Zero Trust: Top 5 Best Practices

Gina Scinta
Deputy CTO

Thales Trusted Cyber Technologies

Zero Trust: Top 5 Best Practices

Tip #1

Focus on the Data

Tip #2

Assess Current Capabilities

Tip #3

Source from a Secure Supply Chain

Tip #4

Leverage Vendor Expertise

Tip #5

Mature Over Time

Tip #1: Focus on the Data

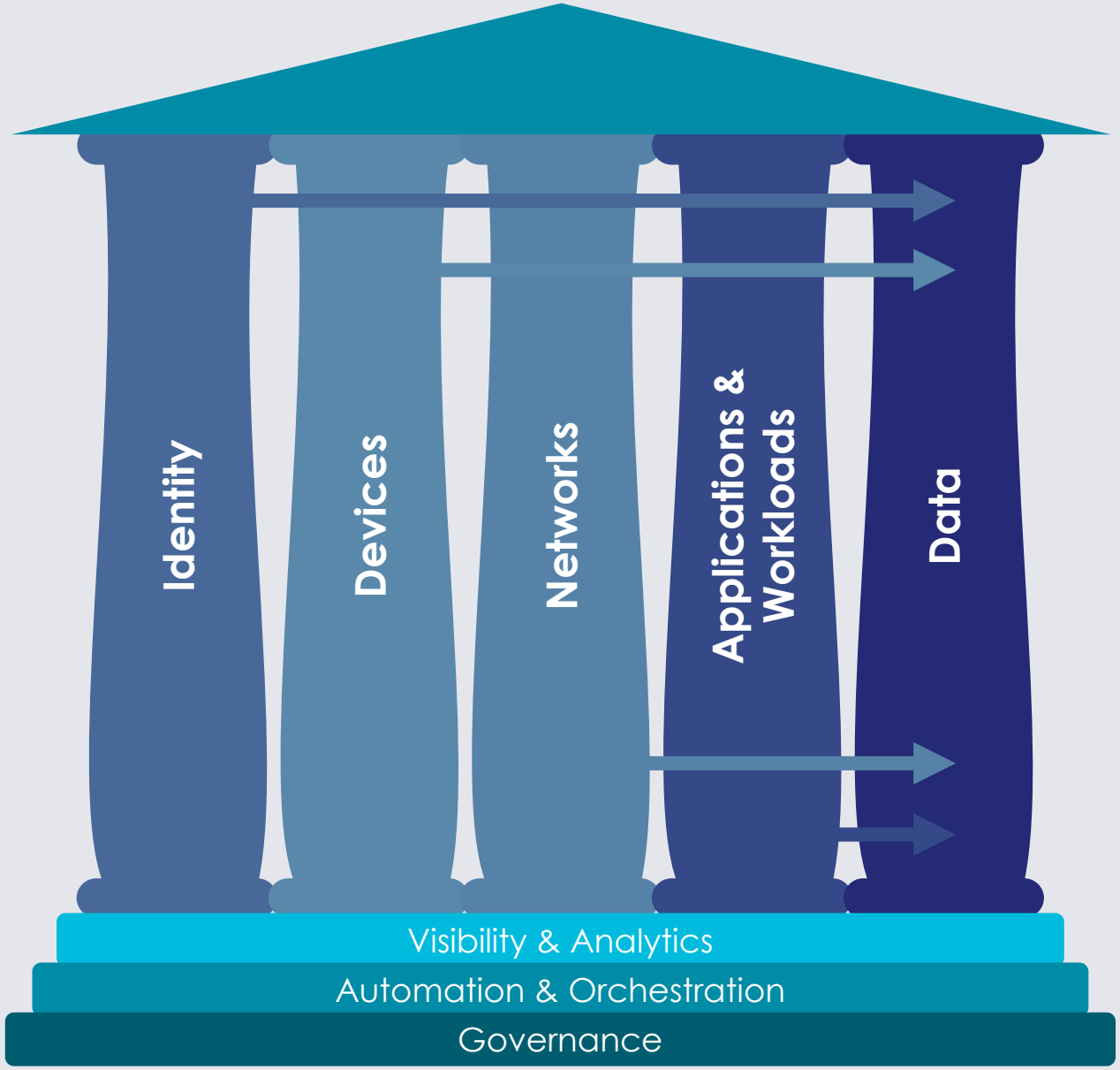
Focus on the Data – CISA Maturity Model

CISA Zero Trust Maturity Model 2.0

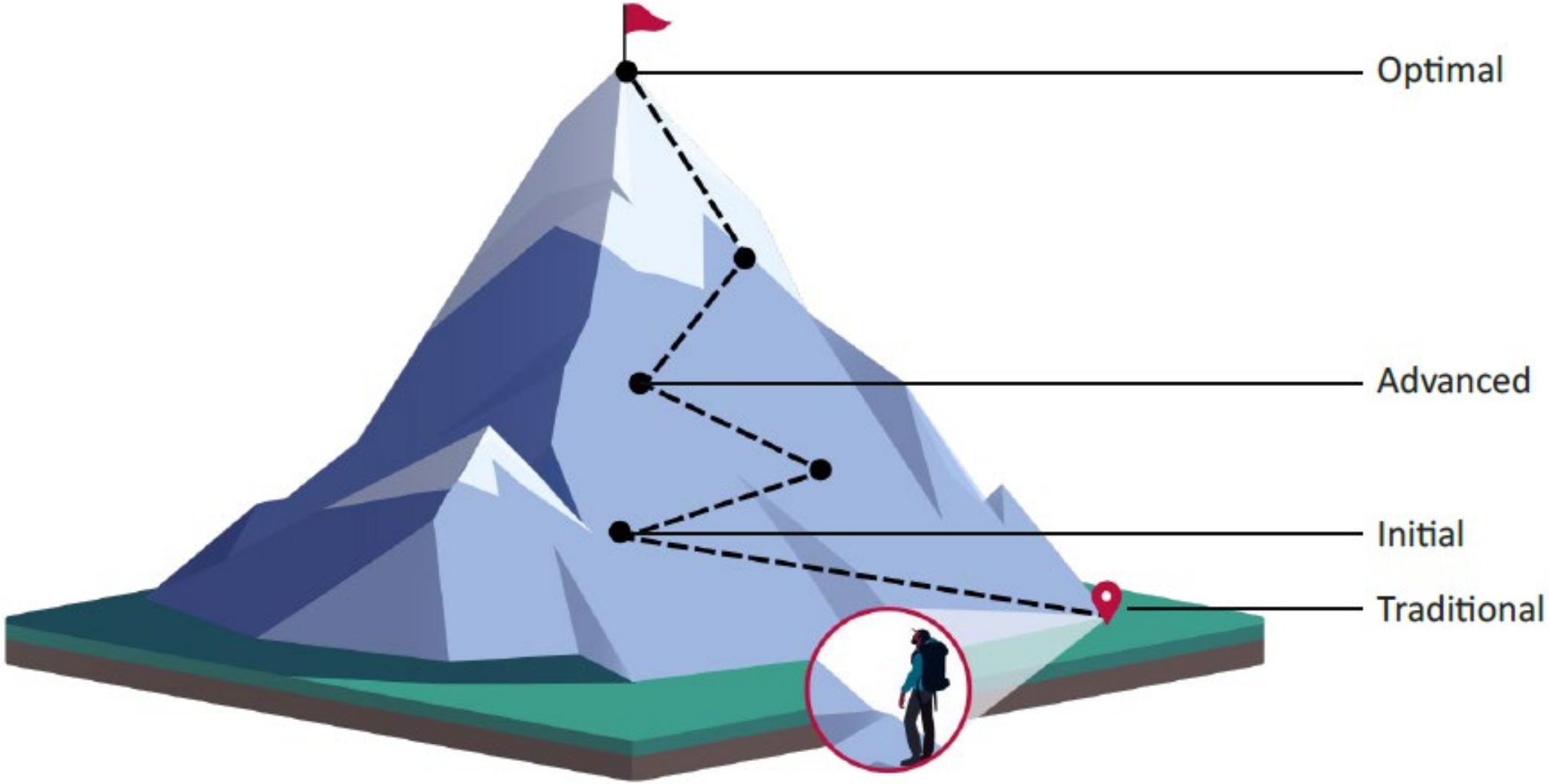
"SP 800-207 emphasizes that the goal of ZT is to '**prevent unauthorized access to data and services** coupled with making the access control enforcement as granular as possible.'"

"Zero trust presents a shift from a location-centric model to an identity, context, and **data-centric** approach…"

"Fundamentally, zero trust may require a change in an organization's cybersecurity philosophy and culture."



CISA Zero Trust Maturity Journey

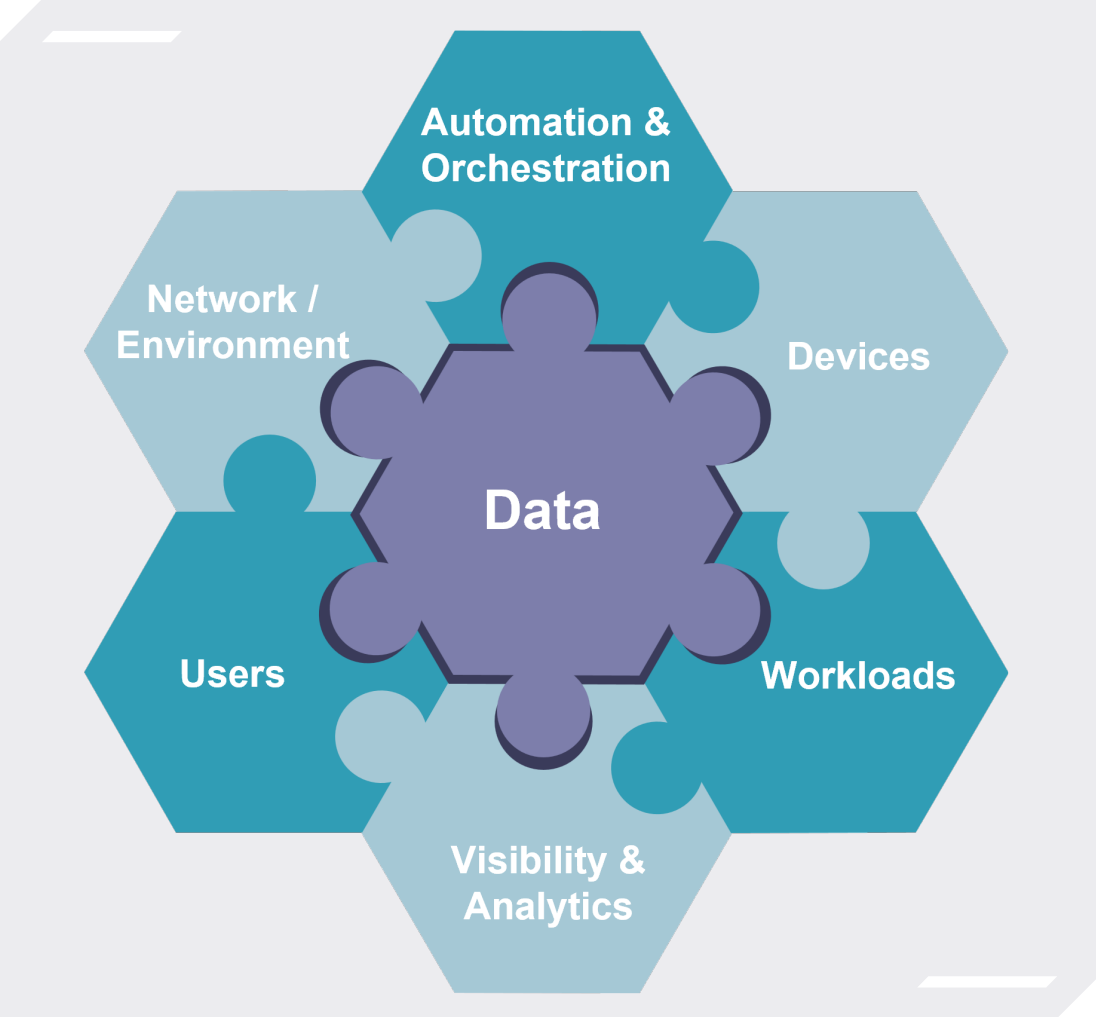


Zero Trust Maturity Model: Then

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	Password or multifactor authentication (MFA) Limited risk assessment	Limited visibility into compliance Simple inventory	Large macro-segmentation Minimal internal or external traffic encryption	Access based on local authorization Minimal integration with workflow Some cloud accessibility	Not well inventoried Static control Unencrypted
Advanced	MFA Some identity federation with cloud and on-premises systems	Compliance enforcement employed Data access depends on device posture on first access	Defined by ingress/egress micro-perimeters Basic analytics	Access based on centralized authentication Basic integration into application workflow	Least privilege controls Data stored in cloud or remote environments are encrypted at rest
Optimal	Continuous validation Real time machine learning analysis	Constant device security monitor and validation Data access depends on real-time risk analytics	Fully distributed ingress/egress micro-perimeters Machine learning-based threat protection All traffic is encrypted	Access is authorized continuously Strong integration into application workflow	Dynamic support All data is encrypted

Zero Trust Maturity Model: Now

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	Password or multifactor authentication (MFA) Limited risk assessment	Limited visibility into compliance Simple inventory	Large macro-segmentation Minimal internal or external traffic	Access based on local authorization Minimal integration with workflow	Not well inventoried Static control Unencrypted
Advancec Initial	MFA with passwords Self-managed and hosted identity stores Manual risk assessments Access expires with automated review	All physical assets tracked Limited device-based access control and compliance enforcement Protections delivered via automation	Initial isolation of critical workloads Increased availability for more applications More encryption, formalize key management	Some mission critical workflows accessible over public networks Formal code deployment through CI/CD pipelines Static & dynamic security testing	Limited automation Begin strategy for categorization Encrypt in-transit Initial centralized key management policies
Optimal	Real time machine learning analysis	monitor and validation Data access depends on real-time risk analytics	ingress/egress micro-perimeters Machine learning-based threat protection	continuously Strong integration into application workflow	All data is encrypted



Focus on the Data – DoD Reference Architecture

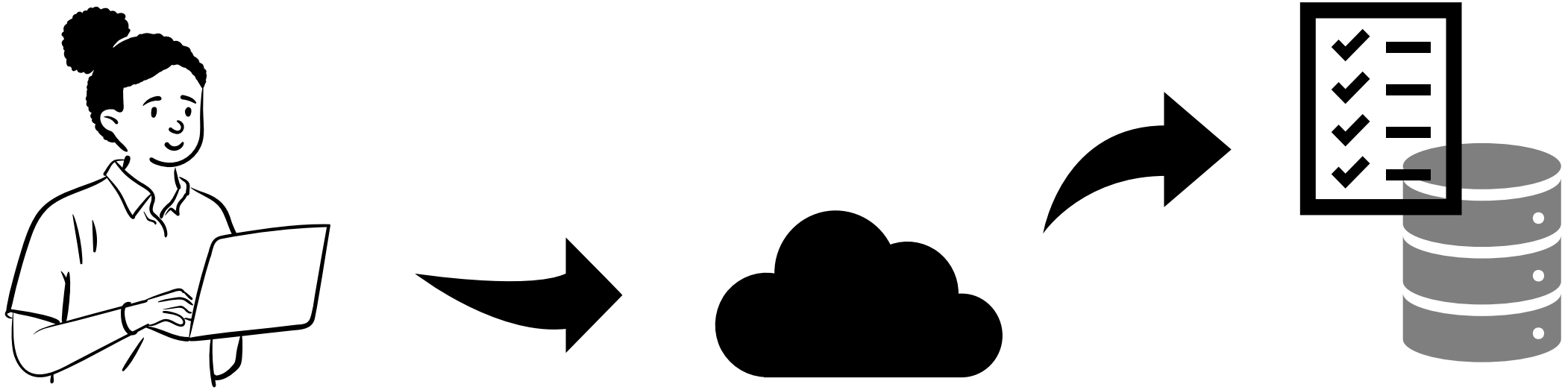
DoD Zero Trust Reference Architecture 2.0

"ZT principles, Pillars and culture will guide mission owners in their efforts to reconfigure, re-prioritize and augment existing DoD capabilities to evolve portfolios and resources **towards a revised, data centric DoD Cybersecurity Reference Architecture** (CS RA)."

"All protection Pillars work together to effectively secure the **Data Pillar**."

Focus on the Data – In Action

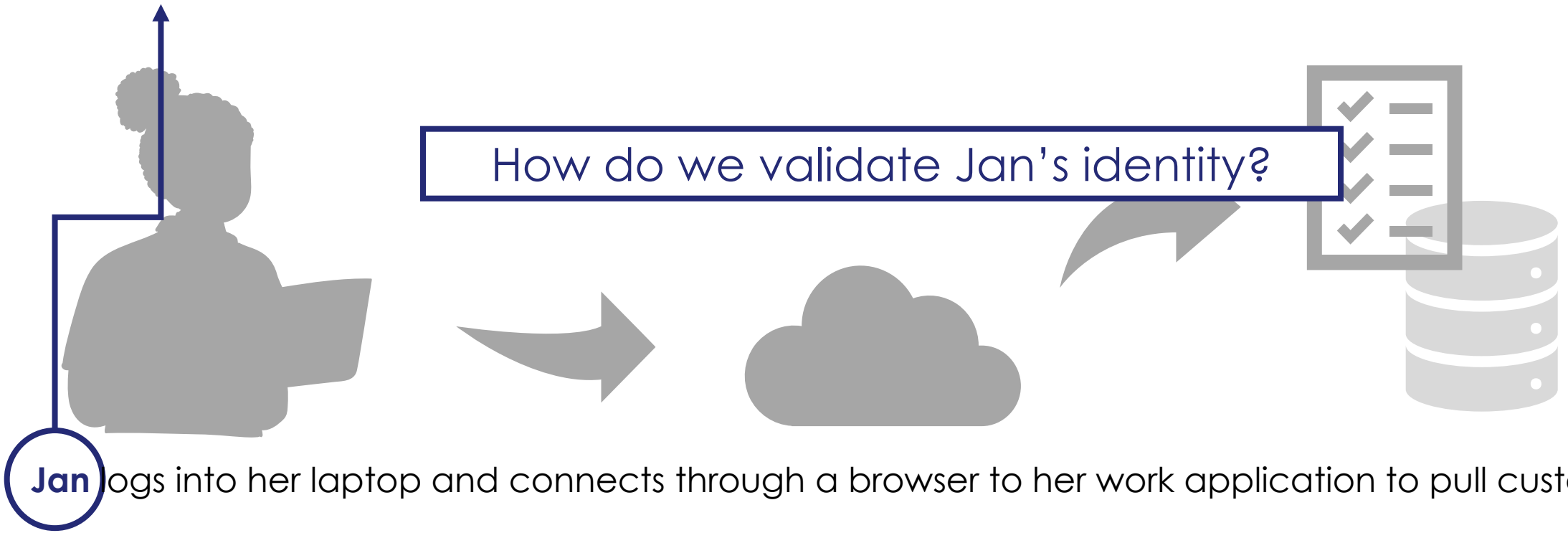
Identity | Device | Network | Application | Data



Jan logs into her laptop and connects through a browser to her work application to pull customer info.

Focus on the Data – In Action

Identity | Device | Network | Application | Data



Jan logs into her laptop and connects through a browser to her work application to pull customer info.

Focus on the Data – In action: Validating the Identity

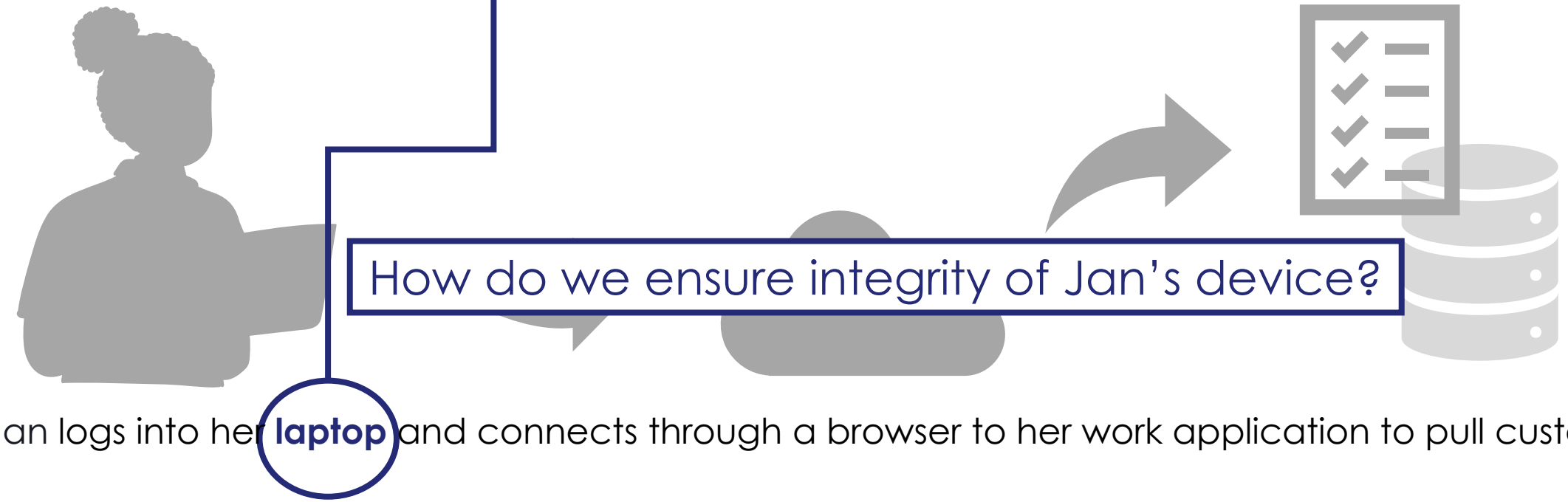
Validating Jan's Identity

Jan presents her **token**
provisioned by a **CMS**
backed by an **HSM-rooted** PKI,
and authenticates with **MFA**.

What if "Jan" is a Non-Person Entity?

"Jan" calls to its **HSM-rooted credential**
backed by an **HSM-rooted** PKI
and authenticates with **MFA**,
as instructed by a **robot orchestrator**.

Focus on the Data – In Action



Jan logs into her **laptop** and connects through a browser to her work application to pull customer info.

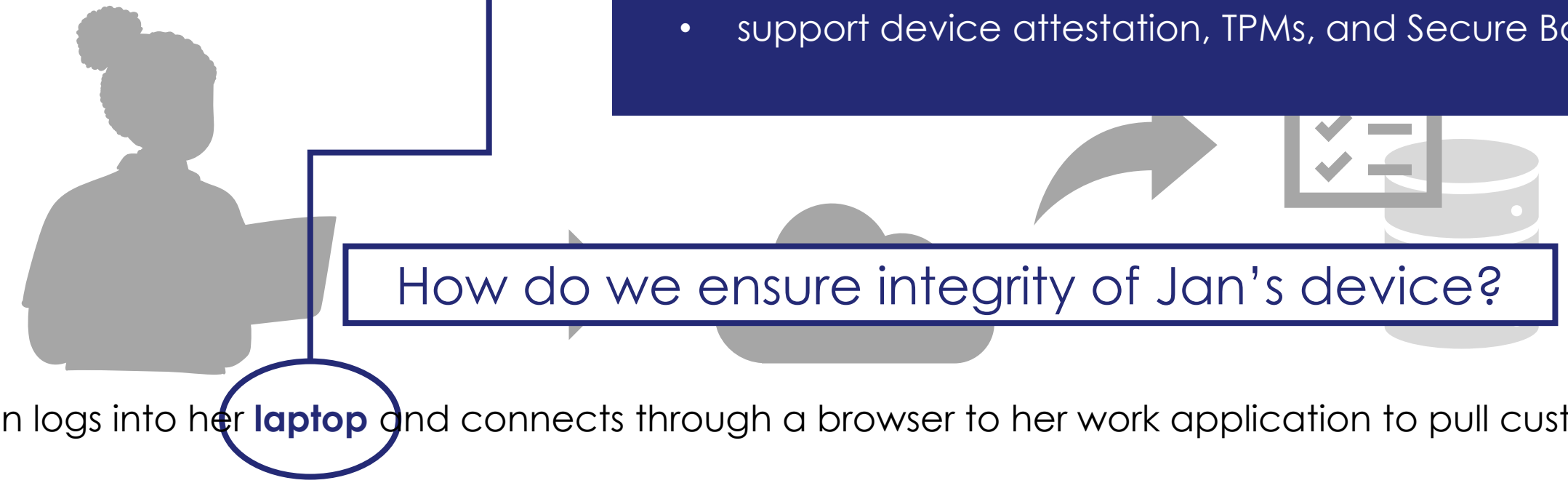
Focus on the Data – In Action: Ensure Integrity of Jan's Device

Identity

Device

Use an **HSM** to:

- store non-person entity credentials,
- generate secure device identities,
- cryptographically sign identity-related data, and
- support device attestation, TPMs, and Secure Boot.

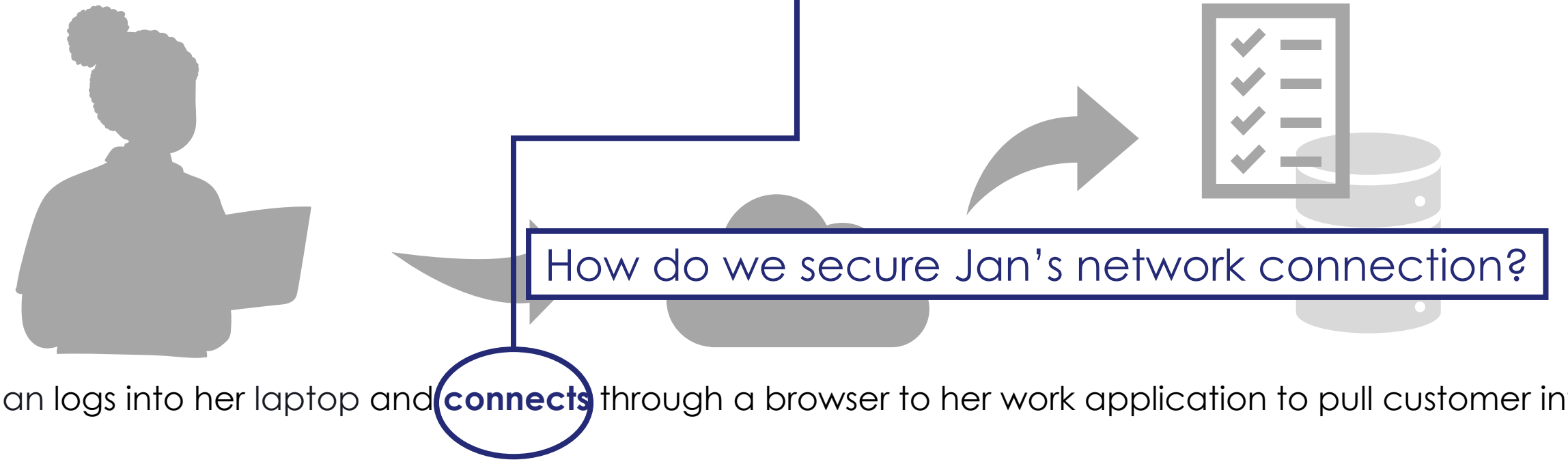


How do we ensure integrity of Jan's device?

Jan logs into her **laptop** and connects through a browser to her work application to pull customer info.

Focus on the Data – In Action

Identity | Device | Network | Application | Data

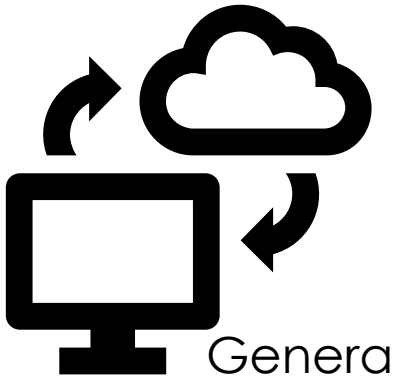


Jan logs into her laptop and **connects** through a browser to her work application to pull customer info.

Focus on the Data – In Action: Protecting Network Traffic

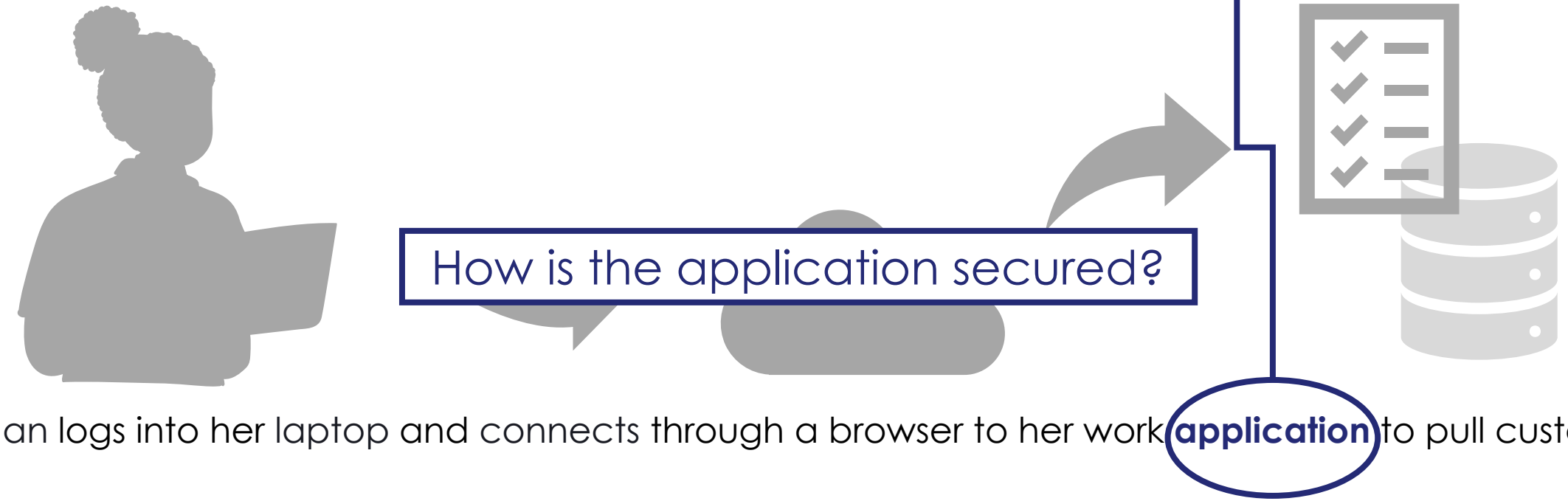
Use a **High Speed Encryptor** for:

- end-to-end, authenticated encryption,
- embedded, zero-touch encryption key management, and
- virtual or hardware-based appliances.



Generate and store SSL/TLS keys on an **HSM**.

Focus on the Data – In Action



Jan logs into her laptop and connects through a browser to her work **application** to pull customer info.

Focus on the Data – In Action: Securing an Application

The application code is signed by keys held in an **HSM**.
Jan is revalidated using her issued **token** and **MFA**.
Application data is **encrypted** through all life cycle states.

Application

Data

How is the application secured?

Jan logs into her laptop and connects through a browser to her work **application** to pull customer info.

Focus on the Data – In Action

Identity | Device | Network | Application | Data

What secures the data held by the organization?

Jan logs into her laptop and connects through a browser to her work application to pull **customer info.**

Focus on the Data – In Action: Securing the Data

The enterprise maintains an **inventory** of its sensitive data.
Encryption keys are maintained in a **centralized key manager**.
All data is encrypted by a **unified encryption platform** or
by a solution rooted in an **HSM**.
Files have been stripped of malware through **content disarm & reconstruction**.
Access to discrete data may again require Jan to revalidate with **MFA**.

Data

Jan logs into her laptop and connects through a browser to her work application to pull **customer info**.

Tip #2: Assess Current Capabilities

Assess Current Capabilities

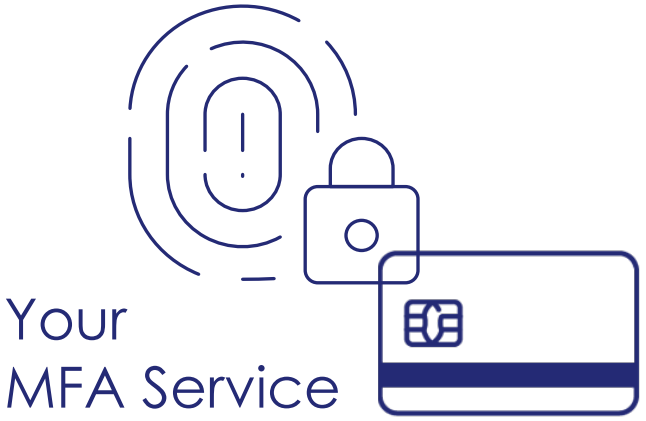
How capable are your current products?

Traditional
Passwords or MFA

Initial
MFA with passwords

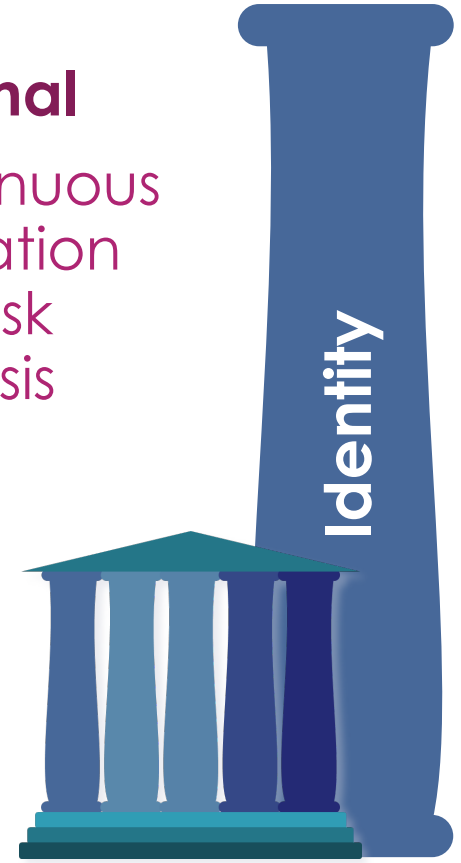
Advanced
Phishing-resistant MFA

Optimal
Continuous validation and risk analysis



Your MFA Service

Deployed Today



Assess Current Capabilities

How capable are your current products?

Traditional
Passwords or MFA

Initial
MFA with passwords

Advanced
Phishing-resistant MFA

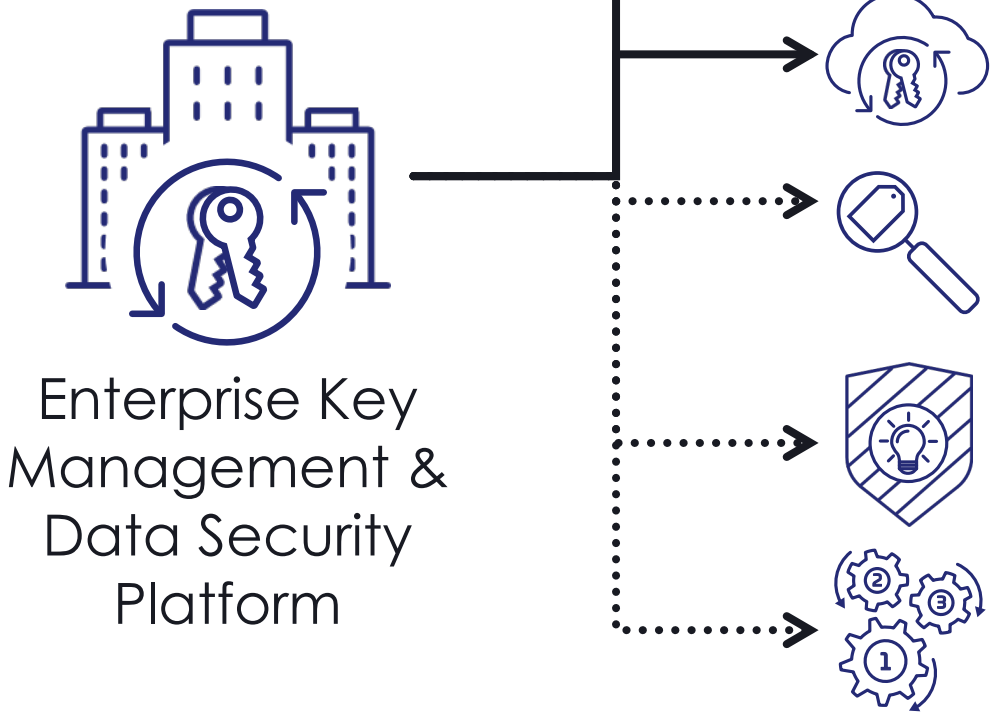
Optimal
Continuous validation and risk analysis

Your MFA Service

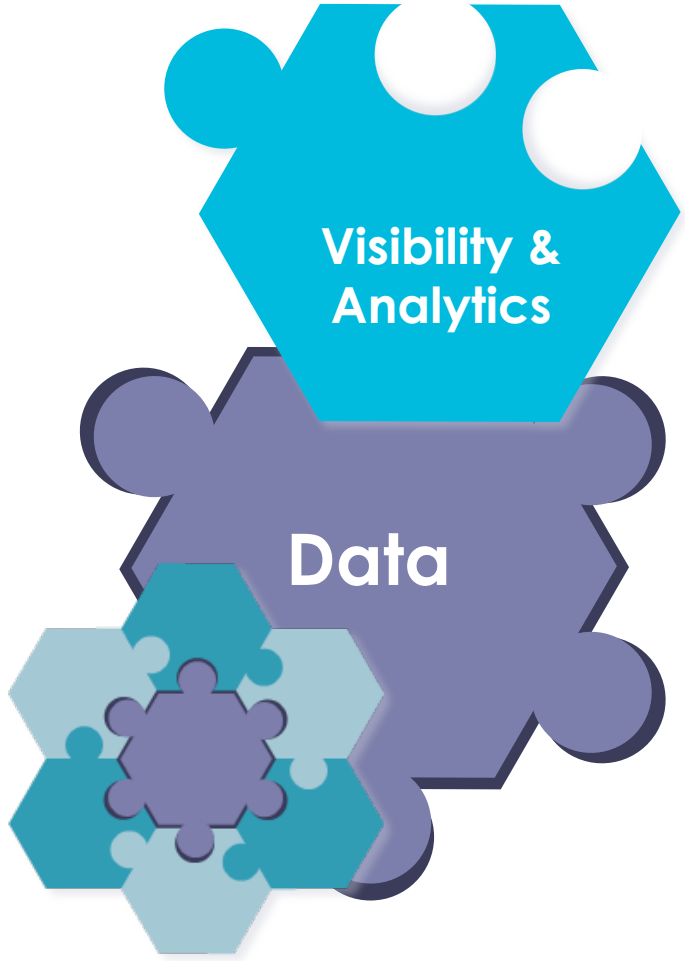
Capable for Tomorrow

Assess Current Capabilities

What platforms can expand through updates, licensing, or integrations?



- Data Encryption & Rights Management
- Data Access Control
- Data Labeling & Tagging
- User & Entity Behavior Analytics
- Automated Dynamic Policies



Tip #3: Source from a Secure Supply Chain

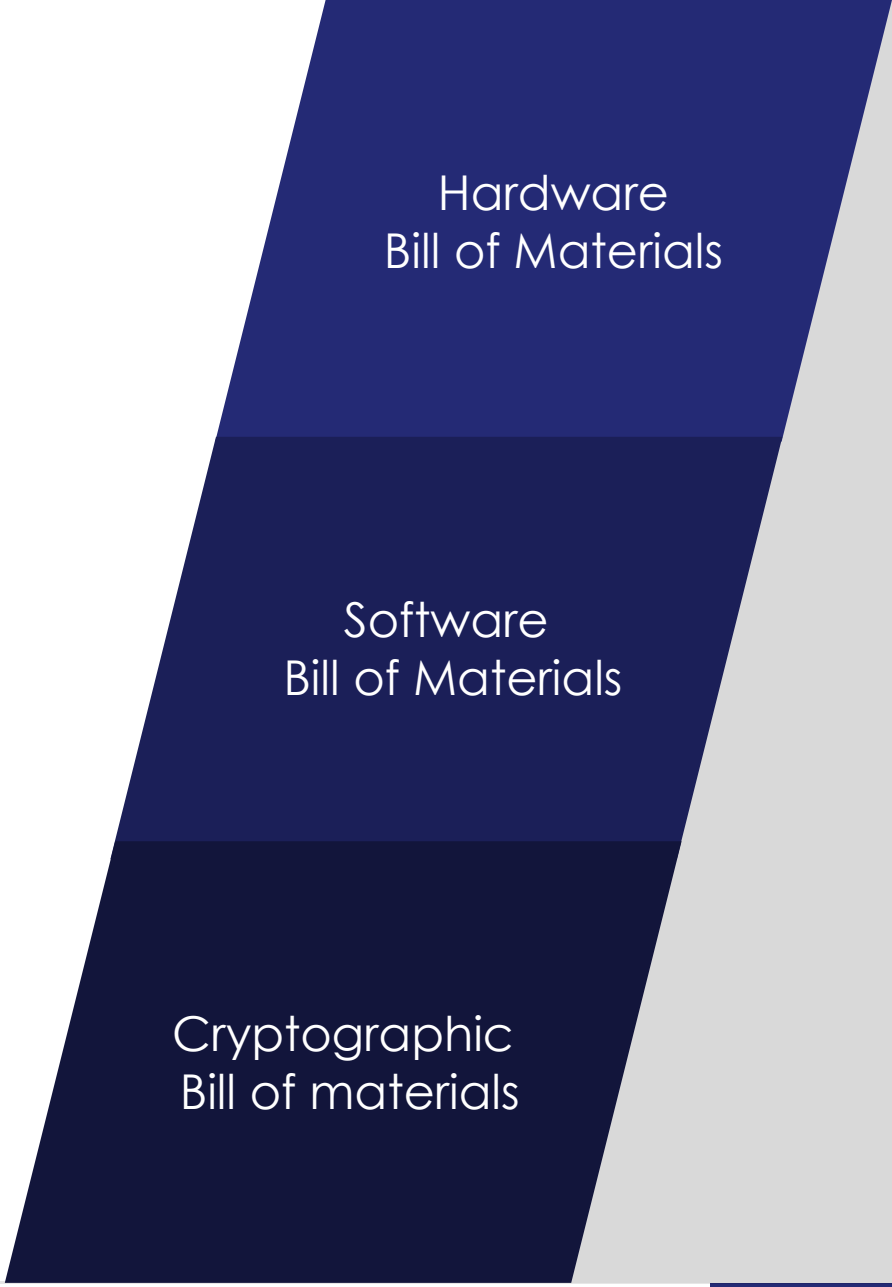
Source from a Secure Supply Chain – BOM Sniffing

What's the provenance of commercial product coming into your network?

CISA added "Asset & Supply Chain Risk Management" to its Zero Trust Maturity Model in v2.0

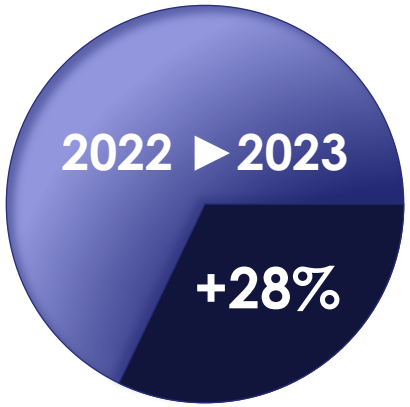
"The earlier that risk assessment and data classification can be applied in the software supply chain, the more mature the ZT application."

-DoD ZT Reference Architecture 2.0



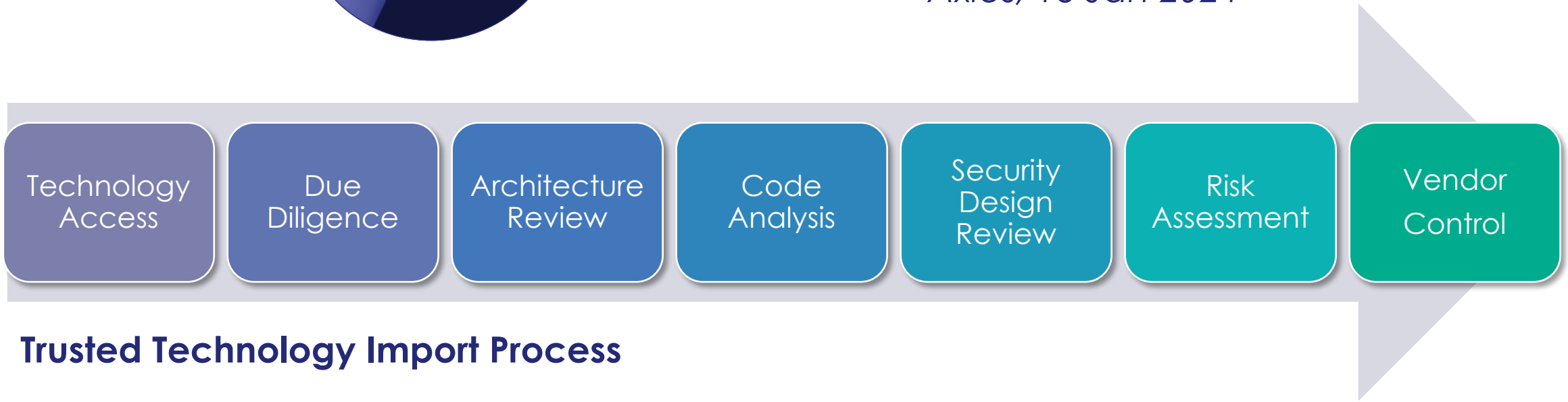
Source from a Secure Supply Chain – Trusted Tech Imports

How are your vendors protecting you from supply chain attacks?



Increase in the number of malicious packages available across three major open-source repositories

-Axios, 16 Jan 2024



Trusted Technology Import Process

Source from a Secure Supply Chain – Trusted Tech Imports

Trusted Technology Import Process

Thales Trusted Cyber Technologies will use a documented and approved process to import technology in a trusted manner such that the technology can be used in even the most sensitive programs and products.

Established in 2016

CFIUS National Security Agreement requires all products derived from Commercial Thales products go through TTI process

Best practice for any import of technology

- Commercial Thales products or components
- Open source software
- 3rd party software packages
- Commercial hardware for use in products

Tip #4: Leverage Vendor Expertise

Leverage Vendor Expertise – Depth is Essential

Network Infrastructure

Applications & Web Servers

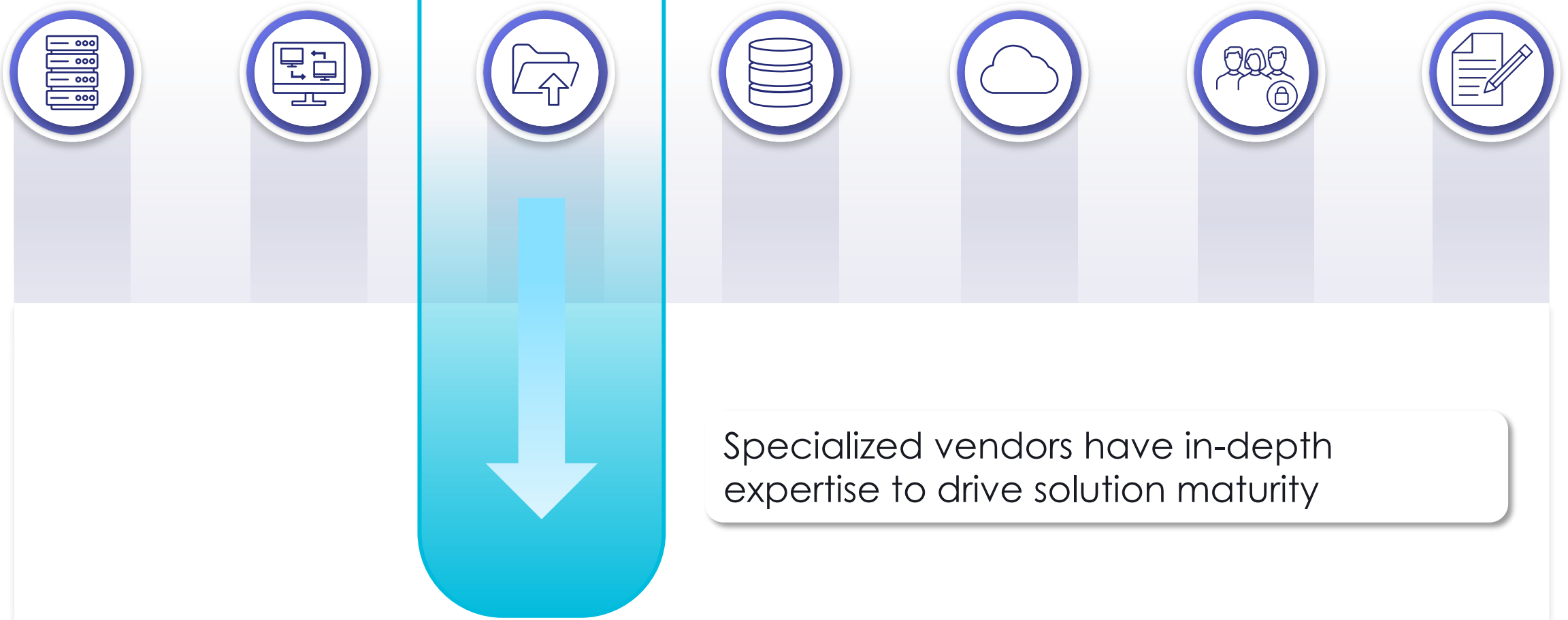
Storage Solutions

Databases

Cloud Infrastructure

Identity Solutions

Auditing & Governance



Specialized vendors have in-depth expertise to drive solution maturity

Leverage Vendor Expertise – Breadth is Unifying

Network Infrastructure

Applications & Web Servers

Storage Solutions

Databases

Cloud Infrastructure

Identity Solutions

Auditing & Governance

Use vendors & system integrators with experience across the Zero Trust pillars as Trusted Advisors

Gain post-procurement support as your architecture matures and extends to new 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

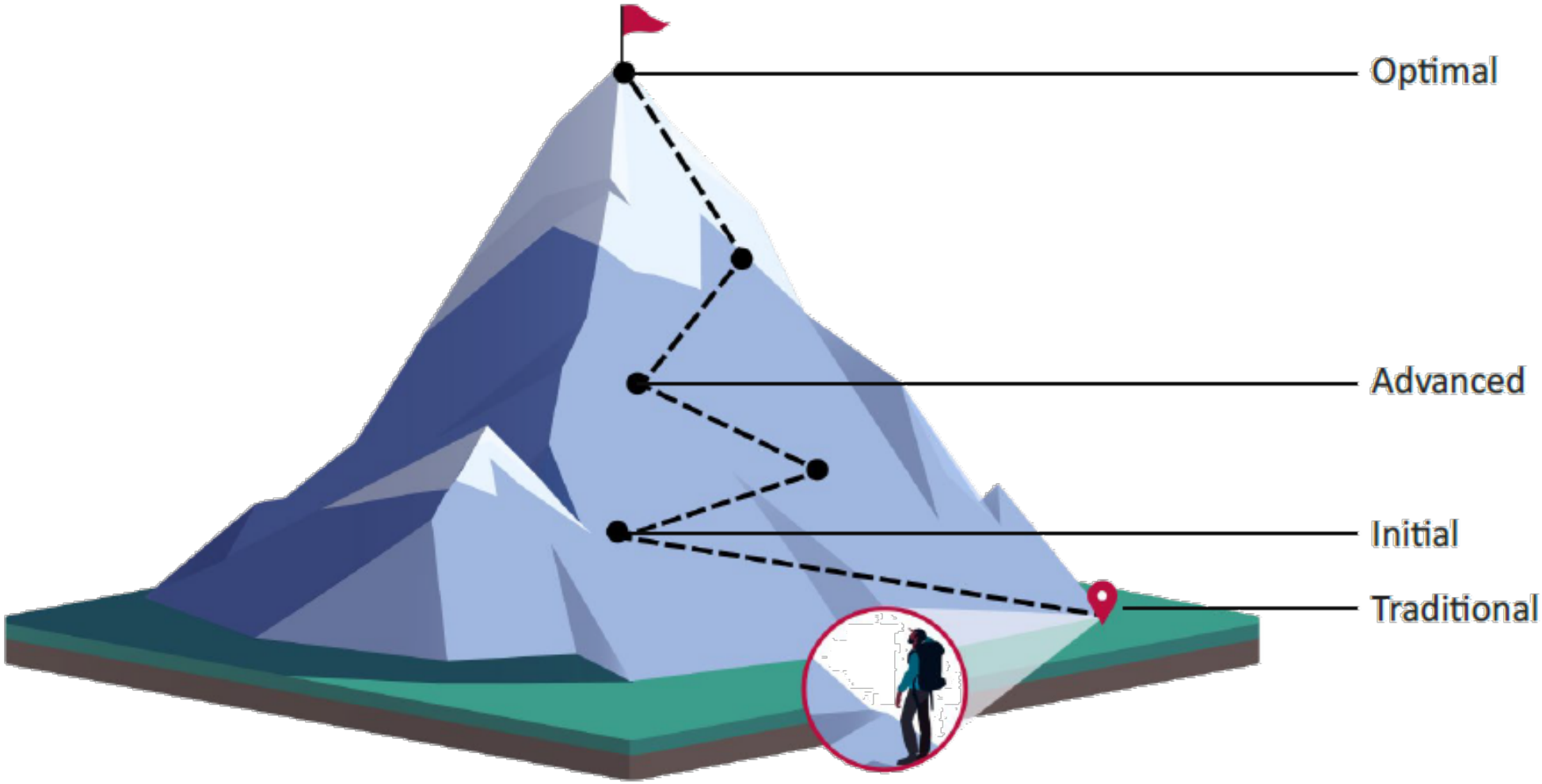
- 3rd Party
- Voice
- Pattern-Based
- Email
- Password
- OTP Push
- Kerberos
- Biometric
- SMS
- Number Matching

High Assurance MFA

- HA Certificate-based Smartcards & Tokens

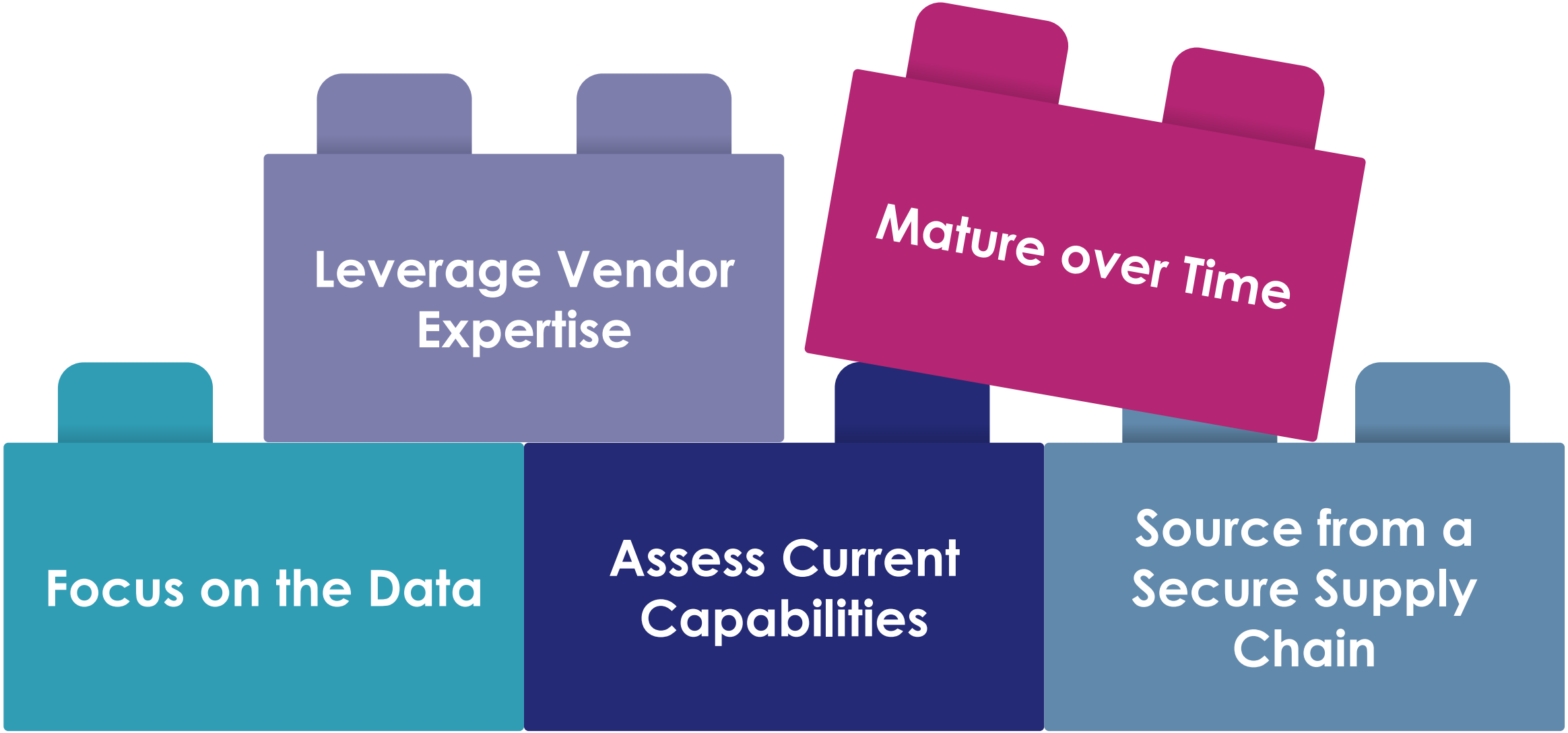
Tip #5: Mature Over Time

Mature Over Time – It's a Journey



CISA Zero Trust Maturity Model v2.0

Mature Over Time – Put all the Pieces Together



THALES
Building a future we can all trust

Questions

Gina Scinta

Deputy CTO

Thales Trusted Cyber Technologies

Gina.Scinta@thalestct.com