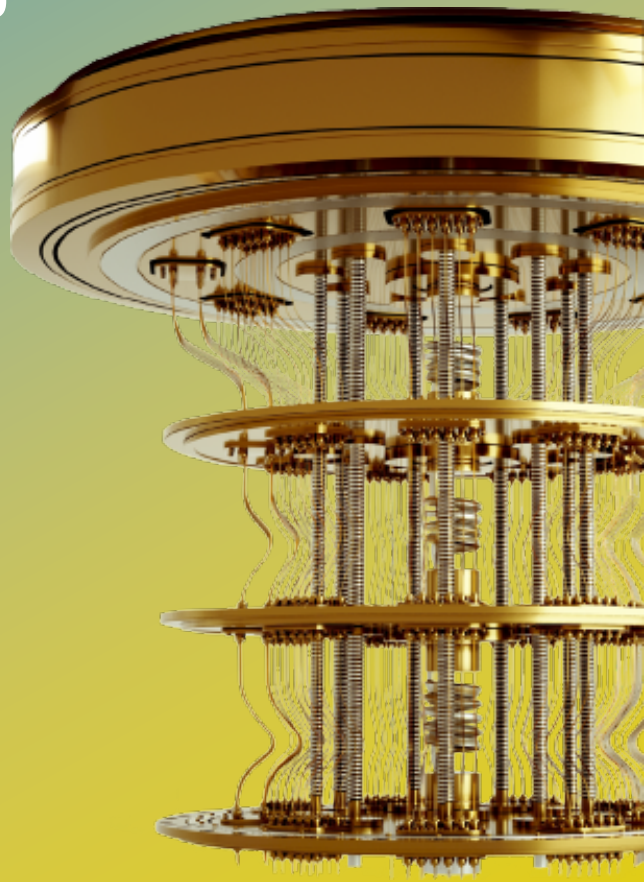
Section 1 (iv) (B) & (D)

"The NSA shall revise and make available relevant references regarding …quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary."

"Agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA."

Emerging Threats: Quantum Computing

Of respondents said they were concerned with ‘tomorrow’s decryption of today’s data’ when asked to identify security threats from quantum computing.
Only **2%** said they were not presently concerned.



Recommended Quantum Safe Transition Strategy

How a quantum computer impacts cryptography

Grover 1

Shor 2

Cryptographic algorithm	Type	Purpose	Impact from large scale QC
AES		ryption	Longer keys needed
SHA-2, S		functions	Larger output needed

Cryptogr algorit		rpose	Impact from large scale QC
RSA		atures, ablishment	No longer secure
Digital Sig Algorit		atures, xchange	No longer secure
ECDSA (Elliptic Curve DSA)	Public key	Signatures, Key exchange	No longer secure

Don't panic!

THALES

How to Prepare

Getting Ready for PQC (NIST)

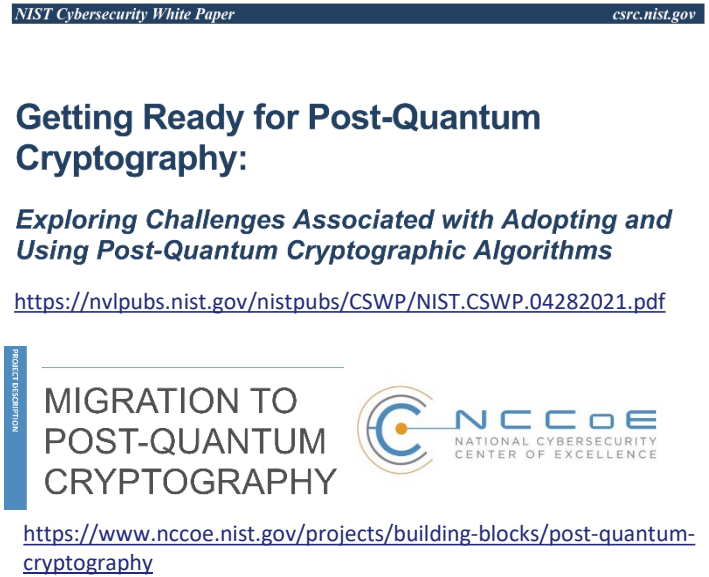
- Monitor standards development
- Risk assessment
  - Where is public-key crypto used
  - Is my equipment crypto-agile

NCCoE Crypto-Agility Project

- Whitepaper, playbooks, and proof-of-concepts
- Discovery tools to identify risk
- Get involved or use the output

NSA PQC FAQ

- Good summary, worth reading.
- Awaiting NIST recommendations



THALES

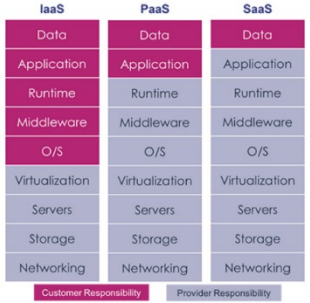
Crypto-agility

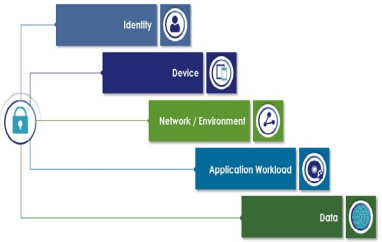
- The ability to quickly modify underlying crypto primitives
- Flexible upgradeable technology
- No built-in obsolescence

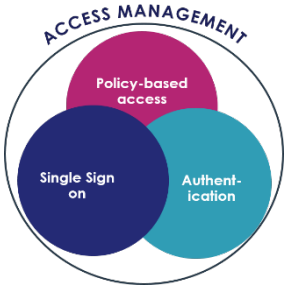
THALES

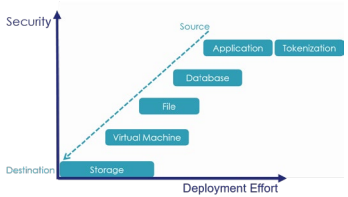
Top 5 Ways to Comply with the Cyber National Security Memo for NSS

1. Cloud Security
2. Zero Trust
3. Multifactor Authentication
4. Data-at-Rest & in-Transit Encryption
5. Quantum









THALES

THALES
Building a future we can all trust

Thank You!